OPEN ACCESS

LAW RESEARCH Review Quarterly

Law Research Review Quarterly is a **Journal for Law, Justice, and Crime in Indonesia and Southeast Asia**. The Journal is a peer-reviewed journal published by Faculty of Law Universitas Negeri Semarang, Indonesia. The Journal published quarterly on February, May, August, and November. ISSN 2716-3415 (Online)
Online at https://journal.unnes.ac.id/snh

Reconceptualizing of Bank Liability for Customer Losses Resulting from Social Engineering Through the Doctrine of Strict Liability and the Reversal of the Burden of Proof Based on the Cheapest Cost Avoider Principle to Ensure Equality of Arms

Rizkya Wina Yahriza Pohan
Universitas Sultan Ageng Tirtayasa, Serang, Indonesia
1111230473@untirta.ac.id

Zahra Arya Zaura
Universitas Sultan Ageng Tirtayasa, Serang, Indonesia
1111230471@untirta.ac.id

Louis Venansius
Universitas Sultan Ageng Tirtayasa, Serang, Indonesia
1111230248@untirta.ac.id

Arsyah Wijaya
Universitas Sultan Ageng Tirtayasa, Serang, Indonesia
1111230256@untirta.ac.id

Muhammad Fauzi Rais Lutfi, S.H., M.H.
Universitas Sultan Ageng Tirtayasa, Serang, Indonesia
muhammad.fauzi@untirta.ac.id

Abstract

The rapid digitalization of banking services in Indonesia has generated a significant surge in social engineering fraud, with 99 percent of banking fraud cases attributable to psychological manipulation. This study aims to reconceptualize bank liability for customer losses arising from social engineering-based OTP fraud and to reconstruct the burden of proof mechanism in civil procedural law to guarantee equality of arms. This research employs a normative legal methodology with a qualitative approach, utilizing statutory, conceptual, and case analysis perspectives. Primary legal materials include relevant legislation and financial authority regulations, while secondary materials consist of legal doctrine, academic journals, and prior scholarly works. The findings reveal two principal conclusions. First, transactions resulting from social engineering contain *Wilsgebreken* under Article 1321 of the Civil Code, as customer authorization is obtained through psychological manipulation rather than free will. Reconceptualizing bank liability under strict liability is justified through the Cheapest Cost Avoider doctrine, which allocates responsibility to banks as the most efficient party to prevent losses, and through fiduciary duty, which obliges banks to actively protect customers from predictable digital risks. Second, conventional proof mechanisms based on *Actori Incumbit Probatio* violate equality of arms, as all forensic evidence is held exclusively by banks. A three-tier burden-shifting mechanism is proposed: customers establish a *Prima Facie* threshold, the burden shifts to banks to prove system integrity and compliance with duty of care, and courts conduct substantive material truth examination. Regulatory harmonization across the Financial Services Authority, Bank Indonesia, and the judiciary is essential for effective implementation.

KEYWORDS
Social Engineering, Bank Liability, Burden of Proof, *Wilsgebreken*, Equality of Arms

Introduction

The transformation of financial services toward a digital banking ecosystem has fundamentally changed the way banks and customers interact. Through mobile banking, internet banking, and digital payment systems, customers can now conduct transactions anytime and anywhere

without having to physically visit a bank branch. This development has prompted banks to implement multi-layered security measures, ranging from PINs, passwords, and biometric verification to One-Time Passwords (OTPs) as authentication tools for digital transactions. However, despite the convenience offered, these advancements in security technology have been accompanied by a corresponding rise in cybercrimes based on psychological manipulation or social engineering, which exploit customer trust and lapses in vigilance.

Empirical data shows that the phenomenon of social engineering in Indonesia's digital banking sector has reached alarming levels. According to an official statement by the Head of the Consumer Protection Department at the Financial Services Authority (OJK), 99 percent of banking fraud cases in Indonesia are social engineering-based crimes, far exceeding the global average of 88 percent.[1] This situation is further exacerbated by data from the 2025 Global Fraud Index, which ranks Indonesia second-lowest out of 112 countries in terms of resilience against fraud, with over 70 percent of recorded fraud cases dominated by social engineering schemes. Meanwhile, a report by the National Cyber and Cryptography Agency (BSSN) notes that economic losses due to cybercrime in Indonesia in 2024 reached Rp 18 trillion, with a 30 percent increase in cases compared to the previous year.[2] These figures make protecting customers from social engineering an urgent legal issue that must be addressed systematically.

Unlike conventional cybercrimes that directly target the technical infrastructure of banking systems, social engineering operates by psychologically manipulating customers into voluntarily handing over

[1] Agustinus Rangga Respati and Erlangga Djumena, "99 Persen Kasus Penipuan Perbankan Di Indonesia Karena 'Social Engineering,'" Kompas.com, 2023, https://money.kompas.com/read/2023/08/03/161100126/99-persen-kasus-penipuan-perbankan-di-indonesia-karena-social-engineering-.

[2] Fajarpos, "Indonesia Peringkat Kedua Terendah Global Fraud Index 2025, Komdigi Ungkap 70% Kasus Didominasi Social Engineering," Fajarpos Network, 2026, https://www.fajarpos.com/16/02/2026/indonesia-peringkat-kedua-terendah-global-fraud-index-2025-komdigi-ungkap-70-kasus-didominasi-social-engineering/.

confidential data, OTP codes, or mobile banking access to the perpetrators. Common methods include fake call centers impersonating banks, phishing links disguised as official websites, smishing via text messages, phishing via voice calls, and impersonation by perpetrators posing as bank employees.[3] The OJK has officially identified at least four social engineering tactics that frequently harm banking customers: manipulation of information regarding changes in transfer fees, offers to upgrade to priority customer status, the creation of fake customer service accounts, and offers to become Laku Pandai agents.[4] In these various cases, the transactions that occur are still technically considered valid by the banking system because they are carried out using valid authentication credentials, even though they essentially stem from psychological manipulation.

The most fundamental legal issue in cases of social engineering-based OTP fraud is the failure of the conventional banking liability system to provide effective protection for affected customers. The current liability system is oriented toward fault-based liability as stipulated in Article 1365 of the Civil Code, which requires the party claiming damages, in this case the customer, to prove the bank's fault or negligence.[5] In practice, this mechanism places customers in a structurally disadvantageous position, given that all relevant technical data such as audit logs, authentication records, transaction timestamps, and suspicious transaction monitoring records are entirely under the bank's exclusive control.[6] This imbalance not

[3] Tias Aprilia Hasanudin, "JAWAB BANK DALAM PENANGGULANGAN KEJAHATAN DIGITAL BERBASIS SOCIAL ENGINEERING : ANALISIS HUKUM PERBANKAN," *Indonesia of Journal Business Law* 5, no. 1 (2026): 99–115, https://doi.org/10.47709/ijbl.v5i1.7476.

[4] Mochamad Januar Rizki, "4 Modus Kejahatan 'Social Engineering' Dan Tanggung Jawab Perbankan," HUKUMONLINE.COM, 2022, https://www.hukumonline.com/berita/a/4-modus-kejahatan-social-engineering-dan-tanggung-jawab-perbankan-lt62ac38ff8cd0b/.

[5] Muhammad Faisal Aziz and Sepriyadi Adhan S, "Perlindungan Hukum Terhadap Nasabah Atas Penyalahgunaan Data Pribadi Oleh Pihak Bank Di Era Digitalisasi Perbankan," *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 3, no. 6 (2025): 8840–52.

[6] Mayang Dias Putri, "Analisis Tanggung Gugat Bank Atas Perbuatan Melawan Hukum Pegawai Bank Yang Merugikan Nasabah (Studi Kasus Putusan Mahkamah Agung Nomor 2600 K / Pdt / 2022)," *Lex Patrimonium* 3, no. 2 (2024).

only violates the principle of equality of arms in civil procedure law but also highlights the inadequacy of the fault-based liability paradigm in addressing the asymmetrical nature of digital banking disputes.

In addition to the issue of proof, the validity of transactions resulting from social engineering also requires in-depth legal analysis. Normatively speaking, transactions arising from psychological manipulation are in fact vitiated by a defect of consent (*Wilsgebreken*) as provided for in Article 1321 of the Civil Code, since the customer's will is formed not through a process of free decision-making (*Vrije Wil*) but as a result of systematic misrepresentation (*dwaling*) or deception (*bedrog*) by the perpetrator.[7] From this perspective, the technical validity of authentication, namely the successful use of the correct OTP, cannot be equated with the legal validity of the transaction, because technical compliance does not eliminate the underlying defect in consent that formed that will. This situation creates a dichotomy between technical validity and legal validity in digital banking transactions, which to date has not received an adequate normative response within the Indonesian legal system.

Reconceptualizing bank liability through strict liability offers a more responsive legal framework for this reality. Under the Cheapest Cost Avoider (CCA) doctrine developed by Guido Calabresi, legal responsibility should be allocated to the party best positioned to prevent losses at the lowest cost, a role clearly occupied by banks, which design authentication systems, control digital security infrastructure, and possess the technical capability to detect abnormal transactions.[8] This reconceptualization is further reinforced by the fiduciary character of the bank-customer relationship, which obliges banks to actively protect customers from

[7] Ahmad Jalaludin Arrodli et al., "Konsekuensi Hukum Cacat Kehendak Dalam Pembentukan Perjanjian Berdasarkan Pasal 1320 Kitab Undang-Undang Hukum Perdata," *LETTERLIJK: JURNAL HUKUM PERDATA* 1, no. 2 (2024).

[8] Wilhemina Setia Admadja, Gavra Datadavie Ginting, and Maheswari Queena Dewani, "Fault-Based Liability Vs . Strict Liability : Comparative Study of the Concept of Unlawful Acts Indonesia – Japan," *Journal of Social Research* 4, no. 11 (2025): 2973–83.

predictable digital fraud risks rather than sheltering behind the technical validity of authenticated transactions.[9]

Prior research has examined related aspects of this problem from various angles. Hasanudin (2026) analyzed bank liability for digital fraud without reaching a strict liability reconceptualization.[10] Atmadja et al. (2025) compared strict liability and fault-based liability without integrating the CCA doctrine and fiduciary duty simultaneously.[11] Arrodli et al. (2024) examined *Wilsgebreken* in contract formation without linking it to digital banking fraud.[12] Sibarani (2023) and Simanjuntak et al. (2024) addressed the reversal of the burden of proof outside the digital banking context. The novelty of this study lies in simultaneously integrating strict liability, the CCA doctrine, and fiduciary duty to reconceptualize bank liability for OTP fraud losses arising from social engineering, grounded in a juridical validity analysis through the concept of *Wilsgebreken* under the Civil Code.

Against this background, this study addresses two principal research questions: first, how should bank liability be reconceptualized under strict liability in light of the CCA doctrine and fiduciary duty for digital banking transactions vitiated by *Wilsgebreken* arising from social engineering; and second, how should the mechanism of *Omkering Van de Bewijslast* (reversal of the burden of proof) be reconstructed for such transactions in order to realize the principle of equality of arms in civil procedural law. Answering these questions is necessary to close the specific normative gap between Indonesia's formal authentication-based liability regime and the

[9] G Jackson, "Banks, Automatic Cross-Border Exchange of Taxpayer Information and English Common Law Fiduciary Duties Owed to Customers," *Bulletin for International Taxation* 77 (2023), https://doi.org/10.59403/2nyp97p.

[10] Mery R.L. Sibarani, "Penerapan Omkering Van Bewijslast Dalam Pembuktian Tindak Pidana Korupsi Indonesia," *Honeste Vivere Journal* 6, no. 2 (2023): 151–60.

[11] Disriani Latifah Soroinda, "Jurnal Hukum & Pembangunan Kekuatan Pembuktian Alat Bukti Elektronik Dalam Hukum Acara Perdata," *Jurnal Hukum Dan Pembangunan* 52, no. 2 (2022).

[12] Galuh Candra Utami and Sidi Ahyar Wiraguna, "Pembuktian Digital Dalam Sengketa Perdata : Menguji Validitas Formil Dan Materiil Dokumen Elektronik Di Era Modern," *Jurnal Hukum Perdata Dan Pidana* 2, no. 4 (2025): 40–52.

substantive legal reality of consent vitiated by psychological manipulation, a gap that current banking regulation, consumer protection law, and civil procedure doctrine have each addressed only partially and in isolation.

Method

This study employs a normative legal research method with a qualitative approach, utilizing statutory, conceptual, and case-based analytical frameworks. Legal materials are drawn from two sources: primary materials comprising legislation governing banking, consumer protection, electronic transactions, and civil procedure law; and secondary materials consisting of academic literature, legal doctrines, and prior research relevant to bank liability and digital banking fraud. These materials are analyzed to examine the reconceptualization of bank liability under the doctrines of *Strict Liability*, *Cheapest Cost Avoider* (CCA), and *Fiduciary Duty* in relation to digital banking transactions involving defects of consent (*Wilsgebreken*) arising from *social engineering*, as well as the reconstruction of the *Omkering van de Bewijslast* mechanism to realize the principle of *equality of arms* in civil procedural law.

Results and Discussion

This section presents the results of a legal analysis of the two main research issues: the reconceptualization of bank liability based on strict liability through the CCA framework and fiduciary duty regarding digital banking transactions involving defects of consent (*Wilsgebreken*) resulting from social engineering; and the reconstruction of the mechanism of the reversal of the burden of proof (*Omkering Van de Bewijslast*) to realize the principle of equality of arms in civil procedure law. The normative analysis indicates that the fault liability paradigm is no longer adequate given that customer losses from social engineering concern the validity of legal intent (*Wilsgebreken*) underpinning the transaction, not merely the technical

validity of authentication.

1. Characteristics of Social Engineering in Digital Banking Transactions and the Issue of Defects of Consent *(Wilsgebreken)*

The characteristics of social engineering in digital banking transactions have direct legal implications for the validity of the customer's intent. Transactions resulting from psychological manipulation are often deemed valid because they utilize the customer's OTP or PIN, even though such consent actually stems from a defect of consent (*Wilsgebreken*); this is the core legal problem driving the reconceptualization of bank liability in this study.

Social engineering operates by exploiting the human factor as the most vulnerable point in digital security systems, so that perpetrators do not need to hack into a bank's technical infrastructure; they simply need to create psychological conditions in which customers "voluntarily" hand over their credentials. Legally, authorization resulting from such manipulation cannot be classified as free consent (*Vrije Wil*) as required by Article 1320 of the Civil Code, but rather contains a defect of will (*Wilsgebreken*) that directly impacts the legal validity of the transaction.

Social engineering is carried out through systematic steps, namely gathering information about the victim, grooming (building false trust by claiming there is a threat to the account or that the account will be blocked), and then providing instructions that encourage the victim to authorize the transaction. Perpetrators generally engage in impersonation, posing as bank employees or authorized officials with convincing visual identities and communication styles. Legally, this series of steps constitutes fraud under Article 1328 of the Civil Code; there is a systematic and premeditated deception that causes the victim

to give consent they would not have given had they known the true circumstances.

Various social engineering tactics, such as phishing, smishing, vishing, and impersonation, share a fundamental legal commonality. They all work by creating a state of deception (*dwaling*) or fraud (*bedrog*) in the victim.[13] When a customer provides an OTP code to a perpetrator posing as a bank employee because they believe their account is in danger, the customer is in a state of *dwaling* regarding the identity and legitimacy of the party communicating with them, a substantive error that, according to Article 1321 of the Civil Code, invalidates the validity of the intent formed therefrom.[14] Thus, even though technically the bank's system records the transaction as authorized, legally the underlying consent is defective.

The conventional banking paradigm, which equates the success of technical authentication with the validity of legal consent, overlooks the fact that in cases of social engineering, such authorization arises from psychological manipulation that substantially infringes upon the customer's free will (*Vrije Wil*), thereby creating a dichotomy between technical validity and legal validity that has yet to receive an adequate normative response. This disparity is further exacerbated by a fault-based liability structure that places the customer, who lacks access to audit logs, system forensic data, or authentication records, in the position of bearing the heaviest burden of proof. Therefore, further legal analysis is needed regarding the validity of such transactions through the construction of *Wilsgebreken*, as well as a reconceptualization of

[13] Satria Sukananda and Wahyu Adi Mudiparwanto, "Mengandung Cacat Kehendak Berupa Kesesatan Atau Kekhilafan (Dwaling) Di Dalam Sistem Hukum Indonesia," *Justitia Jurnal Hukum* 4, no. 1 (2020): 166–83.

[14] Gede Bagus Prema Cahya Sani Putra, Komang Febrinayanti Dantes, and I Gusti Ayu Apsari Hadi, "Pembatalan Perjanjian Karena Cacat Kehendak Ditinjau Dari KUH Perdata," *Jurnal Pacta Sunt Servanda* 7, no. 1 (2026): 24–36.

evidentiary mechanisms that are more proportionate to the asymmetric characteristics of digital banking disputes.[15]

In the context of digital banking, as the party that designs, controls, and reaps the greatest benefits from the digitization of financial services, banks should, in principle, bear greater responsibility for the risks arising from the digital systems they have built themselves. Unlike fault liability, which requires proof of fault, strict liability places direct liability on the bank without relying on proof of negligence, an approach that is proportionate given the disparity in technical capabilities and information access between banks and customers.

In digital banking transactions, banks have proven to be the "cheapest cost avoider"; they have exclusive access to behavioral analytics, machine learning-based fraud detection, device fingerprinting, continuous authentication, and real-time anomaly detection, which enable the rapid and accurate identification of abnormal transactions. These detection capabilities, which ordinary customers do not possess at all, position banks as the most efficient party in preventing losses resulting from social engineering. Therefore, according to the Cheapest Cost Avoider doctrine, the risk of losses resulting from OTP fraud should be borne more proportionally by the bank than by the customer.

In addition to being examined from a legal-economic perspective, the reconceptualization of bank liability can also be analyzed through the doctrine of fiduciary duty. In modern banking law, the relationship between a bank and its customers can no longer be viewed merely as a standard contractual relationship between a debtor and a creditor. Digitalization has created a far more complex

[15] Chrisintia Sitompul, Hasim Purba, and Mahmul Siregar, "Pembatalan Akta Perjanjian Pinjam Meminjam Dan Kuasa Menjual Yang Dibuat Notaris Karena Alasan Adanya Cacat Kehendak (Analisis Putusan Mahkamah Agung Nomor 2828 K/PDT/2017)," *Jurnal Hukum Lex Generalis* 6, no. 4 (2025): 1–30.

relationship of trust and confidence. Modern banks not only hold customer funds but also collect, process, and analyze massive amounts of customer behavioral data through algorithmic systems and artificial intelligence. This mastery of data and technology places banks in a dominant position that gives rise to fiduciary duties toward customers.

Under the framework of fiduciary duty, banks have an obligation to act with a high standard of care to protect the interests of their customers. This obligation is not limited to providing transaction systems, but also includes the obligation to:

a. protecting customers from foreseeable fraud risks;
b. issue warnings regarding suspicious activity;
c. monitoring abnormal transaction patterns; and
d. taking active steps to prevent losses.

With the advancement of AI and big data analytics, banks' due diligence standards have become increasingly stringent as their detection capabilities have also improved. When banks allow highly unusual transactions to proceed without additional verification, such failures can be viewed as a breach of the duty of care and duty to protect inherent in the fiduciary relationship between the bank and its customers.

The following table illustrates the application of these three frameworks in the context of social engineering-based OTP fraud, using the 2023 BSI system outage as a concrete reference case.

TABLE 1. The Relevance of the 2023 BSI System Outage Case to the Reconceptualization of Bank Liability in Digital Banking.[16]

ANALYSIS VARIABLES	FINDINGS IN THE 2023 BSI CASE	LEGAL IMPLICATIONS
DIGITAL SYSTEM SECURITY	Disruptions to electronic banking services that affect customer's ability to conduct transactions.	This demonstrates that cyber risks are an inherent part of digital banking operations.
SOCIAL ENGINEERING RISKS	System disruptions and data security issues could potentially be exploited by cybercriminals to carry out phishing, impersonation, and OTP fraud.	Customers face the risk of psychological manipulation, which is difficult to identify on their own.
Wilsgebreken (Defect of Consent)	Customers may take action or grant authorization based on misleading information.	A contract entered into as a result of fraud (*bedrog*) or mistake (*dwaling*) may lose its legal validity.
Fault Liability	Liability is generally imposed on the customer if the transaction is conducted using valid authentication.	This approach risks overlooking the existence of psychological manipulation that

[16] Nadya Ananda Efendi, Muhammad Ikhsan Harahap, and Muhammad Syahbudi, "PENGARUH SOCIAL ENGINEERING DAN CYBER CRIME TERHADAP PERSEPSI KEAMANAN PADA APLIKASI BSI MOBILE," *Manajemen Terapan Dan Keuangan (Mankeu)* 14, no. 03 (2025): 1237–50.

ANALYSIS VARIABLES	FINDINGS IN THE 2023 BSI CASE	LEGAL IMPLICATIONS
		influences customers' decisions.
Cheapest Cost Avoider (CCA)	The bank has access to security technology, transaction monitoring, and fraud detection systems.	Risk is more appropriately allocated to the party with the greatest ability to prevent losses.
Fiduciary Duty	The bank manages customer funds, data, and transaction activities within a digital system under its control.	This gives rise to a higher duty to protect and a higher duty of care.
Strict Liability	Losses arise in the digital ecosystem designed and operated by banks.	Serves as a legal basis for expanding the bank's liability without requiring prior proof of fault.
Research Relevance	The BSI case highlights the connection between cyber risks, social engineering, and customer protection.	Supporting the need to redefine the bank's liability in digital banking transactions.

Source: PT Bank Syariah Indonesia Tbk. (2023). *Official Statement Regarding the BSI Service Outage*. CNBC Indonesia. (2023). *Timeline of the Bank Syariah Indonesia (BSI) System Outage*.

The analysis above establishes that the structural conditions for strict liability are satisfied; the following subsection addresses the corresponding reconstruction of the burden of proof mechanism.

2. Reconstructing the Mechanism of the Shift in the Burden of Proof (*Omkering Van de Bewijslast*) for Digital Banking Transactions Involving Defects of Consent (*Wilsgebreken*) in Order to Realize the Principle of Equality of Arms in Civil Procedure Law

The legal basis for the burden of proof reversal is found in Article 66 of Law No. 8 of 2010 on Money Laundering and Article 28 of Law No. 8 of 1999 on Consumer Protection, as well as, by way of comparison, in Article 150 of the Dutch Code of Civil Procedure (Rv) of the Netherlands, which permits the shifting of the burden of proof based on the principles of reasonableness and fairness. In OTP fraud disputes, the principle of *Actori Incumbit Probatio* (Article 163 of the HIR and Article 1865 of the Civil Code) creates a structural imbalance: the aggrieved customer is required to prove their claim for damages, even though all audit logs, authentication records, and system forensic data are entirely under the exclusive control of the bank as the defendant. This situation renders the principle of *Actori Incumbit Probatio* no longer a tool of justice, but rather a normative barrier preventing customers from obtaining effective legal protection.

Transactions resulting from social engineering-based OTP fraud are substantively flawed in terms of intent (*Wilsgebreken*) because they do not stem from the customer's free will (*Vrije Wil*). The condition of error or deception committed by the perpetrator is the root cause of the formation of this seemingly outward "consent".[17] Valid technical

[17] Arrodli et al., "Konsekuensi Hukum Cacat Kehendak Dalam Pembentukan Perjanjian Berdasarkan Pasal 1320 Kitab Undang-Undang Hukum Perdata."

authentication does not prove the existence of the customer's free will in the context of *Wilsgebreken*; this is the fundamental justification for reconstructing the mechanism of proof.

The reconstruction of the burden of proof reversal mechanism in disputes over digital banking transactions involving defects of consent can be established through three sequential and mutually reinforcing stages. The first stage relies on the customer's obligation to meet the prima facie threshold. At this stage, the customer is not required to fully prove all elements of the defect of consent, but rather need only demonstrate cumulatively two things: that the disputed transaction did in fact occur, and that there is a reasonable indication of a defect in the formation of consent. This standard of proof is consistent with the concept of presumption (*Vermoeden*) as a form of circumstantial evidence recognized in Article 1866 of the Civil Code and Article 164 of the HIR.

Once this *Prima Facie* threshold has been met, the burden of proof shifts to the bank; this is the essence of the second stage, namely the Reverse Burden of Proof mechanism. The bank is obligated to prove the technical integrity of all stages of the transaction, the compliance of authentication procedures with applicable banking due diligence standards, and the absence of anomalies in the system logs. This framework is grounded in Article 28 of the Consumer Protection Law, which places the burden of proof on business entities, and Article 66 of the Anti-Money Laundering Law, which applies the reversal of the burden of proof to protect parties who are in a weaker informational position.

The third stage positions the judge not merely as an assessor of the formal authenticity of electronic evidence, but as a substantive examiner of the material truth of the case. The study's findings indicate that the mechanism of the shifted burden of proof in digital banking disputes involving defects of consent still faces various normative and

technical obstacles. Therefore, a restructuring is required, including affirming the shifting of the burden of proof to the bank if there are indications of defects of consent, strengthening regulations on electronic evidence, and harmonizing cross-sectoral rules among the OJK, BI, Kominfo, and the judiciary.

A. Defects of Consent (*Wilsgebreken*) as the Legal Foundation for the Reconstruction of Evidence

In the context of digital banking transactions manipulated through social engineering, customers provide OTP codes or mobile banking access not of their own free will, but as a result of systematic psychological manipulation that exploits their trust in financial institutions. This pattern substantially fulfills the elements of fraud as referred to in Article 1328 of the Civil Code, namely the existence of deceit that causes another party to give an agreement that they would not have given had there been no fraud.[18] In some cases, the element of *dwaling* (deception or error) is also present because the customer is under the mistaken belief that the perpetrator is an official bank representative.

Thus, if a transaction resulting from OTP fraud is viewed through the lens of *Wilsgebreken*, the bank cannot simply argue that the transaction is valid merely because technical authentication was successfully completed. Valid technical authentication does not in and of itself prove the customer's free will. From this perspective, the burden of proving that a transaction was carried out based on valid free will should shift to the bank, rather than being placed on the customer who is the victim of manipulation. This is the fundamental point underlying the reconstruction of the reverse burden of proof mechanism in digital banking disputes.

[18] "Kitab Undang-Undang Hukum Perdata" (n.d.).

B. Theoretical Basis for the Reversal of the Burden of Proof (*Omkering Van de Bewijslast*)

The reversal of the burden of proof (*Omkering Van de Bewijslast*) is a legal mechanism that shifts the burden of proof from the party making the claim to the party disputing it.[19] This mechanism does not fundamentally conflict with the principle that the burden of proof lies with the party making the claim; rather, it constitutes an exception specifically justified by certain circumstances in which the application of the general principle would actually result in injustice.

In civil procedure law, the reversal of the burden of proof has essentially been recognized as an instrument of procedural justice. Article 163 of the HIR and Article 1865 of the Civil Code do indeed place the burden of proof on the party making the claim, but the jurisprudence of the Supreme Court has consistently recognized that judges have judicial discretion to distribute the burden of proof proportionally among the disputing parties based on considerations of justice.[20] This judicial discretion serves as a gateway to the application of the burden of proof reversal in civil disputes characterized by significant information asymmetry.

The theoretical justification for the reversal of the burden of proof in the context of consumer disputes has, in fact, been recognized within the Indonesian legal system. Article 28 of Law No. 8 of 1999 on Consumer Protection explicitly stipulates that the burden of proof regarding the existence or absence of fault in claims for damages rests with the business operator, not with the

[19] Arrodli et al., "Konsekuensi Hukum Cacat Kehendak Dalam Pembentukan Perjanjian Berdasarkan Pasal 1320 Kitab Undang-Undang Hukum Perdata."

[20] Sibarani, "Penerapan Omkering Van Bewijslast Dalam Pembuktian Tindak Pidana Korupsi Indonesia."

consumer.[21] This provision affirms that, in the asymmetrical legal relationship between professional service providers and consumers, the reversal of the burden of proof is a legal policy choice that has gained normative standing within the national legal system.

Furthermore, POJK No. 22 of 2023 on Consumer Protection in the Financial Services Sector strengthens the position of customers in disputes with financial services providers. This regulation requires financial services providers to ensure the security of their information systems and cybersecurity in the provision of digital services. The bank's legal obligation regarding the security of such systems forms the basis for the argument that, in disputes involving digital fraud, the bank should bear the burden of proving that its security systems were functioning properly, rather than shifting the burden of proving system failure onto the customer.

C. The Principle of Equality of Arms as a Parameter of Procedural Justice in Digital Banking Disputes

The principle of equality of arms is a fundamental principle of procedural law that requires the parties in a judicial proceeding to have equal opportunities to present, defend, and challenge evidence.[22] This principle not only requires formal equality in the opportunity to speak during a trial, but also demands substantive balance in the ability to access and use relevant evidence. In the context of Indonesian civil procedure law, this principle is closely linked to the principle of *Audi et Alteram Partem* and the judge's

[21] Mardi Candra, "Asas Pembuktian Terbalik Dalam Sengketa Penjaminan Pengembalian Modal Pembiayaan," *Mimbar Hukum Universitas Gadjah Mada* 34, no. 1 (2022): 237–59.

[22] Otoritas Jasa Keuangan Republik Indonesia, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22 Tahun 2023 Tentang Pelindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan" (2023).

obligation to maintain a balance between the rights and obligations of the parties during the trial.[23]

In disputes involving OTP fraud in digital banking, the principle of equality of arms is clearly violated if conventional rules of evidence are applied rigidly. The customer, as the plaintiff, is pitted against the bank, which exclusively controls all relevant evidence infrastructure: system audit logs, access logs for new devices, transaction timestamps, geolocation data, authentication failure logs, and reports from the suspicious activity detection system.[24] Meanwhile, customers who are in fact victims of psychological manipulation have access only to peripheral evidence such as screenshots of communications, phone records, or subjective accounts of the sequence of events. This imbalance in access to evidence means that civil trials are not a balanced arena for seeking the truth, but rather a formal mechanism that structurally favors the bank.

This disparity is actually exacerbated by the technical nature of the evidence required. To prove that a bank failed to detect a suspicious transaction, a login from a new device, or an abnormal change in transaction patterns, customers need a deep understanding of encryption standards, access management systems, fraud detection architecture, and internal banking audit procedures.[25] Such technical expertise is clearly far beyond the reach of the average bank customer. Thus, maintaining the conventional system of evidence in such disputes amounts to allowing the

[23] Dwi Handayani, "Implikasi Hukum Penerapan Asas Keseimbangan Pihak-Pihak Dalam Persidangan Perkara Perdata," *Unes Law Review* 6, no. 3 (2024): 8694–8710.

[24] Misnar Syam, "Politik Hukum Pembuktian Dalam Penyelesaian Sengketa Konsumen Di Indonesia," *Unes Law Review* 6, no. 1 (2023): 1497–1509.

[25] Muamar Azmar Mahmud Farig, "Penerapan Asas Equality Of Arms Dalam Pembuktian Kebocoran Data Pribadi," SUARA BSDK, 2026, https://suarabsdk.com/penerapan-asas-equality-of-arms-dalam-pembuktian-kebocoran-data-pribadi/.

principle of equality of arms to remain a principle that is formally recognized but substantively violated.

A reform of the reverse burden of proof mechanism is essential to ensure the principle of equality of arms in the resolution of digital banking disputes involving defects of consent (*Wilsgebreken*). These efforts must include shifting the burden of proof to the bank if there are indications of *Wilsgebreken*, strengthening standards for electronic evidence, increasing public education on consumer rights, and harmonizing cross-sector regulations among the OJK, BI, Kominfo, and the judiciary.[26]

D. Reconstructing the Burden of Proof in Digital Banking Disputes

The proposed reconstruction divides the burden of proof into three layers. First, the burden of proving the occurrence of fraud and resulting losses remains with the customer, consistent with *Actori Incumbit Probatio*: the customer must demonstrate the existence of unauthorized transaction reports, the communication chronology leading to the fraud, and evidence indicating psychological manipulation. Second, once this initial burden is met, the burden shifts to the bank to prove that its digital security systems operated in accordance with required standards, that suspicious transaction detection functioned properly, and that the bank discharged its duty of care in protecting the customer from digital fraud risk.[27]

Third, if the bank argues that the loss occurred solely due to the customer's negligence, the bank is obligated to substantiate that

[26] Fauziah Lubis et al., "Kajian Asas-Asas Equality Before The Law Dalam Praktik Peradilan Perdata," *Journal of Social Science Research* 5, no. 3 (2025).

[27] Ahdan Ramdani, "Pasal 122 Herziene Indonesisch Reglement: Prinsip Due Process of Law Dan Audi et Alteram Partem," Lawyer Ahdan Ramdani, 2026, https://www.lawyer-ahdanramdani.com/pasal-122-herziene-indonesisch-reglement-prinsip-due-process-of-law-dan-audi-et-alteram-partem/.

claim with concrete evidence through digital forensic data in its possession. The bank's denial of liability on the grounds that the transaction used valid authentication cannot be accepted as sufficient proof, because valid authentication does not, technically speaking, prove the existence of the customer's free will in the context of *Wilsgebreken*.

In this context, access to audit logs and digital forensic data is a key issue. The proposed reconstruction requires banks to have a disclosure obligation regarding relevant technical data to the court and customers during the trial process. This obligation could be based on an expanded interpretation of POJK 22/2023, which mandates transparency and accountability of financial service providers to consumers.[28] Without a mechanism for accessing this digital evidence, the reversal of the burden of proof would lose its practical significance, as banks could easily evade their burden of proof simply by refusing to disclose the data in their possession.

Conclusion

This study confirms that transactions resulting from psychological manipulation based on social engineering substantively involve a defect of consent (wilsgebreken) under Article 1321 of the Civil Code, such that their legal validity remains questionable even if technical authentication requirements are satisfied. This situation simultaneously demonstrates that the fault liability paradigm is no longer adequate to address the complexities of digital banking risks. Based on the Cheapest Cost Avoider (CCA) doctrine and fiduciary duty, the reconceptualization of bank liability toward strict

[28] Shifa Arifatunnisa and Sidi Ahyar Wiraguna, "Kedudukan Bukti Elektronik Dalam Pembuktian Perkara Perdata Pasca Penerapan Peradilan Digital," *Media Hukum Indonesia (MHI)* 4, no. 1 (2025): 365–74.

liability is a normative necessity, given that banks are the parties best positioned to prevent losses due to their control over security systems, fraud detection technology, and the entire digital transaction infrastructure. Regarding the burden of proof, the rigid application of the "actori incumbit probatio" principle places customers in a structurally unequal position, as all technical evidence and forensic data are under the bank's exclusive control; a restructuring through a three-tier burden-shifting model, in which the customer need only meet a prima facie threshold, the burden shifts to the bank to prove system integrity and compliance with the duty of care, and the judge conducts a substantive assessment of material truth, serves as a proportional solution to realize the principle of equality of arms, with regulatory harmonization among the OJK, Bank Indonesia, and the judiciary as a prerequisite for its implementation.

References

Admadja, Wilhemina Setia, Gavra Datadavie Ginting, and Maheswari Queena Dewani. "Fault-Based Liability Vs . Strict Liability : Comparative Study of the Concept of Unlawful Acts Indonesia – Japan." *Journal of Social Research* 4, no. 11 (2025): 2973–83.

Arifatunnisa, Shifa, and Sidi Ahyar Wiraguna. "Kedudukan Bukti Elektronik Dalam Pembuktian Perkara Perdata Pasca Penerapan Peradilan Digital." *Media Hukum Indonesia (MHI)* 4, no. 1 (2025): 365–74.

Arrodli, Ahmad Jalaludin, Andika Ramadhan, Anggita, Denis Zakia Muhammad, and Depi Dwi Pamungkas. "Konsekuensi Hukum Cacat Kehendak Dalam Pembentukan Perjanjian Berdasarkan Pasal 1320 Kitab Undang-Undang Hukum Perdata." *LETTERLIJK: JURNAL HUKUM PERDATA* 1, no. 2 (2024).

Aziz, Muhammad Faisal, and Sepriyadi Adhan S. "Perlindungan Hukum Terhadap Nasabah Atas Penyalahgunaan Data Pribadi Oleh Pihak Bank Di Era Digitalisasi Perbankan." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 3, no. 6 (2025): 8840–52.

Candra, Mardi. "Asas Pembuktian Terbalik Dalam Sengketa Penjaminan Pengembalian Modal Pembiayaan." *Mimbar Hukum Universitas Gadjah Mada* 34, no. 1 (2022): 237–59.

Efendi, Nadya Ananda, Muhammad Ikhsan Harahap, and Muhammad Syahbudi. "PENGARUH SOCIAL ENGINEERING DAN CYBER CRIME TERHADAP PERSEPSI KEAMANAN PADA APLIKASI BSI

MOBILE." *Manajemen Terapan Dan Keuangan (Mankeu)* 14, no. 03 (2025): 1237–50.
Fajarpos. "Indonesia Peringkat Kedua Terendah Global Fraud Index 2025, Komdigi Ungkap 70% Kasus Didominasi Social Engineering." Fajarpos Network, 2026. https://www.fajarpos.com/16/02/2026/indonesia-peringkat-kedua-terendah-global-fraud-index-2025-komdigi-ungkap-70-kasus-didominasi-social-engineering/.
Farig, Muamar Azmar Mahmud. "Penerapan Asas Equality Of Arms Dalam Pembuktian Kebocoran Data Pribadi." SUARA BSDK, 2026. https://suarabsdk.com/penerapan-asas-equality-of-arms-dalam-pembuktian-kebocoran-data-pribadi/.
Handayani, Dwi. "Implikasi Hukum Penerapan Asas Keseimbangan Pihak-Pihak Dalam Persidangan Perkara Perdata." *Unes Law Review* 6, no. 3 (2024): 8694–8710.
Hasanudin, Tias Aprilia. "JAWAB BANK DALAM PENANGGULANGAN KEJAHATAN DIGITAL BERBASIS SOCIAL ENGINEERING : ANALISIS HUKUM PERBANKAN." *Indonesia of Journal Business Law* 5, no. 1 (2026): 99–115. https://doi.org/10.47709/ijbl.v5i1.7476.
Indonesia, Otoritas Jasa Keuangan Republik. Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22 Tahun 2023 Tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan (2023).
Jackson, G. "Banks, Automatic Cross-Border Exchange of Taxpayer Information and English Common Law Fiduciary Duties Owed to Customers." *Bulletin for International Taxation* 77 (2023). https://doi.org/10.59403/2nyp97p.
Kitab Undang-Undang Hukum Perdata (n.d.).
Lubis, Fauziah, Dyna Varissa Indah, Nabilah Putri Ayuni, and Nuur Zayana Purba. "Kajian Asas-Asas Equality Before The Law Dalam Praktik Peradilan Perdata." *Journal of Social Science Research* 5, no. 3 (2025).
Putra, Gede Bagus Prema Cahya Sani, Komang Febrinayanti Dantes, and I Gusti Ayu Apsari Hadi. "Pembatalan Perjanjian Karena Cacat Kehendak Ditinjau Dari KUH Perdata." *Jurnal Pacta Sunt Servanda* 7, no. 1 (2026): 24–36.
Putri, Mayang Dias. "Analisis Tanggung Gugat Bank Atas Perbuatan Melawan Hukum Pegawai Bank Yang Merugikan Nasabah (Studi Kasus Putusan Mahkamah Agung Nomor 2600 K / Pdt / 2022)." *Lex Patrimonium* 3, no. 2 (2024).
Ramdani, Ahdan. "Pasal 122 Herziene Indonesisch Reglement: Prinsip Due Process of Law Dan Audi et Alteram Partem." Lawyer Ahdan Ramdani, 2026. https://www.lawyer-ahdanramdani.com/pasal-122-herziene-indonesisch-reglement-prinsip-due-process-of-law-dan-audi-et-alteram-partem/.
Respati, Agustinus Rangga, and Erlangga Djumena. "99 Persen Kasus Penipuan Perbankan Di Indonesia Karena 'Social Engineering.'" Kompas.com, 2023. https://money.kompas.com/read/2023/08/03/161100126/99-

persen-kasus-penipuan-perbankan-di-indonesia-karena-social-engineering-.

Rizki, Mochamad Januar. "4 Modus Kejahatan 'Social Engineering' Dan Tanggung Jawab Perbankan." HUKUMONLINE.COM, 2022. https://www.hukumonline.com/berita/a/4-modus-kejahatan-social-engineering-dan-tanggung-jawab-perbankan-lt62ac38ff8cd0b/.

Sibarani, Mery R.L. "Penerapan Omkering Van Bewijslast Dalam Pembuktian Tindak Pidana Korupsi Indonesia." *Honeste Vivere Journal* 6, no. 2 (2023): 151–60.

Sitompul, Chrisintia, Hasim Purba, and Mahmul Siregar. "Pembatalan Akta Perjanjian Pinjam Meminjam Dan Kuasa Menjual Yang Dibuat Notaris Karena Alasan Adanya Cacat Kehendak (Analisis Putusan Mahkamah Agung Nomor 2828 K/PDT/2017)." *Jurnal Hukum Lex Generalis* 6, no. 4 (2025): 1–30.

Soroinda, Disriani Latifah. "Jurnal Hukum & Pembangunan Kekuatan Pembuktian Alat Bukti Elektronik Dalam Hukum Acara Perdata." *Jurnal Hukum Dan Pembangunan* 52, no. 2 (2022).

Sukananda, Satria, and Wahyu Adi Mudiparwanto. "Mengandung Cacat Kehendak Berupa Kesesatan Atau Kekhilafan (Dwaling) Di Dalam Sistem Hukum Indonesia." *Justitia Jurnal Hukum* 4, no. 1 (2020): 166–83.

Syam, Misnar. "Politik Hukum Pembuktian Dalam Penyelesaian Sengketa Konsumen Di Indonesia." *Unes Law Review* 6, no. 1 (2023): 1497–1509.

Utami, Galuh Candra, and Sidi Ahyar Wiraguna. "Pembuktian Digital Dalam Sengketa Perdata : Menguji Validitas Formil Dan Materiil Dokumen Elektronik Di Era Modern." *Jurnal Hukum Perdata Dan Pidana* 2, no. 4 (2025): 40–52.