AKASA
PRUDENTIA
JURNAL HUKUM PERDATA
Volume 1 No 1 June 2026
P-ISSN: 0000-000, E-ISSN: 0000-0000
https://doi.org/10.70565/prudentia.v1i1.85

Bank Liability and Customer Protection in Digital Transactions: A Comparative Study of Indonesian and French Private Law

Bambang Fitrianto[1], Gueorgui Armianov[2]

[1] *Faculty of Law, Universitas Pembangunan Panca Budi, Country. E-mail: bambangfitrianto@dosen.pancabudi.ac.id*
[2] *Department of Europe, National Institute for Oriental Languages and Civilizations, Paris, France. E-mail: gueorgui.armianov@inalco.fr*

Keywords: Bank Liability; Customer Protection; Digital Transactions; Private Law; Risk Allocation.

Abstract: The rapid expansion of digital banking and electronic payment services has transformed the contractual relationship between banks and customers while simultaneously increasing exposure to unauthorized transactions, digital fraud, and other technology-related financial losses. These developments raise fundamental questions concerning the allocation of liability between banks and customers, particularly where conventional principles of contractual fault provide insufficient guidance for determining responsibility. This article aims to compare the legal frameworks governing bank liability and customer protection in digital transactions under Indonesian and French private law and to identify principles that may strengthen the Indonesian framework. The research employs a normative juridical method using statutory, conceptual, and comparative approaches, based on legislation, judicial decisions, regulatory instruments, and relevant legal scholarship from both jurisdictions. The findings demonstrate that both systems recognize bank obligations to ensure transaction security and protect customers, but differ in the construction of liability, allocation of risk, burden of proof, and legal consequences of unauthorized transactions. French law provides a more structured framework for allocating losses between payment service providers and customers. The article proposes a clearer risk-allocation model for Indonesian banking law based on control over transaction risks, compliance obligations, and proportional customer responsibility.

1. Introduction

The rapid transformation of banking services through digital technologies has fundamentally changed the manner in which financial transactions are initiated, authenticated, processed, and completed.[1] Mobile banking, internet banking, electronic transfers, digital payment instruments, and increasingly interconnected financial platforms have enabled customers to conduct transactions with greater speed and accessibility.[2] At the same time, digitalization has generated new forms of legal risk arising from unauthorized transfers, account takeovers, phishing, social engineering, identity theft, compromised authentication credentials, and other forms of digital financial fraud. These developments have complicated the traditional contractual relationship between banks and customers because financial losses may result not only from the conduct of either party but also from vulnerabilities involving technological systems and third-party interference.[3] Consequently, determining who should bear the financial consequences of a disputed digital transaction has become an increasingly important issue in contemporary private and banking law.

Bank liability in digital transactions cannot be separated from the contractual relationship established between the bank and its customers. Traditionally, civil liability may arise from a failure to perform contractual obligations or from unlawful conduct causing damage. In digital banking, however, applying conventional fault-based principles becomes more complicated because the bank controls significant elements of the payment infrastructure, security mechanisms, authentication procedures, transaction monitoring systems, and records necessary to establish how a disputed transaction occurred.[4] Customers, by contrast, generally possess substantially less information concerning the technical processes underlying the transaction. This asymmetry creates difficulties in determining fault, causation, the burden of proof, and the appropriate allocation of financial losses when a customer claims that a transaction was conducted without valid authorization.

The problem is particularly significant in Indonesia, where the expansion of digital financial services has increased the importance of effective customer protection alongside banking innovation.[5] Indonesian private law provides general foundations for contractual responsibility and unlawful acts, while banking, payment-

---

[1] S. Ahmed, "The Fatal Flaw of Glocal 'Solutions' to Illicit Financial Flows," *Journal of Economic Criminology* 7 (2025), Scopus, https://doi.org/10.1016/j.jeconc.2024.100116.

[2] H. Abbassi, S. El Mendili, and Y. Gahi, "A Conceptual Real-Time and Privacy-Preserving Architecture for Banking Fraud Detection," in *Int. Conf. Optim. Appl., ICOA - Proc.*, ed. Hachimi H. and EL Mokhi C. (Institute of Electrical and Electronics Engineers Inc., 2025), Scopus, https://doi.org/10.1109/ICOA66896.2025.11236932.

[3] H. Chitimira, E. Torerai, and V. L. M. Jana, "Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector," *Potchefstroom Electronic Law Journal* 27 (2024): 1–30, Scopus, https://doi.org/10.17159/1727-3781/2024/v27i0a18024.

[4] P. Caldarone, "Banking phishing: main defense tools and responsibility profile," *Rivista Italiana di Informatica e Diritto* 5, no. 2 (2023), Scopus, https://doi.org/10.32091/RIID0116.

[5] N. Garg and K. Gupta, "Data Privacy in Online Banking Using Blowfish Algorithm: A Review," *Progressive Computational Intelligence, Information Technology and Networking*, 2025, 888–91, Scopus, https://doi.org/10.1201/9781003650010-145.

system, personal-data, and consumer-protection regulations impose additional obligations upon financial service providers. Nevertheless, the interaction between these different legal regimes may create difficulties when determining the precise boundary between the responsibility of a bank and that of a customer. A transaction recorded as having passed authentication procedures, for example, does not necessarily resolve whether the customer genuinely authorized it, whether adequate security measures were implemented, or whether circumstances surrounding the transaction should have triggered preventive measures by the bank. The legal question therefore extends beyond identifying the person who technically initiated a transaction and concerns how risks should be allocated between parties with substantially different capacities to prevent, detect, and prove digital financial misconduct.

France provides a relevant comparative framework for examining this problem because its private and financial law has developed more specific rules governing payment transactions and the allocation of losses arising from unauthorized payments. French law operates within the broader European payment-services framework and establishes legal consequences concerning authorization, notification of disputed transactions, reimbursement, authentication, and circumstances in which customer fraud or gross negligence may affect the allocation of losses.[6] This approach provides an important comparative perspective for Indonesia because it demonstrates how general principles of private law can interact with a specialized statutory framework governing digital payment relationships. The comparison is not intended to suggest the direct transplantation of French rules into Indonesian law, but rather to identify legal principles and regulatory techniques that may provide useful lessons for developing a more coherent allocation of responsibility.

Existing scholarship on digital banking has extensively addressed consumer protection, cybersecurity, electronic payments, financial technology, and bank responsibility for unauthorized transactions. Other studies have examined banking liability primarily through contractual obligations, negligence, consumer-protection principles, or regulatory compliance.[7] Comparative studies concerning European payment law have similarly emphasized authentication standards, unauthorized payments, and the distribution of losses between payment service providers and users. Although these contributions have clarified important dimensions of digital financial protection, the literature remains comparatively fragmented between private-law liability and sector-specific banking regulation. In the Indonesian context in particular, greater attention is required to the relationship between contractual

[6] Z. Aladwan, "Legal Basis for the Fraud Exception in Letters of Credit under English Law," *Journal of Financial Crime* 30, no. 2 (2023): 594–600, Scopus, https://doi.org/10.1108/JFC-01-2020-0004.

[7] A. M. Abdalsatar and M. S. Mohammed, "The Impact of Artificial Intelligence Applications on Banking Operations: A Case Study on the Bank (HSBC) British for the Period (2016–2022)," in *Lect. Notes Networks Syst.*, 1697 LNNS, ed. Abdelgawad A., Hameed A.A., and Jamil A. (Springer Science and Business Media Deutschland GmbH, 2025), 570–81, Scopus, https://doi.org/10.1007/978-3-032-09562-6_42.

liability, regulatory duties, control over transaction infrastructure, customer conduct, causation, and the allocation of digital transaction risks.

A further gap concerns the tendency to conceptualize bank liability through a binary determination of whether the bank or the customer was at fault. Such an approach may be insufficient for digital transactions in which responsibility can involve several interconnected elements, including authentication systems, customer credentials, transaction monitoring, security warnings, customer behavior, and third-party fraud. The central legal issue should therefore not be limited to identifying formal fault after the loss has occurred. It should also consider which party was legally responsible for controlling the particular risk, which party possessed the greater capacity to prevent or detect the irregularity, whether the applicable standard of care was satisfied, and whether the customer materially contributed to the occurrence of the loss. From this perspective, digital banking liability requires a more structured model of risk allocation rather than an exclusively fault-oriented analysis.

The comparison between Indonesia and France is particularly useful in developing such a framework because the two jurisdictions provide different regulatory contexts while sharing fundamental private-law concerns regarding contractual obligations, good faith, fault, causation, and compensation for loss.[8] Comparative analysis can therefore reveal not merely differences in statutory provisions but also different approaches to determining authorization, evidentiary responsibility, reimbursement, and the consequences of customer conduct. The French experience can subsequently be evaluated according to Indonesia's own private-law principles and banking regulatory structure rather than treated as a model to be adopted without contextual adjustment. Such an approach allows comparative law to function as an analytical instrument for identifying weaknesses and possible directions of legal reform.

Against this background, this article addresses two interconnected problems: how bank liability and customer protection in digital transactions are constructed under Indonesian and French private law, and what principles derived from the comparison can contribute to strengthening the allocation of responsibility for digital transaction losses in Indonesia. Accordingly, the article aims to analyze the legal foundations and boundaries of bank liability in both jurisdictions, compare their approaches to unauthorized transactions, customer conduct, burden of proof, and allocation of financial risks, and formulate a more proportionate framework for customer protection under Indonesian law.

2. Method

This research employs a normative juridical method to examine bank liability and customer protection in digital transactions from a comparative private law

[8] Sanne Akerboom and Robin Kundis Craig, "How Law Structures Public Participation in Environmental Decision Making: A Comparative Law Approach," *Environmental Policy and Governance* 32, no. 3 (June 2022): 232–46, https://doi.org/10.1002/eet.1986.

perspective.[9] The analysis combines statutory, conceptual, case, and comparative approaches to identify the legal foundations governing the allocation of responsibility between banks and customers in Indonesia and France. The statutory approach examines relevant provisions of private law, banking law, payment-services regulation, consumer protection law, and other regulatory instruments governing digital financial transactions in both jurisdictions. The conceptual approach analyzes the doctrines of contractual liability, fault, duty of care, causation, authorization, burden of proof, customer responsibility, and risk allocation. The case approach examines relevant judicial decisions concerning unauthorized transactions and disputes involving bank responsibility to determine how these principles are interpreted and applied in practice.[10] The comparative approach is employed functionally rather than merely descriptively by comparing how Indonesian and French law address similar legal problems concerning transaction authorization, reimbursement, evidentiary responsibility, customer negligence, and the allocation of financial losses. The legal materials consist of primary and secondary sources. Primary legal materials include legislation, regulatory instruments, and judicial decisions from Indonesia and France, while secondary materials comprise peer-reviewed journal articles, books, legal commentaries, and other scholarly publications concerning banking liability, private law, digital payments, and customer protection. The collected materials are analyzed qualitatively through legal interpretation, doctrinal analysis, and comparative legal reasoning. Particular attention is given to identifying which party controls the relevant transaction risk, the capacity of each party to prevent or detect irregularities, compliance with applicable legal obligations, and the causal relationship between such conduct and customer losses. The results of the comparative analysis are subsequently used to formulate a control-based and risk-allocation framework for Indonesian law, while taking into account differences in the institutional and regulatory structures of the two jurisdictions rather than directly transplanting the French legal model.

3. Result and Discussion

3.1. Bank Liability and Customer Protection in Unauthorized Digital Transactions under Indonesian and French Private Law

The expansion of digital banking has fundamentally altered the legal structure of the relationship between banks and their customers.[11] Transactions that previously required direct interaction with bank personnel are increasingly initiated through mobile applications, internet banking, electronic payment instruments, and interconnected payment infrastructures. Although this transformation increases

[9] Elisabeth Nurhaini Butar-Butar, *Metode Penelitian Hukum, Langkah-Langkah Untuk Menemukan Kebenaran Dalam Ilmu Hukum* (Bandung: PT. Refika Aditama, 2018).
[10] II Amalia, "Kepastian Hukum Pengawasan Hakim Oleh Komisi Yudisial Terhadap Perkara Perdata Di Indonesia," *Perpustakaan Pascasarjana*, no. Query date: 2026-03-13 11:28:29 (2022).
[11] J. Phiri, T. Lavhengwa, and M. A. Segooa, "Online Banking Fraud Detection: A Comparative Study of Cases from South Africa and Spain," *South African Journal of Information Management* 26, no. 1 (2024), Scopus, https://doi.org/10.4102/sajim.v26i1.1763.

efficiency and accessibility, it also changes the distribution of transactional risks. Unauthorized transfers, phishing, credential theft, account takeover, social engineering, malware, and manipulation of authentication mechanisms may result in financial losses even where the bank's core information system has not technically failed. Consequently, the principal private-law question is no longer limited to whether a transaction was technologically processed correctly, but extends to whether it was legally authorized and, if not, which party should bear the resulting loss.

An unauthorized digital transaction should be distinguished from an unsuccessful, incorrectly executed, or economically disadvantageous transaction. The defining issue in an unauthorized transaction is the absence of legally valid consent attributable to the account holder. This distinction is crucial because the technical use of correct credentials does not necessarily establish genuine authorization.[12] A transaction may pass through a bank's authentication system using a valid password, personal identification number, one-time password, biometric credential, or registered device while the customer's consent has nevertheless been compromised through fraud or manipulation. Private law must therefore avoid equating successful technical authentication with conclusive proof of legal authorization. Authentication is evidence relevant to authorization, but the two concepts should not be treated as legally identical.

Under Indonesian law, the legal relationship between a bank and its customer is constructed through several overlapping regimes. At the private-law level, the relationship is fundamentally contractual. The bank undertakes obligations associated with maintaining the customer's account, executing valid payment instructions, protecting customer funds within the limits prescribed by law, and performing agreed banking services. General principles of contractual liability consequently remain relevant where the bank fails to perform its obligations properly. Depending upon the factual circumstances, liability may also arise through the general law of unlawful acts where conduct causing loss satisfies the applicable elements of civil responsibility.[13] Digital banking disputes, however, demonstrate that reliance solely on traditional contractual or tort categories may be insufficient because the content of the bank's obligations is increasingly determined by sector-specific banking, payment-system, cybersecurity, data-protection, and consumer-protection requirements.

Indonesia's regulatory framework has progressively strengthened this sector-specific dimension. Bank Indonesia Regulation No. 3 of 2023 on Bank Indonesia Consumer Protection identifies principles including fair treatment, transparency, responsible business conduct, protection of consumer assets against misuse,

[12] K. Upreti et al., "Detection of Banking Financial Frauds Using Hyper-Parameter Tuning of DL in Cloud Computing Environment," *International Journal of Cooperative Information Systems* 34, no. 1 (2025), Scopus, https://doi.org/10.1142/S0218843023500247.

[13] R. Agnia, SC Ar-Rusd, and ..., "Restrukturisasi Kredit Dalam Perspektif Hukum Perbankan: Dampak Terhadap Hubungan Kontraktual Antara Bank Dan Nasabah," *Journal of Legal, Political …*, no. Query date: 2026-06-07 18:14:46 (2025), http://scriptaintelektual.com/custodia/article/view/375.

protection of consumer data and information, effective complaint handling, and compliance enforcement.[14] Its scope includes payment-system providers and other parties under Bank Indonesia's regulatory and supervisory authority that deal directly with consumers. OJK Regulation No. 22 of 2023 similarly strengthened consumer and public protection in the financial-services sector in response, among other factors, to increasingly rapid digitalization and the growing complexity of financial products and services.[15] These developments demonstrate that bank–customer relationships can no longer be understood exclusively through the contractual terms accepted when an account or digital banking service is opened.

The regulatory development is significant from a private-law perspective because statutory and regulatory obligations influence the standard of conduct reasonably expected from banks. Banks occupy a structurally different position from ordinary contractual counterparties. They design or select the transaction infrastructure, establish authentication procedures, maintain transaction records, determine certain security protocols, and possess technical information that is ordinarily inaccessible to customers. This does not mean that banks should automatically bear every loss occurring through digital banking.[16] It does, however, justify a heightened examination of whether the bank complied with obligations falling within its sphere of control. A legally defensible liability model should therefore distinguish between risks generated or controllable within the banking infrastructure and risks primarily attributable to customer conduct or external fraud beyond what the bank could reasonably prevent.

The Indonesian payment-system framework is also undergoing substantial regulatory development. Bank Indonesia Regulation No. 10 of 2025 on the Payment System Industry applies to payment service providers, payment infrastructure providers, commercial banks, supporting providers, infrastructure participants, connected parties, and other relevant actors. Its regulatory scope expressly encompasses governance and risk management, information-technology infrastructure, market conduct, Bank Indonesia consumer protection, and payment-system data and information. This increasingly risk-oriented architecture is important for unauthorized transaction disputes because the legal assessment of liability cannot be isolated from the bank's responsibility to manage operational and technological risks associated with its payment services.

Nevertheless, the Indonesian framework still raises an important doctrinal question concerning the precise allocation of losses after an unauthorized digital

[14] D. Agustuti and A. Irawan, "Kajian Normatif Pertanggungjawaban Pidana Pengurus Bank Terkait Tindak Pidana Perbankan Dalam Proses Pemberian Kredit," *Indonesian Journal of Law and Justice*, no. Query date: 2026-06-07 18:14:46 (2024), http://kurniajurnal.com/index.php/ijlj/article/view/174.

[15] Abdurrakhman Alhakim and Sofia Sofia, "Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia," *Jurnal Komunitas Yustisia* 4, no. 2 (August 2021): 377–85, https://doi.org/10.23887/jatayu.v4i2.38089.

[16] S. Shajahan and A. R. Nair, "Jurisdictional Conundrum in Digital Banking Frauds: Reinvestigation of the Effectiveness of International Conventional Laws vs. Contemporary Approaches on Cyberspace," *Revista Brasileira de Alternative Dispute Resolution* 7, no. 13 (2025): 261–74, Scopus, https://doi.org/10.52028/rbadr.v7.i13.ART13.IN.

transaction has occurred. General private-law principles ordinarily require an assessment of breach or unlawful conduct, fault where relevant, loss, and causation. Sectoral regulation adds more specific standards of conduct, but disputes may still center on whether the bank or customer should ultimately bear the financial consequences. This becomes particularly difficult in social-engineering cases. A customer may technically perform an authentication step after being deceived by a third party, while the bank may argue that its system operated normally. Conversely, the customer may contend that the transaction was anomalous and should have triggered security controls. Such cases expose the limitations of resolving digital banking disputes through the binary proposition that either the bank's system failed or the customer was negligent.

The evidentiary dimension is equally important. In conventional civil litigation, the party asserting a right generally bears an evidentiary burden consistent with procedural law. Digital banking disputes, however, involve substantial information asymmetry. Banks generally control authentication logs, device information, timestamps, transaction histories, security alerts, risk assessments, and other technical records relevant to determining how a disputed transaction was executed.[17] Customers may possess little more than account statements, notifications, or communications associated with the fraud. A formally equal distribution of evidentiary responsibility may therefore produce substantively unequal outcomes when one party possesses most of the relevant technical evidence. Customer protection in digital banking accordingly requires attention not only to substantive liability but also to the allocation of evidentiary burdens.

French law offers a significantly more structured approach to this problem. The Code monétaire et financier establishes a specific liability regime for unauthorized payment transactions rather than leaving the matter entirely to general contractual liability.[18] Article L133-18 provides, subject to the statutory conditions, that when an unauthorized payment transaction is reported, the payer's payment service provider must reimburse the amount immediately after becoming aware or being informed of it and, in any event, no later than the end of the following business day, except where there are good reasons to suspect fraud by the payment-service user and those reasons are communicated in writing to the Banque de France.[19] The provision also requires restoration of the debited account to the position in which it would have been had the unauthorized transaction not occurred. The starting point is therefore

[17] Mochammad Syahrul Asy'ari, "Analisis Kelayakan Nasabah Menggunakan Prinsip 5C 1S Dalam Pembiayaan Pemilikan Rumah (PPR) (Studi Pada KB Bank Syariah KC Sidoarjo)," *Jurnal Ilmiah Ekonomi Dan Manajemen* 2, no. 11 (2024).

[18] M. Bujalski, "Could French Law Provide a Model for Regulation of the Enforcement of Security Rights in Digital Assets?," *Forum Prawnicze*, no. Query date: 2026-09-12 12:13:22 (2025), https://access.heinonline.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/frmpwn2025§ion=19.

[19] M. Combot, "Subsidiarity and Unjustified Enrichment: Perspective under French Law," *European Review of Private Law= Revue …*, no. Query date: 2026-09-12 12:13:22 (2026), https://search.proquest.com/openview/5299a4823434a5c9a932065b57c72945/1?pq-origsite=gscholar&cbl=7100263.

materially different from a system in which the customer must first establish the bank's negligence before obtaining restoration of the funds.[20]

This reimbursement principle does not amount to absolute bank liability. French law simultaneously allocates certain risks to the payer. Article L133-19 establishes differentiated consequences according to the circumstances surrounding the unauthorized transaction.[21] In cases involving loss or theft of a payment instrument, the payer may, under specified circumstances, bear losses occurring before notification within a statutory ceiling of EUR 50. More importantly, the payer bears losses resulting from fraudulent conduct or from intentional failure or gross negligence in complying with specified obligations concerning the payment instrument and security credentials. Conversely, absent customer fraud, the payer generally bears no financial consequence where an unauthorized transaction occurs without the payment service provider requiring the strong customer authentication prescribed by law. The French model therefore does not simply favor the customer; it establishes a differentiated statutory allocation of risk.[22]

The distinction between ordinary negligence and gross negligence is particularly significant. If every customer mistake were sufficient to transfer the entire loss to the customer, the protective purpose of the unauthorized-payment regime would be substantially weakened. Digital fraud frequently succeeds precisely because fraudsters manipulate human behavior rather than directly attacking banking infrastructure.[23] The legal system must therefore determine when customer conduct crosses the threshold from understandable vulnerability to conduct sufficiently serious to justify reallocating the financial loss. This approach recognizes customer responsibility while preventing banks from avoiding reimbursement merely by demonstrating that valid credentials were technically used.

The French evidentiary regime reinforces this protective structure. Article L133-23 of the Code monétaire et financier provides that where a payment-service user denies authorizing an executed transaction, the payment service provider must prove that the transaction was authenticated, properly recorded and accounted for, and unaffected by a technical or other deficiency.[24] More importantly, the recorded use of the payment instrument is not necessarily sufficient by itself to establish either that the payer authorized the transaction or that the payer intentionally or through

[20] AA Lytvynenko, "The Institute of Trade Secrets in English and French Law in the 19th and Early 20th Centuries: Doctrine and Jurisprudence," *International Comparative Jurisprudence*, no. Query date: 2026-09-12 12:13:22 (2024), https://www.ceeol.com/search/article-detail?id=1249603.

[21] MS Al Kattan, "The Use of Technology in Compulsory Enforcement: A Comparative Study in Emirati and French Law," *Digital Evidence and Procedural Law in the UAE*, no. Query date: 2026-09-12 12:13:22 (2026), https://www.igi-global.com/chapter/the-use-of-technology-in-compulsory-enforcement/406892.

[22] C. Pecnard and A. Jarlot, "Arbitration and Intellectual Property in French Law," *… Handbook on Intellectual Property Rights and …*, no. Query date: 2026-09-12 12:13:22 (2024), https://www.elgaronline.com/edcollchap/book/9781800378360/book-part-9781800378360-31.xml.

[23] David Debenham, "Big Data Analytics, Big Financial Institutions, and Big Money Fraud Litigation," *Westlaw, 32 Banking and Finance Law Review* 103 (2016).

[24] T. Gisclard, *Utility Models in French Law*, no. Query date: 2026-09-12 12:13:22 (n.d.).

gross negligence breached the relevant obligations. The provider must supply evidence capable of establishing fraud or gross negligence by the user. This provision directly addresses the information asymmetry inherent in digital payment disputes.

From a private-law perspective, this French approach is significant because it separates three questions that are sometimes conflated in digital banking disputes: authentication, authorization, and liability. Authentication asks whether the security mechanism recognized the credentials associated with the customer. Authorization concerns whether the customer legally consented to the transaction. Liability determines who must ultimately bear the loss when authorization is absent or disputed.[25] A transaction may therefore be authenticated without being legally authorized, and the fact that authentication occurred does not automatically determine the allocation of liability. This distinction provides a more sophisticated legal response to fraud involving stolen credentials or manipulation of customers.

The comparison consequently reveals an important structural difference between Indonesia and France. Indonesia has developed increasingly comprehensive consumer-protection and payment-system regulation, including principles concerning asset protection, responsible business conduct, risk management, information security, and complaint resolution. France, however, supplements general private-law principles with a more explicit statutory architecture governing the consequences of unauthorized payment transactions, including reimbursement, differentiated customer responsibility, strong authentication, and evidentiary allocation. The distinction is therefore not simply that one jurisdiction protects customers while the other does not. Rather, the principal difference concerns the degree of specificity with which the law allocates transaction risks after unauthorized payments occur.

This comparison also demonstrates why an automatic-liability approach would be inappropriate for Indonesia. Imposing liability upon banks for every unauthorized digital transaction could create moral hazard and disregard customers' obligations to safeguard credentials, promptly report irregularities, and refrain from fraudulent or seriously negligent conduct. Conversely, automatically shifting losses to customers whenever correct credentials were used would disregard banks' superior control over payment infrastructure, authentication architecture, transaction monitoring, and technical evidence. A balanced private-law framework should therefore allocate responsibility according to the particular risk materializing in each case rather than according to a predetermined assumption that either banks or customers must always bear the loss.

A useful analytical distinction can be made between infrastructure risk, authentication risk, monitoring risk, credential risk, and conduct risk. Infrastructure and authentication risks generally fall more directly within the bank's technological and organizational sphere, although the precise allocation depends on the circumstances. Monitoring risk concerns whether objectively abnormal transactions

[25] Nancy E. Muenchinger, "French Law and Practice Concerning Multimedia and Telecommunications," *Westlaw, European Intellectual Property Review* 18, no. 4 (1996).

could reasonably have been detected or subjected to additional verification. Credential risk may involve both parties because the bank determines security architecture while customers are responsible for protecting personalized credentials. Conduct risk focuses on whether the customer acted fraudulently, intentionally disregarded security obligations, or engaged in conduct sufficiently serious to affect the allocation of loss. Such categorization provides a more precise method of connecting legal responsibility with the capacity to control the relevant source of risk.

Causation remains indispensable within this framework. A regulatory breach should not automatically result in civil liability merely because a customer has suffered a loss. There must be a legally sufficient relationship between the obligation breached and the damage claimed. If a bank failed to implement a required security measure and that failure enabled the unauthorized transaction, the causal connection may support liability.[26] By contrast, a regulatory deficiency unrelated to the mechanism producing the loss should not automatically transform the bank into an insurer against all forms of digital fraud. Similarly, customer negligence should affect liability only where the conduct materially contributed to the unauthorized transaction and meets the relevant legal threshold. This causal analysis is necessary to maintain proportionality between customer protection and the fundamental principles of private-law responsibility.

The contractual terms governing digital banking also require careful scrutiny. Standard-form banking agreements frequently allocate security responsibilities to customers, including obligations concerning passwords, personal identification numbers, devices, and authentication codes. Such clauses serve legitimate risk-management purposes, but contractual autonomy should not permit financial institutions to transfer risks arising from their own mandatory obligations or areas under their exclusive control. Consumer-protection principles therefore operate as a limit on contractual risk shifting. The crucial distinction is between a legitimate allocation of customer responsibilities and an exculpatory arrangement that effectively removes the bank's responsibility for security, system integrity, or other non-transferable legal duties.

The French experience is valuable for Indonesia not because French rules should be transplanted wholesale, but because it illustrates the advantages of articulating the consequences of unauthorized transactions through clearer legal presumptions, evidentiary rules, and differentiated standards of responsibility. Comparative private law must account for differences in regulatory institutions, payment infrastructures, procedural law, and the broader European framework within which French payment law operates. Nevertheless, the underlying principle is transferable at the conceptual level: the party with greater control over a particular risk and greater access to evidence concerning its materialization should bear a correspondingly greater legal responsibility for explaining and managing that risk.

[26] R. Tiwari, V. Tiwari, and VJ Varma, *Human Rights Disclosure in the Indian Banking Sector*, no. Query date: 2026-06-07 18:17:45 (2026), https://www.researchgate.net/profile/Vinit-Varma/publication/404113920_Human_Rights_Disclosure_in_the_Indian_Banking_Sector/links/69ea039032a2ba2b2d54b14f/Human-Rights-Disclosure-in-the-Indian-Banking-Sector.pdf.

Accordingly, customer protection in unauthorized digital transactions should not be understood as requiring unconditional reimbursement in every case, nor should bank liability depend exclusively upon proof of conventional technical failure. A more coherent approach is to begin with the legal status of the transaction—particularly whether genuine authorization existed—and subsequently determine responsibility through the allocation of control, applicable standards of conduct, evidentiary capacity, causation, and any material contribution by the customer. French law demonstrates how these factors can be incorporated into a specialized payment-liability regime, while Indonesia's evolving regulatory architecture provides the normative foundations from which a more explicit model could be developed.

The comparative analysis ultimately indicates that the central challenge for Indonesian private and banking law is not the absence of customer protection, but the need for greater doctrinal clarity concerning who bears which digital transaction risk, under what circumstances, and on what evidentiary basis. The movement toward risk-based payment regulation and stronger consumer protection provides an important foundation, but effective protection also requires a liability structure capable of distinguishing genuine authorization from technical authentication, ordinary customer error from serious misconduct, and unavoidable third-party fraud from losses connected to failures within the bank's sphere of control. These distinctions provide the foundation for reconstructing the allocation of digital transaction risks through a more proportionate model of bank liability and customer responsibility.

3.2. Reconstructing the Allocation of Digital Transaction Risks: Comparative Lessons from French Law for Indonesian Banking Law

The reconstruction of liability for digital banking transactions in Indonesia requires a shift from a predominantly fault-oriented approach toward a more structured risk-allocation model.[27] Digital losses may arise from interconnected factors, including technological infrastructure, authentication mechanisms, customer credentials, transaction monitoring, third-party fraud, and customer conduct. Liability should therefore be determined by identifying the risk that materialized, the party with greater capacity to control it, and whether the relevant legal obligations were properly performed.

This approach is increasingly relevant as Indonesian payment regulation becomes more technology- and risk-oriented. Bank Indonesia Regulation No. 10 of 2025 on the Payment System Industry incorporates governance, risk management, information-technology infrastructure, market conduct, and consumer protection into payment-system regulation. However, these regulatory obligations should be more clearly connected with the private-law consequences arising when such risks result in customer losses.

[27] Primerta Putri Hapsari and Salsabila Shafa Khairunnisa, "Evaluasi Efektivitas Pengaturan Dan Pengawasan Bank Indonesia Dan OJK Terhadap Kinerja Perbankan Di Indonesia," *J-CEKI : Jurnal Cendekia Ilmiah* 4, no. 4 (2025): 1431.

A fundamental distinction must be maintained between transaction risk and investment or commercial risk. Banks should not automatically be liable for losses arising from transactions voluntarily undertaken by customers, including unsuccessful investments or payments to third parties. Liability becomes more relevant where the loss concerns unauthorized payments, defective authentication, improper execution, or failures involving obligations within the bank's sphere of control. This distinction prevents customer protection from developing into unlimited banking liability.[28]

A further distinction concerns authentication and authorization. The successful use of passwords, one-time passwords, biometrics, or registered devices may establish technical authentication but does not necessarily prove that the customer knowingly authorized the transaction. This distinction is particularly important in phishing, account takeover, credential theft, and social-engineering cases. Accordingly, technical authentication should constitute relevant evidence of authorization rather than conclusive proof of legally valid consent.

French payment law offers an important comparative lesson in this respect. Under Article L133-18 of the French Code monétaire et financier, an unauthorized payment transaction generally triggers an obligation upon the payer's payment service provider to reimburse the payer under the statutory conditions and restore the debited account to the position in which it would have been had the unauthorized transaction not occurred. This approach is significant because the legal analysis begins with the authorization status of the transaction rather than requiring the customer first to establish conventional negligence by the financial institution.

The reimbursement principle is nevertheless combined with customer responsibility. French law provides circumstances in which the payer may bear losses, particularly where the customer has acted fraudulently or intentionally or through gross negligence failed to comply with legally prescribed security obligations. The model therefore does not impose strict and unlimited liability upon banks. Instead, it differentiates risks according to their source and the conduct of the parties.[29] This structure provides a useful conceptual reference for Indonesia because customer protection and customer responsibility are treated as complementary rather than contradictory principles.

The allocation of the burden of proof constitutes another important element of this framework. Article L133-23 of the French Code monétaire et financier places significant evidentiary responsibility upon the payment service provider where the user denies having authorized a transaction. The provider must establish matters relating to authentication and proper recording, while the recorded use of the payment instrument is not necessarily sufficient in itself to establish authorization or

[28] P. Thalib et al., "Legal Framework and Employee Liability in Banking Compliance and Crime Prevention: The Case Analysis of Indonesia," *Yustisia* 13, no. 3 (2024): 298–312, Scopus, https://doi.org/10.20961/yustisia.v13i3.93370.

[29] M. Polzin, "The Basic-Structure Doctrine and Its German and French Origins: A Tale of Migration, Integration, Invention and Forgetting," *Indian Law Review*, no. Query date: 2026-08-09 22:53:13 (2021), https://doi.org/10.1080/24730580.2020.1866882.

fraud or gross negligence by the payer. The underlying logic is particularly relevant to digital banking because the provider generally controls the technological infrastructure and possesses substantially greater access to transaction evidence.

Indonesia should not necessarily reproduce the French statutory model verbatim. France operates within the European Union's harmonized payment-services framework, while Indonesia possesses a different institutional, regulatory, procedural, and technological environment. Comparative legal analysis should therefore function as a mechanism of functional adaptation rather than legal transplantation. What can be derived from France are the structural principles underlying the model: differentiation between authorization and authentication, clearer allocation of unauthorized-payment risks, proportionate customer responsibility, and evidentiary obligations reflecting the parties' unequal access to technical information. These comparative findings can be organized into several dimensions that are relevant to reconstructing the Indonesian framework.

Table 1. Comparative Framework for the Allocation of Digital Transaction Risks in Indonesia and France

Dimension	Indonesian Framework	French Framework	Direction for Indonesian Reconstruction
Legal basis of liability	Combination of private law, banking regulation, payment regulation, and consumer protection	General private law complemented by a specific statutory payment-liability regime	Develop clearer interaction between general civil liability and specific digital-payment rules
Authentication and authorization	Greater doctrinal clarification remains necessary in disputed digital transactions	Legally differentiated within the unauthorized-payment framework	Expressly distinguish technical authentication from legally valid authorization
Initial allocation of unauthorized-payment risk	Determined through multiple legal and regulatory obligations and factual circumstances	Unauthorized transactions are subject to a structured reimbursement regime	Establish clearer presumptions concerning initial loss allocation
Customer responsibility	Relevant through contractual and	Fraud, intentional conduct, and gross negligence	Develop differentiated standards rather

	regulatory security obligations	can alter loss allocation	than treating every customer error equally
Burden of proof	May involve significant practical information asymmetry	Provider bears important evidentiary obligations when authorization is disputed	Allocate evidentiary responsibility according to possession and control of technical evidence
Bank's sphere of control	Security, payment infrastructure, authentication, monitoring, and regulatory compliance	Provider obligations are connected with payment security and statutory liability	Adopt a control-based assessment of banking responsibility
Transaction monitoring	Governed through banking/payment risk-management obligations	Operates alongside payment-security requirements	Connect monitoring failures with liability where a causal relationship to loss is established
Causation	General principles of civil liability remain important	Specialized payment rules operate alongside broader private-law principles	Preserve causation as a safeguard against unlimited liability
Customer remedy	Depends on applicable banking, consumer, payment, contractual, and dispute-resolution mechanisms	Statutory reimbursement rules provide a clearer starting point for unauthorized transactions	Develop more predictable remedies and reimbursement procedures
Regulatory orientation	Increasingly risk-based and consumer-oriented	Risk allocation is more specifically structured for payment transactions	Move toward an integrated risk-allocation model adapted to Indonesian law

Source: Authors' comparative legal analysis based on Indonesian banking and payment-system regulation and the French Code monétaire et financier.

Table 1 demonstrates that the principal difference does not lie in the existence or absence of customer protection. Both jurisdictions recognize obligations associated with payment security and customer interests. The more significant difference concerns the legal architecture through which losses are allocated after an unauthorized transaction occurs. French law provides a more structured connection between authorization, reimbursement, customer conduct, and evidentiary responsibility. Indonesia, by comparison, can strengthen the interaction between its increasingly sophisticated regulatory requirements and the private-law determination of responsibility for customer losses.

On this basis, reconstruction should begin with the principle of risk control. Responsibility should presumptively follow the party possessing the greater legal and practical capacity to manage the risk in question. Banks ordinarily possess superior control over payment-system architecture, authentication design, security protocols, transaction records, and certain forms of transaction monitoring. Customers, however, possess greater control over their personal conduct, devices in particular circumstances, and the confidentiality of security credentials. This distribution does not predetermine liability, but provides a principled starting point for determining which party should explain why a particular protective mechanism failed.

The control-based approach should be complemented by the principle of risk prevention capacity. Control and prevention are related but not identical. A bank may not directly control the criminal conduct of a fraudster, but it may possess technological capacity to identify certain transaction anomalies, impose additional verification requirements, temporarily restrict suspicious transactions where legally justified, or communicate security warnings. Conversely, a customer may have no control over the bank's infrastructure but may possess the capacity to avoid voluntarily disclosing confidential authentication information.[30] Liability should therefore consider whether a party could reasonably have prevented or mitigated the particular risk within the limits of its legal obligations.

This framework does not mean that every failure to identify an unusual transaction should generate bank liability. Such a standard could effectively convert banks into insurers against all customer losses and impose an unrealistic obligation to prevent every instance of fraud. The relevant inquiry must remain connected to the applicable standard of care and the characteristics of the transaction. Factors such as deviation from established transaction patterns, transaction value, changes in devices or access patterns, repeated transfers, security alerts, and other objectively identifiable indicators may be relevant, but their legal significance must be assessed according to applicable regulation and the technological capabilities reasonably expected of the provider.

[30] Suaibatul Aslamiyah and Rahmat Agus Santoso, *Implementasi Strategi Pemasaran Pada PT. Bank Perkreditan Rakyat (BPR) MCM*, n.d.

A third component should therefore be causal responsibility. Even where a bank breaches a regulatory or contractual obligation, compensation should not automatically follow unless the breach bears a sufficient causal relationship to the customer's loss. The same principle should apply to customer conduct. Disclosure of information, failure to respond to a warning, or other negligent behavior should affect the allocation of loss only to the extent that the conduct materially contributed to the unauthorized transaction. Causation prevents a control-based model from becoming an unlimited liability regime and preserves the fundamental private-law connection between legally relevant conduct and compensable damage.

Customer conduct should additionally be assessed through a graduated standard of responsibility. Digital fraud is increasingly based on sophisticated social engineering capable of deceiving reasonably careful individuals. It would therefore be disproportionate to characterize every successful deception as serious customer negligence. A reconstructed Indonesian framework could distinguish ordinary error, negligence, gross negligence, intentional violation of security obligations, and fraud.[31] The degree of customer responsibility could then influence the allocation of loss. The French distinction involving fraud and gross negligence provides a useful comparative reference for developing such differentiation, although the precise standards must be adapted to Indonesian legal doctrine.[32]

The burden of proof should similarly reflect evidentiary control. A customer disputing a transaction should be required to provide a sufficiently clear allegation and information reasonably within their possession. However, it is difficult to justify requiring customers to prove technical matters exclusively controlled by financial institutions. Transaction logs, authentication records, device identification, security-system responses, and internal monitoring information generally remain within the provider's informational domain. A more balanced framework would therefore require the bank to demonstrate the operation of security and authentication mechanisms when authorization is genuinely disputed, without eliminating the customer's obligation to cooperate and disclose relevant information.

Such evidentiary allocation would also reinforce procedural fairness. Formal equality between the parties does not necessarily produce substantive equality when one party possesses virtually all of the evidence necessary to determine how a digital transaction occurred. The principle should not be understood as automatically reversing the entire burden of proof in every banking dispute. Rather, the burden concerning a particular technical fact should correspond, where legally appropriate, to the party possessing superior access to evidence of that fact. This approach is consistent with the control-based logic underlying the broader reconstruction.

---

[31] M. C. Marakalala, "Forensic Identification: The Biometric Technology Linked to Online Financial Fraud and Crime Related to the South African Banking Industry," *OIDA International Journal of Sustainable Development* 17, no. 12 (2024): 81–98, Scopus.

[32] M. Salas and S. Wardani, "Perkembangan Doktrin Perbuatan Melawan Hukum Oleh Penguasa," *… Ilmu Sosial & …*, no. Query date: 2026-04-26 18:09:31 (2026), http://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZayn/article/view/3608.

The model should further recognize the limits of contractual risk allocation. Banks legitimately require customers to maintain the confidentiality of passwords, PINs, authentication codes, and other personalized security credentials. Such obligations are necessary for digital payment systems to function. However, standard contractual terms should not be permitted to shift risks arising from the bank's mandatory security, infrastructure, or regulatory obligations entirely onto customers. Contractual freedom should remain subject to consumer-protection requirements, good faith, mandatory banking regulation, and the prohibition of contractual arrangements that effectively eliminate accountability for obligations falling within the provider's own sphere of responsibility.[33]

A reconstructed Indonesian framework can consequently be conceptualized through four cumulative questions. First, what type of risk materialized? Second, which party possessed the greater control or preventive capacity over that risk? Third, did either party fail to perform an applicable contractual, statutory, regulatory, or security obligation? Fourth, did that failure materially cause or contribute to the loss? Only after these questions have been answered should the ultimate financial responsibility be determined. Such sequencing provides greater analytical precision than beginning with a general assumption of customer negligence or automatic bank liability.

This approach also permits proportional or contributory allocation where both parties materially contributed to the loss, insofar as consistent with the applicable Indonesian legal framework. Digital fraud frequently does not result exclusively from a single failure. A customer may have disclosed sensitive information, while a bank's security or monitoring system may simultaneously have failed to respond to objectively abnormal circumstances. A binary all-or-nothing liability model may therefore produce disproportionate outcomes. A risk-allocation framework allows the legal analysis to recognize multiple causal contributions while maintaining a clear distinction between the respective spheres of responsibility.

The proposed reconstruction can thus be expressed through the relationship risk identification → control and prevention capacity → applicable duty → breach → causation → evidentiary responsibility → allocation of loss. This sequence does not abandon fault-based private law. Rather, it contextualizes fault within the technological and informational realities of digital banking. Fault remains relevant, but it is assessed after identifying which party was legally expected to control the risk that materialized. This makes the framework particularly suitable for disputes where conventional assumptions regarding physical possession, signatures, and direct payment instructions no longer correspond to the operation of digital transactions.

French law provides an important comparative lesson because it demonstrates that strong customer protection can coexist with meaningful customer responsibility. A structured reimbursement regime does not necessarily eliminate the customer's obligations, while enhanced provider responsibility does not require

[33] M. Klamert, "Good Faith in European Union Law," *Gleams of Good Faith in Constitutional Law*, no. Query date: 2026-06-03 15:02:06 (2026), https://doi.org/10.1007/978-3-032-06486-8_4.

banks to guarantee customers against every form of fraud. The essential achievement is greater predictability concerning the legal consequences of unauthorized transactions. For Indonesia, this predictability would benefit customers, banks, regulators, dispute-resolution institutions, and courts by providing a clearer analytical structure for determining responsibility.

Ultimately, the reconstruction of digital transaction risk allocation should move Indonesian banking law from an overly binary bank fault versus customer fault paradigm toward a control-based, evidence-sensitive, and proportionate risk-allocation model. The comparative lesson from France is not that Indonesia should reproduce European payment law, but that unauthorized digital transactions require rules capable of connecting authorization, control, prevention, evidence, customer conduct, and causation within a coherent liability structure. Such a model would strengthen customer protection without transforming banks into absolute guarantors of digital transactions and would simultaneously preserve customer responsibility where loss results from conduct genuinely falling within the customer's sphere of control. The resulting balance between protection and responsibility provides a stronger private-law foundation for the continuing development of Indonesia's digital banking system.

4. Conclusion

The comparative analysis demonstrates that effective customer protection in digital banking transactions requires a liability framework that moves beyond a binary determination of bank fault or customer negligence toward a more structured and proportionate allocation of digital transaction risks. While Indonesian law has progressively strengthened risk management and consumer protection within the banking and payment-system framework, greater doctrinal clarity remains necessary regarding unauthorized transactions, authentication, authorization, evidentiary responsibility, and the allocation of financial losses. French private and payment law provides valuable comparative lessons by establishing a more structured relationship between reimbursement, customer conduct, gross negligence, and the burden of proof, although its framework cannot be directly transplanted into Indonesia’s distinct regulatory environment. Accordingly, Indonesian banking law should develop a control-based and risk-allocation model that determines responsibility according to the source of the risk, each party’s capacity to control or prevent it, compliance with applicable legal obligations, access to relevant technical evidence, and the causal contribution of each party to the resulting loss. Such an approach would distinguish genuine customer responsibility from risks falling within the bank’s sphere of control, strengthen legal certainty and customer protection, and prevent banks from being transformed into absolute guarantors against every form of digital financial loss.

Acknowledgments (Optional)

None.

References

Abbassi, H., S. El Mendili, and Y. Gahi. "A Conceptual Real-Time and Privacy-Preserving Architecture for Banking Fraud Detection." In *Int. Conf. Optim. Appl., ICOA - Proc.*, edited by Hachimi H. and EL Mokhi C. Institute of Electrical and Electronics Engineers Inc., 2025. Scopus. https://doi.org/10.1109/ICOA66896.2025.11236932.

Abdalsatar, A. M., and M. S. Mohammed. "The Impact of Artificial Intelligence Applications on Banking Operations: A Case Study on the Bank (HSBC) British for the Period (2016–2022)." In *Lect. Notes Networks Syst.*, 1697 LNNS, edited by Abdelgawad A., Hameed A.A., and Jamil A., 570–81. Springer Science and Business Media Deutschland GmbH, 2025. Scopus. https://doi.org/10.1007/978-3-032-09562-6_42.

Agnia, R., SC Ar-Rusd, and ... "Restrukturisasi Kredit Dalam Perspektif Hukum Perbankan: Dampak Terhadap Hubungan Kontraktual Antara Bank Dan Nasabah." *Journal of Legal, Political …*, no. Query date: 2026-06-07 18:14:46 (2025). http://scriptaintelektual.com/custodia/article/view/375.

Agustuti, D., and A. Irawan. "Kajian Normatif Pertanggungjawaban Pidana Pengurus Bank Terkait Tindak Pidana Perbankan Dalam Proses Pemberian Kredit." *Indonesian Journal of Law and Justice*, no. Query date: 2026-06-07 18:14:46 (2024). http://kurniajurnal.com/index.php/ijlj/article/view/174.

Ahmed, S. "The Fatal Flaw of Glocal 'Solutions' to Illicit Financial Flows." *Journal of Economic Criminology* 7 (2025). Scopus. https://doi.org/10.1016/j.jeconc.2024.100116.

Akerboom, Sanne, and Robin Kundis Craig. "How Law Structures Public Participation in Environmental Decision Making: A Comparative Law Approach." *Environmental Policy and Governance* 32, no. 3 (June 2022): 232–46. https://doi.org/10.1002/eet.1986.

Aladwan, Z. "Legal Basis for the Fraud Exception in Letters of Credit under English Law." *Journal of Financial Crime* 30, no. 2 (2023): 594–600. Scopus. https://doi.org/10.1108/JFC-01-2020-0004.

Alhakim, Abdurrakhman, and Sofia Sofia. "Kajian Normatif Penanganan Cyber Crime Di Sektor Perbankan Di Indonesia." *Jurnal Komunitas Yustisia* 4, no. 2 (August 2021): 377–85. https://doi.org/10.23887/jatayu.v4i2.38089.

Amalia, II. "Kepastian Hukum Pengawasan Hakim Oleh Komisi Yudisial Terhadap Perkara Perdata Di Indonesia." *Perpustakaan Pascasarjana*, no. Query date: 2026-03-13 11:28:29 (2022).

Aslamiyah, Suaibatul, and Rahmat Agus Santoso. *Implementasi Strategi Pemasaran Pada PT. Bank Perkreditan Rakyat (BPR) MCM*. n.d.

Asy'ari, Mochammad Syahrul. "Analisis Kelayakan Nasabah Menggunakan Prinsip 5C 1S Dalam Pembiayaan Pemilikan Rumah (PPR) (Studi Pada KB Bank Syariah KC Sidoarjo)." *Jurnal Ilmiah Ekonomi Dan Manajemen* 2, no. 11 (2024).

Bujalski, M. "Could French Law Provide a Model for Regulation of the Enforcement of Security Rights in Digital Assets?" *Forum Prawnicze*, no. Query date: 2026-

09-12 12:13:22 (2025). https://access.heinonline.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/frmpwn2025§ion=19.

Caldarone, P. "Banking phishing: main defense tools and responsibility profile." *Rivista Italiana di Informatica e Diritto* 5, no. 2 (2023). Scopus. https://doi.org/10.32091/RIID0116.

Chitimira, H., E. Torerai, and V. L. M. Jana. "Leveraging Artificial Intelligence to Combat Money Laundering and Related Crimes in the South African Banking Sector." *Potchefstroom Electronic Law Journal* 27 (2024): 1–30. Scopus. https://doi.org/10.17159/1727-3781/2024/v27i0a18024.

Combot, M. "Subsidiarity and Unjustified Enrichment: Perspective under French Law." *European Review of Private Law= Revue …* , no. Query date: 2026-09-12 12:13:22 (2026). https://search.proquest.com/openview/5299a4823434a5c9a932065b57c72945/1?pq-origsite=gscholar&cbl=7100263.

David Debenham. "Big Data Analytics, Big Financial Institutions, and Big Money Fraud Litigation." *Westlaw, 32 Banking and Finance Law Review* 103 (2016).

Elisabeth Nurhaini Butar-Butar. *Metode Penelitian Hukum, Langkah-Langkah Untuk Menemukan Kebenaran Dalam Ilmu Hukum*. Bandung: PT. Refika Aditama, 2018.

Garg, N., and K. Gupta. "Data Privacy in Online Banking Using Blowfish Algorithm: A Review." *Progressive Computational Intelligence, Information Technology and Networking*, 2025, 888–91. Scopus. https://doi.org/10.1201/9781003650010-145.

Gisclard, T. *Utility Models in French Law*. no. Query date: 2026-09-12 12:13:22 (n.d.).

Hapsari, Primerta Putri, and Salsabila Shafa Khairunnisa. "Evaluasi Efektivitas Pengaturan Dan Pengawasan Bank Indonesia Dan OJK Terhadap Kinerja Perbankan Di Indonesia." *J-CEKI : Jurnal Cendekia Ilmiah* 4, no. 4 (2025): 1431.

Kattan, MS Al. "The Use of Technology in Compulsory Enforcement: A Comparative Study in Emirati and French Law." *Digital Evidence and Procedural Law in the UAE*, no. Query date: 2026-09-12 12:13:22 (2026). https://www.igi-global.com/chapter/the-use-of-technology-in-compulsory-enforcement/406892.

Klamert, M. "Good Faith in European Union Law." *Gleams of Good Faith in Constitutional Law*, no. Query date: 2026-06-03 15:02:06 (2026). https://doi.org/10.1007/978-3-032-06486-8_4.

Lytvynenko, AA. "The Institute of Trade Secrets in English and French Law in the 19th and Early 20th Centuries: Doctrine and Jurisprudence." *International Comparative Jurisprudence*, no. Query date: 2026-09-12 12:13:22 (2024). https://www.ceeol.com/search/article-detail?id=1249603.

Marakalala, M. C. "Forensic Identification: The Biometric Technology Linked to Online Financial Fraud and Crime Related to the South African Banking Industry." *OIDA International Journal of Sustainable Development* 17, no. 12 (2024): 81–98. Scopus.

Nancy E. Muenchinger. "French Law and Practice Concerning Multimedia and Telecommunications." *Westlaw, European Intellectual Property Review* 18, no. 4 (1996).

Pecnard, C., and A. Jarlot. "Arbitration and Intellectual Property in French Law." *… Handbook on Intellectual Property Rights and …*, no. Query date: 2026-09-12 12:13:22 (2024). https://www.elgaronline.com/edcollchap/book/9781800378360/book-part-9781800378360-31.xml.

Phiri, J., T. Lavhengwa, and M. A. Segooa. "Online Banking Fraud Detection: A Comparative Study of Cases from South Africa and Spain." *South African Journal of Information Management* 26, no. 1 (2024). Scopus. https://doi.org/10.4102/sajim.v26i1.1763.

Polzin, M. "The Basic-Structure Doctrine and Its German and French Origins: A Tale of Migration, Integration, Invention and Forgetting." *Indian Law Review*, no. Query date: 2026-08-09 22:53:13 (2021). https://doi.org/10.1080/24730580.2020.1866882.

Salas, M., and S. Wardani. "Perkembangan Doktrin Perbuatan Melawan Hukum Oleh Penguasa." *… Ilmu Sosial & …*, no. Query date: 2026-04-26 18:09:31 (2026). http://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/AlZayn/article/view/3608.

Shajahan, S., and A. R. Nair. "Jurisdictional Conundrum in Digital Banking Frauds: Reinvestigation of the Effectiveness of International Conventional Laws vs. Contemporary Approaches on Cyberspace." *Revista Brasileira de Alternative Dispute Resolution* 7, no. 13 (2025): 261–74. Scopus. https://doi.org/10.52028/rbadr.v7.i13.ART13.IN.

Thalib, P., F. Kurniawan, S. M. Salsabila, and M. N. Kholiq. "Legal Framework and Employee Liability in Banking Compliance and Crime Prevention: The Case Analysis of Indonesia." *Yustisia* 13, no. 3 (2024): 298–312. Scopus. https://doi.org/10.20961/yustisia.v13i3.93370.

Tiwari, R., V. Tiwari, and VJ Varma. *Human Rights Disclosure in the Indian Banking Sector*. no. Query date: 2026-06-07 18:17:45 (2026). https://www.researchgate.net/profile/Vinit-Varma/publication/404113920_Human_Rights_Disclosure_in_the_Indian_Banking_Sector/links/69ea039032a2ba2b2d54b14f/Human-Rights-Disclosure-in-the-Indian-Banking-Sector.pdf.

Upreti, K., P. Vats, A. Srinivasan, K. V. D. Sagar, R. Mahaveerakannan, and G. C. Babu. "Detection of Banking Financial Frauds Using Hyper-Parameter Tuning of DL in Cloud Computing Environment." *International Journal of Cooperative Information Systems* 34, no. 1 (2025). Scopus. https://doi.org/10.1142/S0218843023500247.