



## Pick-Up Service Transaction Manipulation Crimes in the Banking Legal Domain: A Model for Customer Legal Protection

\*I Made Aditya

Mantara Putra

Universitas Warmadewa,  
Indonesia

Johannes Ibrahim

Kosasih

Universitas Warmadewa,  
Indonesia

I Putu Suwantara

Universitas Warmadewa,  
Indonesia

---

**\*Corresponding author:**

I Made Aditya Mantara Putra, Universitas  
Warmadewa, Indonesia.

✉ [adityamantara@gmail.com](mailto:adityamantara@gmail.com)

---

**Article Info:**

**Article history:**

Received: August 10, 2026

Revised: September 23, 2026

Accepted: September 28, 2026

Available Online: October 2, 2026

---

**Keywords:**

Crime; Manipulation; Pick Up  
Service; Banking



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:** Pick-up service cash deposits increase convenience but expose customers to risks of manipulation during cash handover, transaction recording, and account crediting. The issue does not arise from a complete regulatory void; rather, existing banking, consumer-protection, anti-fraud, contractual, and governance rules do not specifically integrate the risk allocation and evidentiary safeguards required for this service.

**Objective:** This study analyzes when irregularities in pick-up service cash transactions constitute banking crimes or general crimes and formulates a customer-protection model.

**Methods:** Normative legal research was conducted through statutory and conceptual analysis of banking, consumer-protection, anti-fraud, and related legal materials. One interview concerning supervisory practices was used solely as supporting contextual material and analyzed descriptively to identify operational vulnerability points; it did not alter the normative research design.

**Results:** Manipulation of bank records, bookkeeping, documents, or transaction data by legally specified banking actors may fall within applicable banking-crime provisions, whereas the appropriation of entrusted funds or the use of deceit without such manipulation is assessed under applicable general criminal law. *Internal fraud* is treated as a governance and risk classification rather than as an independent offense. The study identifies eight operational vulnerability points, from scheduling to complaint handling, and proposes four protection layers: contractual, operational, institutional, and recovery protection.

**Conclusion:** The Layered Customer Protection Model is proposed as a normative framework to strengthen legal certainty, evidentiary protection, internal controls, complaint handling, and pathways for customer recovery, subject to implementation and further empirical evaluation.

---

**To cite this article:** Putra, I. M. A. M., Kosasih, J. I., & Suwantara, I. P. (2026). Pick-up service transaction manipulation crimes in the banking legal domain: A model for customer legal protection. *Journal of Law & Social Politics*, 4(4), 932-942. <https://doi.org/10.59261/jlsp.v4i4.270>

---

### INTRODUCTION

Indonesia's constitutional guarantees of equality before the law and legal certainty provide the general normative foundation for customer protection (Harahap, 2025; Taklima et al., 2023). In banking transactions, these guarantees are given concrete expression through sector-specific duties of prudence, transparency, accountability, and consumer protection. The analysis therefore focuses on whether the legal and institutional framework adequately protects

customers when cash is entrusted to bank officers outside bank premises through pick-up service arrangements.

In the national economic landscape, the banking industry is not merely a financial entity but also constitutes an epistemic and practical pillar supporting public trust in a civilized economic system (Azlina et al., 2022; Borg & Hooker, 2019). The development of information technology has encouraged the transformation of banking services, both digital and conventional, including pick-up service cash services—a conventional service that provides convenience by enabling banks to collect customer funds outside bank premises. In response to developments and intense competition in the banking industry, banks have introduced various business innovations while continuing to maximize their conventional business activities. In this regard, trust is the primary capital in banking business activities. This means that the public tends to prefer one financial institution over another based on the belief that their funds are safe and can be withdrawn whenever needed (Rasyid, 2026).

Under the financial-sector framework established by Law Number 4 of 2023 concerning Development and Strengthening of the Financial Sector (P2SK Law), as subsequently amended, banks operate as financial services institutions that collect and channel public funds and are therefore subject to banking governance, prudential, and consumer-protection obligations. According to Kasmir, customers are consumers who purchase or utilize products offered by banks. Based on this definition, customers in this study are, in principle, entitled to protection in every banking transaction they undertake.

In examining the role of banks as institutions that collect funds from the public and redistribute them, a relationship between banks and customers is established on the basis of trust and legal obligations. Banks can operate and develop only if the public trusts them to deposit their funds in various banking products offered by the banks. This trust enables banks to collect funds from the public and subsequently redistribute them in the form of credit to support economic activities (Ningsih, 2021).

In carrying out banking activities, fundamental principles are required as a foundation. The principles underlying the contractual relationship between banks and customers include the principle of economic democracy, the fiduciary principle, the prudential principle, the confidentiality principle, and the know your customer principle (Anugrahita & Baidhowi, 2025). The application of these principles is important for banks in creating a sense of security and comfort for customers when conducting transactions. Additionally, the principles underlying the contractual relationship between banks and customers affect the level of customer trust, both when saving and borrowing funds from banks.

Historically, cash-service activities conducted outside bank premises were expressly addressed in Bank Indonesia Regulation Number 13/27/PBI/2011. Because that regulation is no longer in force, this study uses it only to trace the regulatory development of off-premises cash services and not as the primary basis for determining the current legal status of pick-up service transactions. The present normative assessment is instead mapped through the Banking Law, as amended, the P2SK framework, applicable consumer-protection rules, and the current OJK anti-fraud framework.

A normative mapping of the relevant legal regimes indicates that the problem should not be characterized as a complete regulatory void. Under *lex lata*, customer protection in pick-up service transactions can be constructed cumulatively from banking law, consumer-protection rules, anti-fraud obligations, contractual principles, prudential duties, and bank-governance requirements. The remaining issue is a service-specific normative gap: these general regimes do not expressly integrate the allocation of risk during off-premises cash custody, evidentiary standards for cash handover, verification duties, and a dedicated recovery pathway. As *lex ferenda*, this study therefore proposes more explicit service-specific standards that coordinate these existing protections without implying that customer protection is presently absent.

The formal relationship between customers and banks is reflected in forms completed by customers and approved by banks. These forms contain applications, orders, or authorizations addressed to banks. They are generally prepared by banks and contain provisions governing the transactions requested by customers. This means that customers who complete application,

order, or authorization forms for banking services are essentially acting on the basis of their trust in banks. Customers or consumers manifest this trust by submitting application forms and authorizations to the bank. One of the banking activities carried out to provide convenience for customers in conducting transactions, particularly deposits and fund withdrawals, is the provision of pick-up service cash services. In the implementation of these cash services, various problems continue to arise in practice. This condition encourages researchers to examine legal certainty for customers concerning issues arising from cash-service activities, particularly customer fund collection through pick-up service, considering that customers have entrusted their funds to the bank. Criminal cases involving pick-up service transactions represent an evolution in banking crime, requiring banking institutions to remain vigilant against emerging modes of banking crime involving not only internal banking personnel but also external parties.

Prior studies address important aspects of this problem but remain fragmented. Putera (2019) discuss prudential banking principles in pick-up service transactions; Halim et al. (2022) examine criminal conduct by bank employees involving embezzlement; and Purnomo et al. (2026) analyze corporate accountability for employee negligence. These studies respectively illuminate service prudence, individual criminal conduct, and institutional responsibility. Within the literature reviewed in this study, however, no prior work was identified that integrates an element-by-element distinction between banking offenses and general offenses with a protection model specifically structured around the operational chain of pick-up service. The present study addresses that gap by linking legal classification, operational vulnerability points, and a four-layer customer-protection model comprising contractual, operational, institutional, and recovery protection.

## METHOD

This study used normative legal research as its primary research design. The legal analysis examined statutory materials and doctrinal concepts governing banking, consumer protection, anti-fraud controls, contractual relations, and bank accountability. The statutory approach was used to map applicable legal norms and their amendments, while the conceptual approach was used to distinguish banking offenses, general criminal offenses, internal fraud governance categories, and forms of bank responsibility. No decided court cases were treated as a formal case-approach dataset; accordingly, the study did not claim to employ a separate case approach. Legal materials were collected through a literature review and subsequently identified, classified, and interpreted systematically (Atmadja, 2018; Firmanto, 2024; Rosidi, 2026).

Empirical material was supplementary and did not convert the research design into socio-legal or empirical legal research. The manuscript reported one supporting informant, a Supervisor at Bank Rakyat Indonesia, Mahendradata Denpasar Unit, Bali, whose supervisory role provided operational context regarding pick-up service stages and control vulnerabilities. The interview record identified the informant and her professional role but did not state a date. The interview content was summarized thematically according to operational stage and was used only to contextualize the normative analysis; legal classifications and the proposed protection model were derived from the legal materials. The overall analysis was descriptive-qualitative, combining systematic legal interpretation with contextual comparison of the identified operational risks.

## RESULTS AND DISCUSSION

### Results

#### **Irregularities in Pick-Up Service Cash Transactions as a Form of Crime Regulated by Banking Legal Norms**

Pick-up service is an off-premises banking cash service in which bank personnel visit customers to receive cash or facilitate transactions without requiring customers to come to a bank office. Its practical value lies in convenience and accessibility, particularly for customers handling recurring or substantial cash deposits (Mukhtar, 2016). Because the service transfers physical control of cash to a bank officer before the funds are credited to the customer's account, it also creates distinct chain-of-custody and evidentiary risks that must be assessed in light of banking and consumer-protection duties.

Analytically, this section separates three levels: the supporting interview is used to identify operational vulnerability points; those points are then mapped against legal norms through the authors' normative analysis; and the Layered Customer Protection Model is presented later as a normative proposal. Unless expressly attributed to the interview, the legal classifications in this section represent the authors' legal interpretation rather than statements made by the informant.

This service provides benefits in the form of efficiency, operational security, and convenience for customers making cash deposits of certain amounts or at certain frequencies. However, service models conducted outside the bank office also create several points of risk, primarily because there is a time gap and multiple stages between the customer's handover of cash, the officer's physical possession of the money, the recording of the transaction, and the crediting of the funds to the customer's account.

Conceptually, the relationship between banks and depositing customers is based on a fiduciary relationship, commonly referred to as a fiduciary relation. Banks primarily operate with public funds deposited with them on the basis of trust, so every bank needs to continuously maintain its soundness by preserving public trust in the bank (Saputra, 2025). In the context of pick-up service, this trust is manifested through the granting of authority to bank officers to receive and carry customer funds. Therefore, abuse of authority by officers cannot be viewed merely as individual behavior but must also be analyzed as a potential failure of the bank's internal control system.

Pick-up service cash services are essentially a banking facility that provides convenience for customers to hand over cash to bank officers at an agreed location without having to come directly to a bank office. Although this service provides efficiency and practical benefits, there are several vulnerable points at which deviations may occur, whether due to procedural weaknesses, abuse of authority by employees, or failures in the bank's internal control system.

The eight vulnerability points below constitute an analytical synthesis rather than a verbatim interview transcript. The supporting interview with a supervisor from Bank Rakyat Indonesia provides an operational description of the pick-up service process. The authors subsequently categorize these descriptions into distinct stages and interpret their legal significance by comparing the interview findings with relevant legal materials and literature on banking controls. The points therefore identify contextual operational risks; they do not, by themselves, establish criminal or institutional liability.

### **1. Pick-Up Scheduling**

The first stage with potential for deviation is the scheduling of cash pick-ups. Under normal implementation, pick-ups should be conducted based on customer requests or approval, according to a predetermined schedule, and by officers officially appointed by the bank. The schedule should be verifiable through the bank's official communication channels. Deviations may occur if pick-ups are conducted outside the scheduled time, without official confirmation, or without a valid assignment letter or other evidence of authorization. This condition allows unauthorized individuals to pose as bank officers and request customers to hand over money on the pretext of making a deposit. Legally, this condition relates to negligence in the verification process and weaknesses in the bank's standard operating procedures. If the bank does not provide adequate verification mechanisms, such as official notifications, assignment codes, or confirmation through bank channels, these weaknesses may be assessed as failures by the bank to apply the prudential principle and maintain adequate internal controls.

### **2. Officer Identification**

The next stage is the identification of the officer conducting the pick-up. Officer identity is a crucial element because customers hand over funds based on the belief that the individual is acting for and on behalf of the bank (Putera, 2019). Deviations may include the use of fake identification cards, unauthorized uniforms, expired assignment letters, the use of another employee's identity, or assignments that have actually been revoked. The *modus operandi* may also involve former employees who remain known to customers or active employees acting outside their authority. The risk to customers is fraud and unauthorized appropriation of funds. Customers are in a vulnerable position because they generally do not have direct access to

information concerning the officer's employment status, scope of authority, or the validity of the officer's assignment letter.

### **3. Cash Handover and Counting**

The cash-handover stage is the most direct point in the transfer of physical control of funds from the customer to the bank officer. At this stage, counting should be conducted openly, the amount should be verified, and the recording should be witnessed or confirmed by the customer (Arens et al., 2024). Deviations may occur if the amount of money received differs from the amount recorded in the receipt document. For example, the customer hands over Rp100,000,000.00, but the officer records only Rp90,000,000.00. This discrepancy may occur because the counting is conducted unilaterally, documents are completed after the officer leaves the location, or the customer does not receive a copy clearly stating the amount received. The resulting risk is the reduction or loss of part of the customer's funds. The difficulty of proving the actual amount handed over increases when there are no witnesses, recordings, valid documents, or electronic evidence establishing the amount of money actually delivered.

### **4. Issuance of a Receipt**

Receipts have an important evidentiary function because they establish that funds have been handed over by the customer and received by the bank officer. A receipt should contain the identities of the parties, the date and time of receipt, the amount of money, the transaction number, and the officer's signature or other form of authentication. Deviations may occur if the officer provides an unofficial receipt, uses blank forms, creates a false receipt, or issues evidence that does not contain complete information. In some practices, officers may provide only handwritten notes or short messages that are not integrated with the bank's system. The risk to customers is a weakened evidentiary position when the funds do not enter the account. The bank may contend that the document is not an official document, was not recorded in the system, or was issued by an employee acting outside the prescribed procedure.

### **5. Transportation and Temporary Custody of Money**

After receipt, the cash remains in the officer's physical custody until delivery to the bank or an authorized processing point. This interval creates chain-of-custody risks: funds may be delayed, partially appropriated, used to cover earlier shortages, lost, or otherwise fail to reach the customer's account. The legal significance of any resulting loss depends on the applicable service procedure, evidence of handover, scope of the officer's authority, and allocation of risk and responsibility under the relevant legal relationship.

### **6. Crediting Funds to Customer Accounts**

The crediting stage is the process of entering the deposit amount into the customer's account. At this stage, conformity among the amount of money received, the receipt documents, and the account balance must be ensured. Deviations may include delayed crediting, recording only part of the funds, crediting the funds to a different account, or failure to credit the funds at all (Djoni & Rachmadi, 2012). Manipulation may also be carried out by making transactions appear successful through false transfer evidence or fabricated confirmations. The risk to customers is that the account balance does not increase even though the money has been physically handed over. This condition can disrupt customers' business activities, particularly when the funds are needed to pay obligations, complete trade transactions, or meet specific deadlines.

### **7. Reconciliation and Detection of Data Discrepancies**

Reconciliation is the process of matching receipt documents, money received, system records, and customer account balances. This stage serves as a control mechanism for detecting discrepancies or noncompliant transactions. Deviations become more difficult to detect if the bank does not conduct daily reconciliation, does not have an automated warning system, or allows one employee to control the entire process from receipt through account crediting. In such circumstances, discrepancies in data may be concealed or allowed to persist for an extended period. The risk to customers is repeated and escalating losses. A single manipulation scheme may affect several customers because of the absence of early detection. In some cases, losses may be discovered only after the perpetrator has left the bank, fled, or become unable to cover the resulting shortage of funds.

## 8. Complaint Handling and Denial of Responsibility

The final vulnerable point arises after the customer discovers that the funds have not been credited or that a transaction discrepancy exists. At this stage, the customer submits a complaint and requests clarification and recovery of the loss. Problems may occur when the bank refuses to assume responsibility on the grounds that the act was a personal action by the employee, was conducted outside the prescribed procedure, or was not recorded in the bank's system. Denial may also be based on the assertion that the customer was negligent in checking the officer's identity or accepting an unofficial receipt (Fuady, 2005). The resulting risk is that the burden of the loss is shifted to the customer, even though the customer handed over funds to a person reasonably believed to be an official bank officer. The customer's position becomes increasingly weak because the bank controls documents, transaction systems, employment data, communication records, and internal investigation results.

The operational vulnerabilities identified above are contextual findings and do not automatically determine criminal qualification. Legal classification requires a separate element-by-element assessment of the actor, mental element, conduct, object, means used, and nexus with the bank's business activities. The Banking Law, in its consolidated form following subsequent amendments, including Law Number 4 of 2023 as amended by Law Number 4 of 2026, provides the primary basis for assessing banking-specific manipulation of records and documents, while other conduct must be mapped to the applicable general criminal-law provisions. Accordingly, the same incident may generate different legal consequences depending on which elements are proven.

Not every loss of money in *pick-up service* automatically constitutes a banking crime. The legal qualification is determined based on the perpetrator, *modus operandi*, object of the act, means used, and relationship between the act and the bank's business activities, as analyzed below.

### **Banking Crime**

For a banking-specific offense, the analysis uses Article 49 of the Banking Law in its consolidated form after the relevant amendments, including Law Number 4 of 2023 as amended by Law Number 4 of 2026. The relevant analytical elements are: (1) a legally specified banking subject; (2) intentional conduct; (3) a false, omitted, altered, obscured, concealed, deleted, or eliminated record or document within bank bookkeeping, reporting, or business activities; and (4) a sufficient nexus to banking business activities. Applied to *pick-up service*, merely taking customer cash is not enough. The banking-offense classification becomes relevant when, for example, an authorized banking actor intentionally records a lower deposit amount, suppresses a receipt, alters transaction data, or creates a false bank record so that the bank's official administration no longer reflects the actual handover. Where these elements are not established, the conduct must be assessed under other applicable offenses or liability regimes.

This norm shows that the object of legal protection is not merely the customer's money but also the administrative integrity and information systems of banking (Halim et al., 2022). Therefore, the principal element of a banking crime lies in the manipulation of the bank's administrative mechanisms in a manner that causes transaction data to no longer reflect the actual state of affairs.

### **General Crimes Committed in Banking Activities**

General criminal-law classification applies when the conduct does not depend on manipulation of the bank's official records or reporting system. For embezzlement-type conduct, the relevant elements are lawful initial possession or control of the customer's funds arising from the entrusted service, followed by intentional and unlawful appropriation of those funds as if they belonged to the perpetrator. This corresponds to a situation in which an authorized officer validly receives cash and subsequently diverts it before the funds are credited to the customer's account. For fraud-type conduct, the decisive elements are deceit, false capacity, or misrepresentation used from the outset to induce the customer to surrender funds, as may occur through a false identity, fabricated assignment letter, or other deceptive representation. These classifications are distinct from a banking-record offense and must be matched to the general criminal-law provisions in force when the conduct is adjudicated.

### ***Occupational Fraud or Internal Fraud***

Occupational fraud or internal fraud is used here as a governance and risk-management classification, not as the name of an independent criminal offense. It describes misconduct by insiders who exploit their position, authority, access, or control weaknesses to obtain an improper benefit. The criminal character of the underlying act must still be established by mapping the conduct to the elements of the applicable banking-specific or general criminal offense.

This qualification obtains its legal basis in POJK Number 12 of 2024 concerning the Implementation of Anti-Fraud Strategies for Financial Services Institutions, which requires every financial services institution to implement an anti-fraud strategy through four pillars, namely: 1) prevention; 2) detection; 3) investigation, reporting, and sanctions; 4) monitoring, evaluation, and follow-up.

Within this governance framework, appropriation of customer funds, falsification of receipts, manipulation of transaction records, and concealment of documents are fraud-risk events that activate prevention, detection, investigation, reporting, sanction, and follow-up duties. Their classification as internal fraud does not itself establish criminal liability; criminal liability must be proven separately under the substantive offense that corresponds to the conduct.

### ***Violation of the Prudential Principle and Bank Governance***

The final qualification is not oriented toward the criminal liability of the perpetrator but toward the institutional accountability of the bank. Article 2 of the Banking Law affirms that bank business activities must be conducted based on economic democracy using the prudential principle (Purnomo et al., 2026). This principle does not apply only to credit provision but encompasses all operational activities of the bank, including cash services through *pick-up service*.

Violations of the prudential principle may occur if the bank does not implement adequate procedures, such as segregation of duties, dual control, officer identity verification, daily reconciliation, electronic documentation, transaction monitoring, and early detection systems for deviations.

A weakness in internal control does not automatically establish bank liability, and the applicable responsibility regimes must be distinguished. Employee criminal liability depends on proof of the elements and culpability of the relevant offense. Bank administrative responsibility concerns compliance with prudential, consumer-protection, anti-fraud, risk-management, and supervisory obligations. Civil liability and customer compensation depend on the applicable contractual or civil-liability basis, causation, loss, evidence of handover, and the relationship between the employee's conduct and the bank's service. Corporate-governance responsibility concerns failures in oversight, control design, monitoring, or remediation. Accordingly, an internal-control weakness is evidence relevant to institutional attribution, but it is not a substitute for proving the requirements of each distinct liability regime (Purnomo et al., 2026; Zainal Asikin, 2015).

Based on this analysis, the construction of pick-up service manipulation crime can be formulated as a crime committed intentionally by bank employees, officers working for the bank's benefit, or other parties taking advantage of the bank's identity and facilities by abusing authority, appropriating funds without legal right, providing false information, or manipulating documents and transaction records, resulting in customer funds not being received or not being credited according to the actual state of affairs. This qualification shows that the objects of protection in *pick-up service* cases consist of three layers: customer assets, customer trust in the bank, and the integrity of the banking system.

### **Protection for Customers Against the Risk of Losses Due to Bank Employee Manipulation in Bank Pick-Up Service Transactions**

Customer protection must be built through a combination of preventive and repressive protection. Legal protection is inadequate if it is provided only after losses occur. Banks must first prevent opportunities for manipulation from arising and ensure that customers obtain reliable transaction evidence.

### **a. Preventive Legal Protection**

Preventive protection is carried out before losses occur (Kusuma, 2019). The preventive model resulting from this research consists of the following elements:

First, regulation of services in written agreements. The *pick-up service* agreement should at least include the identity and authority of the parties, the schedule and location of pick-ups, authorized officers, cash-counting procedures, receipt format, crediting time limit, confirmation mechanism, risk allocation, emergency procedures, complaint mechanisms, and compensation obligations. Clauses that entirely shift bank responsibility to customers when losses occur due to employee actions or bank systems should be avoided. POJK Number 22 of 2023 regulates consumer protection in the financial services sector, including obligations concerning data security and restrictions on the use of exculpatory standard clauses.

Second, layered officer verification. Customers must be able to verify an officer's identity through official bank channels. Verification should not depend solely on uniforms, identification cards, or personal recognition but should be supplemented with assignment codes, notifications through applications or official messages, and confirmation with the bank office.

Third, use of traceable receipts. Every cash receipt must generate evidence containing the time, place, amount of money, officer and customer identities, assignment number, and a verifiable transaction code. Transaction evidence should preferably be generated electronically and directly connected to the bank's system so that it does not depend on manual documents that can be easily altered.

Fourth, application of the dual-control principle. Counting, receiving, transporting, and recording money in certain amounts should not be fully controlled by a single officer. Segregation of functions reduces opportunities for employees to manipulate transactions without detection.

Fifth, automatic reconciliation and real-time notification. After the money is received, the customer should receive an official notification. If the funds have not been credited to the account within the specified time limit, the system should generate alerts for the customer, relevant operational units, and internal-control functions.

Sixth, implementation of anti-fraud strategies. Banks need to conduct risk mapping, background checks on officers, job rotation, mandatory leave, transaction-pattern monitoring, violation-reporting channels, independent investigations, and periodic evaluations. This is consistent with POJK Number 12 of 2024, which requires financial services institutions to implement anti-fraud strategies and fraud-detection systems.

Seventh, strengthening customer literacy. Customers need to be provided with information that money should be handed over only to officers whose identities have been verified, receipts must be checked, and account balances must be confirmed within the specified time limit.

### **b. Repressive Legal Protection**

Repressive protection is provided after an alleged manipulation or loss has occurred (Gunawan, 2024). Drawing on the operational risks identified through the supporting interview and the applicable legal-protection framework, the following measures are formulated as components of the study's normative protection model: 1) prompt receipt and examination of customer complaints; 2) transaction blocking and evidence preservation; 3) independent internal investigation; 4) recovery or replacement of customer losses; 5) imposition of employment and administrative sanctions; 6) reporting of criminal acts to the competent authorities; 7) dispute resolution through the Financial Services Sector Alternative Dispute Resolution Institution or a court; 8) submission of fraud-incident reports to OJK in accordance with applicable regulations.

The P2SK Law strengthens the framework for consumer protection and law enforcement in the financial services sector. Law Number 4 of 2023 has been amended by Law Number 4 of 2026, which came into effect on June 17, 2026. Accordingly, the legal basis in the final report should be stated as Law Number 4 of 2023 as amended by Law Number 4 of 2026. Furthermore, POJK Number 38 of 2025 regulates OJK's authority to file lawsuits for consumer protection in the financial services sector. This regulation revokes and replaces certain provisions concerning lawsuits under POJK Number 22 of 2023.

### **c. Bank Accountability for Employee Actions**

The research results indicate that banks cannot simply absolve themselves of responsibility by stating that manipulation was an employee's personal act. The determination of responsibility must consider: 1) whether the officer is an employee or a party appointed by the bank; 2) whether the act was performed in the execution of or in connection with the officer's work; 3) whether the customer reasonably believed that the officer was acting for the bank; 4) whether the bank provided the means, identity, documents, or access used by the perpetrator; 5) whether there were weaknesses in supervision and internal control; 6) whether the bank fulfilled its prudential and consumer-protection obligations.

When a customer hands over funds to an authorized officer at the agreed time and place and possesses evidence that can reasonably be attributed to the bank's service, the transaction should be assessed as part of the bank-customer service relationship rather than automatically treated as a purely personal act of the employee. Under *lex lata*, any obligation to compensate must be determined on the basis of the applicable contract, consumer-protection rules, civil-liability principles, banking duties, and supervisory requirements. Under the protection model proposed in this study, prompt recovery after internal verification is a normative recommendation (*lex ferenda*), not an assertion of an unconditional statutory duty that applies before the legal basis and facts have been established.

Under the proposed model, customer recovery does not prevent the bank from pursuing employment sanctions, recourse, compensation claims, or criminal reporting against the responsible employee when the applicable legal requirements are met. This sequencing is intended to avoid automatically shifting internal organizational risk to a customer who lacks control over bank personnel, while preserving the need to determine liability under the applicable legal regime.

Based on the normative analysis, this study proposes a Layered Customer Protection Model in Pick-Up Service Cash Services as a *lex ferenda* and governance framework. Unless a component is independently required by applicable law, the measures below are presented as normative recommendations rather than as a statement that every component is already an unconditional legal duty:

#### **First Layer: Contractual Protection**

The service agreement should clearly regulate procedures, the timing and allocation of risk transfer, the scope of bank responsibility, transaction-evidence standards, complaint mechanisms, and pathways for loss recovery.

#### **Second Layer: Operational Protection**

Under the proposed operational layer, banks should implement officer verification, dual control, electronic receipts, real-time notification, crediting time limits, automatic reconciliation, and traceable monitoring from cash receipt to account crediting.

#### **Third Layer: Institutional Protection**

Under the proposed institutional layer, banks should maintain effective anti-fraud functions, violation-reporting channels, risk-based audits, appropriate employee rotation, independent investigation procedures, and periodic evaluation of officers and customers using the service.

#### **Fourth Layer: Recovery Protection**

Under the proposed recovery layer, banks should provide an accessible complaint procedure, rapid securing of funds and evidence, objective complaint assessment, legally grounded compensation or recovery pathways, and access to LAPS SJK, OJK, law-enforcement authorities, and courts, as applicable.

Based on the above explanation, this model can be summarized in the following flow: prevention → verification → receipt and recording → confirmation → detection → complaint → investigation → recovery → law enforcement → system evaluation. This model shows that customer protection is not solely the responsibility of the service unit. Protection must involve operational functions, compliance, risk management, internal audit, human resources, information technology, legal units, and the bank's board of directors.

## CONCLUSION

Irregularities in pick-up service cash transactions must be classified by matching the proven conduct to the elements of the relevant legal regime. Banking-specific criminal qualification is appropriate when a legally specified banking actor intentionally manipulates records, bookkeeping, documents, reporting, or transaction data within the bank's business activities. Where an authorized officer initially receives funds lawfully and subsequently appropriates them unlawfully, the conduct should be assessed under the applicable general criminal-law rules concerning appropriation or embezzlement; where deceit is used from the outset to induce the surrender of funds, fraud-type provisions become relevant. Internal fraud is a governance and risk classification and does not replace this substantive criminal-law analysis. Bank administrative, civil, and governance responsibility must likewise be assessed separately according to their respective legal requirements.

Customer protection against losses due to bank employee manipulation in pick-up service transactions must be provided preventively and repressively. Preventive protection is carried out through clear agreements, officer verification, dual control, electronic receipts, automatic reconciliation, real-time notification, and implementation of anti-fraud strategies. Repressive protection is manifested through complaint examination, evidence preservation, independent investigation, loss compensation, dispute resolution, and law enforcement. Banks cannot simply absolve themselves of responsibility on the grounds that an employee acted personally if the act was carried out in the employment relationship, used bank facilities, or was made possible by weaknesses in internal control.

The principal normative contribution of this study is the Layered Customer Protection Model, consisting of four mutually connected layers: contractual protection clarifies service procedures, evidence, risk allocation, and complaint rights; operational protection strengthens verification, dual control, electronic evidence, notification, and reconciliation; institutional protection integrates anti-fraud, audit, oversight, and investigation functions; and recovery protection structures complaint handling, evidence preservation, legally grounded compensation pathways, dispute resolution, and law enforcement. Because the model is proposed normatively and has not yet been empirically tested across multiple banks, its effectiveness should be evaluated through future implementation and broader empirical research.

## ACKNOWLEDGEMENT

The authors would like to express their gratitude to Universitas Warmadewa for providing academic support and research facilities during the completion of this study. The authors also acknowledge the contribution of all parties who provided valuable insights and assistance in supporting the development of this research.

## AUTHOR CONTRIBUTION STATEMENT

Author contributions are as follows: I Made Aditya Mantara Putra contributed to the conceptualization, research design, legal analysis, data interpretation, and manuscript preparation. Johannes Ibrahim Kosasih contributed to the theoretical framework, legal review, critical evaluation, and refinement of the manuscript. I Putu Suwantara contributed to methodological review, validation of the analysis, and manuscript improvement. All authors have read and approved the final version of the manuscript.

## REFERENCES

- Anugrahita, R., & Baidhowi. (2025). Prinsip Kehati-hatian Dalam Perbankan Dan Akad Murabahah. *Jurnal Akademik Ekonomi Dan Manajemen*, 2(2).
- Arens, Randal J. Elder, Mark S. Beasley, & Chris E. Hogan. (2024). Auditing And Assurance Services. In *Pearson Education Limited*.
- Atmadja, I. N. P. B. , and I. N. P. B. B. (2018). *Teori-teori hukum*.
- Azlina, N., Maesarach, R. M., & Said, M. (2022). Islamic Economic Methodology Aproach to Achieve Economic Equity: Epistemological Study. *BASKARA: Journal of Business and Entrepreneurship*, 4(2). <https://doi.org/10.54268/baskara.v4i2.12189>

- Borg, E., & Hooker, B. (2019). Epistemic Virtues Versus Ethical Values in the Financial Services Sector. *Journal of Business Ethics*, 155(1). <https://doi.org/10.1007/s10551-017-3547-x>
- Djoni, G. S., & Rachmadi, U. (2012). Hukum Perbankan. *Sinar Grafika, Jakarta*.
- Firmanto, T. (2024). *Metodologi penelitian hukum: Panduan komprehensif penulisan ilmiah bidang hukum*. PT. Sonpedia Publishing Indonesia.
- Fuady, M. (2005). *Perbuatan melawan hukum (Pendekatan kontemporer)*.
- Gunawan, I. (2024). Upaya Preventif dan Represif dalam Penanggulangan Kebocoran Data Pada Penyelenggaraan Pinjaman Online. *Officium Notarium*, 4(1). <https://doi.org/10.20885/jon.vol4.iss1.art3>
- Halim, G., Zarzani, T. R., & Aspan, H. (2022). Analisis Yuridis Terhadap Pegawai Bank Yang Melakukan Tindak Pidana Penggelapan Dalam Jabatan Menurut Undang-Undang Nomor 10 Tahun 1998 Tentang Perbankan. *Jurnal Rectum*, 4(2).
- Harahap, N. and N. H. (2025). Beyond the Liberty-Justice Dichotomy: A Constitutional-Maqasid Synthesis for Indonesia's Plural Legal Order . *KASTA: Jurnal Ilmu Sosial, Agama, Budaya Dan Terapan*, 5(3), 980–1003.
- Kusuma, M. J. and M. S. (2019). *Hukum perlindungan nasabah bank: Upaya hukum melindungi nasabah bank terhadap tindak kejahatan ITE di bidang perbankan*. Nusamedia.
- Muktar, B. (2016). *Bank dan lembaga keuangan lain*. Prenada Media.
- Ningsih, S. (2021). Dampak Dana Pihak Ketiga Bank Konvensional Dan Bank Syariah Serta Pertumbuhan Ekonomi Di Indonesia. In *Paper Knowledge . Toward a Media History of Documents* (Vol. 3, Number April).
- Purnomo, P., Kadi Sukarna, Muhammad Junaidi, Kukuh Sudarmanto, & Miftah Arifin. (2026). Pertanggungjawaban Korporasi atas Kelalaian Karyawan Bank di Indonesia. *JURNAL USM LAW REVIEW*, 9(3). <https://doi.org/10.26623/julr.v9i3.12709>
- Putera, A. P. (2019). Hukum Perbankan : Analisis Mengenai Prinsip, Produk, Risiko Dan Manajemen Risiko Dalam Perbankan. In *Sustainability (Switzerland)* (Vol. 11, Number 1).
- Rasyid, F. M. (2026). *Ekonomi digital: Konsep, transformasi, inovasi dan tantangan*. Star Digital Publishing.
- Rosidi, A. (2026). *Metodologi Penelitian Hukum: Teori, Paradigma, Dan Praktik Kontemporer*. Cv. Edu Akademi.
- Saputra, A. (2025). Menjaga Kepercayaan Dalam Transaksi Keuangan: Pengaturan Prinsip Kepercayaan di Bank. *Media Hukum Indonesia (MHI)*, 2(5).
- Taklima, M., Sulistiyono, A., & Syamsudin, M. (2023). CONSUMER PROTECTION AS AN INSTRUMENT FOR FULFILLING HUMAN RIGHTS IN THE ECONOMIC SECTOR AND ITS CONSTITUTIONALIZING EFFORTS IN THE 1945 CONSTITUTION. *Jurisdictie: Jurnal Hukum Dan Syariah*, 14(1). <https://doi.org/10.18860/j.v14i1.20844>
- Zainal Asikin. (2015). *Pengantar hukum perbankan Indonesia*.