

Reconstructing the Civil Liability of Banks for Social Engineering Fraud in Indonesia's Digital Banking Ecosystem: Vitiating Consent, Duty of Care and Risk-Based Loss Allocation

Velliana Tanaya*, Fitra Suanadia

Universitas Pelita Harapan, Indonesia

DOI: <https://doi.org/10.47772/IJRISS.2026.100800654>

Received: 26 August 2026; Accepted: 31 August 2026; Published: 15 September 2026

ABSTRACT

The migration of Indonesian banking into fully digital channels has been accompanied by an escalation of social engineering fraud, in which offenders manipulate account holders into authorising transfers that are technically valid but substantively involuntary. Indonesian positive law lacks a specific and integrated rule allocating the resulting loss: several components of a solution exist in consumer, anti-money-laundering and banking law, but no norm joins them for the socially engineered yet authenticated transaction. In that gap, banks rely on the validity of the one-time password (OTP) or PIN and on standard-form exoneration clauses to place the entire burden on the customer, whose bargaining position and evidentiary access are structurally inferior. This article asks whether the doctrine of vitiating consent (*wilsgebreken*) can qualify a manipulated transfer instruction as a legally defective expression of will, and how the duty of care doctrine should be expanded to reallocate the bank's civil liability. The study applies normative legal research combining statutory, conceptual and case approaches, supported by semi-structured interviews with a bank legal division head and a legal academic, and analysed through deductive legal syllogism. The findings are threefold. First, an instruction produced by social engineering materially satisfies the elements of mistake (*dwaling*, Article 1322 of the Civil Code) and fraud (*bedrog*, Article 1328), so that authentication verifies identity but not will. Second, the standard applicable to a bank as a professional electronic system operator already encompasses behavioural anomaly detection, because Articles 18(2) and 26 of Law No. 8 of 2010 require that capability for anti-money-laundering purposes; failure to deploy it for the customer's protection is an omission actionable under Articles 1365 and 1366. Third, Article 28 of the Consumer Protection Law already reverses the burden of proving fault, and needs application rather than creation. The article proposes a bounded risk-based liability model with a rebuttable presumption against the bank, a safe harbour and proportionate loss sharing, benchmarked against the United Kingdom's mandatory reimbursement scheme and Singapore's Shared Responsibility Framework.

Keywords: digital banking; social engineering; duty of care; vitiating consent (*wilsgebreken*); risk-based liability

INTRODUCTION

Indonesian banking has completed a structural migration from branch-based intermediation to a fully digital service architecture. Mobile banking applications, open application programming interfaces and cloud-hosted core systems have collapsed the physical distance between the customer and the institution, and in doing so have relocated the point of vulnerability [1]. Where the classical risks of banking were mechanical and internal, such as forged instruments, teller error, system downtime, the dominant risk in the contemporary ecosystem is behavioural and external. The offender no longer breaches the bank's technical perimeter. The offender persuades the account holder to open it [2].

Social engineering describes this family of fraud. Its operational forms vary such as impersonation of a bank officer by telephone or messaging application, fabricated notification of a service fee, a counterfeit application package distributed as a wedding invitation or delivery receipt, an urgent instruction to "secure" an account

against a supposed unauthorised transaction, but the structure is constant. The offender constructs a false situation, induces urgency, and directs the victim to perform the authorisation himself. The output is a transfer instruction bearing a valid PIN or OTP which, at the level of the transaction log, is indistinguishable from a genuine instruction [3].

The legal problem arises from that indistinguishability. Indonesian positive law lacks a specific and integrated rule allocating the loss produced by a socially engineered but authenticated transaction; as Part IV demonstrates, several necessary components of such a rule already exist in consumer, anti-money-laundering and banking law, but no instrument joins them. Law No. 7 of 1992 on Banking, as amended by Law No. 10 of 1998, was drafted for an environment of physical intermediation and does not contemplate third-party psychological manipulation as a risk category.

Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 and, most recently, by Law No. 1 of 2024, legitimises electronic signatures and authentication codes as proof of the identity of the sender, but says nothing about the integrity of the will standing behind them. The second amendment refined the regime governing electronic evidence, electronic certification and digital identity, including the new Article 13A, and in doing so strengthened the attribution function of authentication; it did not alter the statute's silence on the quality of the will expressed through an authenticated instruction. The technical regulations of the Financial Services Authority (Otoritas Jasa Keuangan, OJK) address prudential supervision, consumer complaint handling and information security, but they do not resolve the private law question of who bears a loss when an authenticated instruction turns out to be a manipulated one [4].

That vacuum is filled contractually, and it is filled in one direction. Standard-form account opening terms and mobile banking terms of use contain exoneration clauses under which the customer accepts responsibility for every transaction executed using his credentials, and releases the bank from liability for any consequence of credential disclosure. The clause is presented on a take it or leave it basis to a party who has no realistic alternative to digital banking and no capacity to negotiate [5]. When a dispute arises, the bank invokes the clause and the log; the customer is characterised as negligent; and the analysis ends.

The customer's difficulty is compounded procedurally. Under Article 1865 of the Indonesian Civil Code and Article 163 HIR, a party asserting a right must prove it. A customer alleging that the bank's fraud detection system failed must prove the operation of a system located on the bank's servers, governed by the bank's internal documentation, and protected by the bank's commercial confidentiality. The evidentiary burden is not merely heavy; in most retail cases it is unmeetable, and the value at stake rarely justifies the cost of digital forensic expertise. The result is a recovery rate through civil litigation that is negligible relative to reported losses, at a time when the National Cyber and Crypto Agency and the Indonesian National Police's cyber patrol unit continue to report substantial and rising volumes of online fraud directed at the financial sector [4].

The consequence is a structural mismatch. The bank designs the security architecture, selects the authentication method, sets the transaction limits, controls the detection logic, and captures the efficiency gains of digitalisation. The customer controls none of these and bears all of the residual risk. Whatever else may be said about that allocation, it does not follow from any deliberate legislative choice. It is the by-product of a gap.

Research Questions

This article addresses two questions:

First, how can the doctrine of vitiated consent (*wilsgebreken*) be applied to qualify a transfer instruction produced by social engineering as an agreement that is legally defective in its formation?

Second, how should the limits of a bank's civil liability be expanded through the doctrine of duty of care in order to mitigate the risk of transactions containing an element of social engineering?

Contribution

Indonesian scholarship on digital banking losses has developed along two separate tracks. One track analyses unauthorised transactions, namely skimming, account takeover, system malfunction, in which the customer performed no act at all, and where liability follows relatively straightforwardly from the failure of the bank's system [20], [21]. The other treats social engineering primarily as a criminal law and cybersecurity problem, focused on prosecution and prevention rather than on private loss allocation [22]. Social engineering falls awkwardly between them, because the customer did act, and the act was formally valid.

The contribution of this article is to connect three elements that are normally treated in isolation: the classical private law of defective consent; the prudential standard of care owed by a professional operator of an electronic system; and the anti money laundering monitoring duty that Indonesian banks already discharge. The article argues that the third of these supplies the evidentiary bridge that the first two have lacked.

A bank that is statutorily obliged to identify a transaction deviating from a customer's profile for the purpose of protecting the financial system cannot coherently claim to be incapable of identifying the same deviation for the purpose of protecting the customer. The article then converts that doctrinal position into an operational loss allocation model, benchmarked against two jurisdictions that have already adopted one through binding or quasi-binding regulatory instruments.

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

Theory of Legal Protection

Hadjon distinguishes preventive from repressive legal protection [9]. Preventive protection gives the subject an opportunity to raise an objection before a decision becomes definitive; repressive protection provides a remedy after harm has occurred. The distinction is usually applied to administrative decision-making, but it maps onto digital banking with unusual precision, and the mapping carries a normative consequence.

In a social engineering incident, repressive protection is close to worthless. Funds transit a chain of mule accounts within minutes; the customer discovers the loss after the fact; the evidence required to establish the bank's failure sits inside the bank; and the transaction that must be undone has already been settled. Whatever protection the legal order can realistically deliver must therefore be delivered before execution, through the design of the system itself, detection, friction, confirmation, suspension. Preventive protection in this context is not an administrative courtesy. It is the whole of the protection [10].

Theories of Civil Liability

Indonesian civil law offers a spectrum of liability bases. Article 1365 of the Civil Code establishes liability for an unlawful act, requiring an unlawful act, fault, loss and causation. Article 1366 extends liability to loss caused by negligence or want of care, and therefore reaches omissions as well as positive acts. Article 1367 imposes vicarious liability for the acts of persons for whom one is responsible. Article 19 of Law No. 8 of 1999 on Consumer Protection imposes a form of strict liability on business actors for loss arising from defective goods or services [11], [13]. Beyond these, the doctrine of risk-based liability allocates loss to the party that controls the source of risk and derives benefit from the activity generating it, independently of moral fault. Its rationale is not retributive but economic and distributive: the party best placed to prevent the harm, and best placed to absorb and spread the residual cost, should bear it [12]. That party can internalise the cost through pricing, provisioning and insurance, whereas an individual retail customer cannot. This article argues that digital banking fraud is a paradigm case for the doctrine, and that Indonesian law already contains the components required to apply it.

Duty of Care and the Prudent Banking Principle

Article 2 of the Banking Law requires Indonesian banks to conduct their business on the basis of economic democracy and the prudential principle, and Article 29(2) requires them to maintain soundness in accordance

with capital adequacy, asset quality, management quality, liquidity and solvency. In practice the prudential principle has been read as a solvency concept, concerned with credit and liquidity risk [1]. Sjahdeini argues that in a technology-mediated environment this reading is too narrow: a bank operating an electronic banking system owes an obligation to provide information technology governance that is secure in a holistic sense, encompassing network infrastructure, data integrity and application-level protection [7].

Comparative scholarship reaches the same destination from the direction of the common law duty of care. Savitri observes that in several jurisdictions the professional standard applicable to a bank offering digital services has moved beyond the delivery of a functioning system towards an obligation to monitor, to query irregular instructions and to intervene where the pattern of a transaction is inconsistent with the customer's established behaviour [8]. The standard is dynamic: it tracks the state of available technology and the evolving *modus operandi* of offenders, rather than remaining fixed at whatever the regulatory floor happened to be when the product was launched.

Vitiated Consent in Indonesian Contract Law

Article 1320 of the Civil Code sets out four cumulative conditions for a valid agreement: consent, capacity, a determinate subject matter and a lawful cause. Article 1321 provides that no valid consent exists where consent was given by mistake, or obtained by duress or fraud [15], [16].

Mistake (*dwaling*) under Article 1322 vitiates consent where the error concerns the essential quality of the subject matter of the agreement, or the identity of the person with whom the party intended to contract in cases where that identity was the determining reason for entering into it. Fraud (*bedrog*) under Article 1328 vitiates consent where one party has employed artifice and a series of falsehoods of such a nature that, without them, the other party would not have entered into the agreement; fraud is not presumed and must be proved [17], [18].

Indonesian doctrine and case law recognise a fourth, non-codified ground, the abuse of circumstances (*misbruik van omstandigheden*), which addresses the exploitation of a party's economic or psychological vulnerability by a counterparty holding superior knowledge or position [19].

The consequence of vitiated consent is annulment rather than nullity. The agreement is voidable at the instance of the party whose will was defective, in contrast to the absolute nullity that follows from the absence of an objective condition [16].

Research Gap

Prior Indonesian studies have examined the bank's liability for skimming [20], for system failure in mobile banking [21], for personal data leakage [6], and for banking crime in the information technology era from a criminal law perspective [22]. Handayani has considered the position of the bank customer as a consumer in electronic banking transactions [23]. What these studies share is a focus on transactions the customer did not authorise, or on failures internal to the bank.

The harder case has not been systematically theorised. In social engineering the customer did authorise, and the authorisation was formally perfect. Resolving that case requires an argument that operates at two levels simultaneously: a private law argument that the authorisation was not a free expression of will, and a regulatory argument that the bank's failure to interdict was a breach of a standard it was already obliged to meet. This article supplies both and joins them.

RESEARCH METHOD

This study employs normative legal research, which examines law as a system of norms comprising principles, statutory rules and doctrine [24]. Three approaches are combined. The statutory approach analyses the legislation and regulations governing digital banking transactions and consumer protection. The conceptual approach develops the analysis from the doctrines of vitiated consent, duty of care and risk-based liability.

The case approach examines the Indonesian jurisprudence in which the Supreme Court has recognised and applied the doctrines on which the argument depends, in particular the line of decisions receiving the doctrine of abuse of circumstances into Indonesian contract law (Mahkamah Agung Decisions No. 1904 K/Sip/1982, No. 3431 K/Pdt/1985, No. 3641 K/Pdt/2001 and No. 3406 K/Pdt/2019), together with the industry's documented treatment of disputed transactions under the 2023 Bye Laws [25], [26]. Reported Indonesian decisions adjudicating the allocation of social engineering losses specifically remain scarce, and the case approach therefore operates on this adjacent jurisprudence concerning defective consent and on institutional practice, rather than on a body of directly applicable precedent; that constraint is acknowledged in the limitations section.

Legal Materials

Primary legal materials comprise: the Indonesian Civil Code (Burgerlijk Wetboek), in particular Articles 1320, 1321, 1322, 1328, 1338, 1365, 1366, 1367 and 1865; Law No. 7 of 1992 on Banking as amended by Law No. 10 of 1998; Law No. 8 of 1999 on Consumer Protection, in particular Articles 4, 7, 18, 19 and 28; Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 19 of 2016 and by Law No. 1 of 2024; Law No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering, in particular Articles 1(5), 18(2) and 26; Law No. 27 of 2022 on Personal Data Protection; Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, as amended by Law No. 4 of 2026; OJK Regulation No. 22 of 2023 on Consumer and Public Protection in the Financial Services Sector; OJK Regulation No. 44 of 2024 on Bank Secrecy; and the 2023 Interbank By Laws on the Postponement of Fund Transfer Transactions.

Secondary legal materials comprise books, peer-reviewed articles and expert opinion. Tertiary materials comprise legal dictionaries and encyclopaedias.

Supplementary Expert Interviews

To test the doctrinal analysis against operational reality, two semi-structured expert interviews were conducted using purposive sampling. The informants were selected to represent the two perspectives that must be reconciled by any workable reform: Mr Addy E. Widyatmaka, Legal Division Head of PT Bank National Nobu Tbk, representing the operational and compliance perspective of a licensed commercial bank; and Prof. Dr. Fajar Sugianto, S.H., M.H., a legal academic, representing the doctrinal and regulatory perspective. The interviews covered the basis on which banks currently treat an authenticated transaction as valid, the feasibility of detecting manipulated instructions, the appropriate measure of the standard of care, the viability of reversing the burden of proof, and the prospects for regulatory synchronisation.

The interview material is used qualitatively, as a source of expert opinion and industry practice against which the normative argument is examined. It is not used to generate statistical inference, and no claim of empirical generalisability is made on the basis of two informants.

Each interview was conducted on the record and with written informed consent, was recorded and transcribed, and the transcript was verified with the informant concerned. The transcripts were analysed thematically: responses were coded against the five topics listed above and condensed into the propositions reported in Part IV.B [40]. A strict division of labour is maintained between the interview material and the normative analysis. Statements drawn from the interviews are reported in Part IV.B, are attributed expressly to the informant concerned, and are used only as evidence of industry practice and expert opinion. Every doctrinal claim advanced in Parts IV.C to IV.G rests on the legal materials and authorities cited there, and none depends for its validity on the interview evidence.

Analysis

Legal materials were analysed qualitatively using deductive legal syllogism: the applicable norm as major premise, the factual or operational pattern as minor premise, and the legal qualification as conclusion. Where

the norms conflicted or left a gap, the analysis proceeded through legal interpretation and, where necessary, legal construction, in order to formulate the reconstruction proposed in Part IV.

RESULTS AND DISCUSSION

The Regulatory Architecture and Its Blind Spot

Bank secrecy: OJK Regulation No. 44 of 2024

Article 2(1) of OJK Regulation No. 44 of 2024 obliges banks and affiliated parties to keep confidential all information concerning depositor customers and their deposits. Article 3 sets out the exceptions, which include the interests of the judiciary in civil proceedings between a bank and a customer or between customers, the exchange of information between banks, and international mutual legal assistance. Article 7(1) empowers the OJK to issue written authorisation for the disclosure of bank secrecy to law enforcement officers, and Article 7(4) specifies the documents an applicant must supply, including the name of the bank at which the account is held and identifying particulars of the suspect. Article 19(1)(b) obliges a bank's directors to disclose a customer's financial position in civil proceedings on the written request of the court. Article 23(1) permits the exchange of customer information between banks for risk management and crime prevention purposes, while Article 23(6) prohibits the use of that information for commercial purposes such as marketing. Articles 5 and 26 provide for graduated administrative sanctions for unauthorised disclosure.

Analysed against the timeline of a social engineering incident, this architecture reveals a systematic mismatch. The regulation is calibrated for orderly, verified disclosure; the incident is measured in minutes. A victim who telephones the bank within ten minutes of a fraudulent transfer does not know the identity of the beneficiary, and Article 7(4) requires precisely that identity before authorisation to disclose can be sought. A criminal report must be filed, an investigator assigned, an application prepared and forwarded, and central authorisation obtained by which time the funds have passed through several layers of mule accounts. The exception list contains no pathway for emergency asset preservation on the strength of a plausible victim complaint [27].

The result is a protective paradox. A secrecy regime designed to protect the customer operates, in the specific setting of social engineering, to protect the account of the offender. That observation does not argue for the dilution of bank secrecy. It argues that the exception list is incomplete, and that a narrowly drawn exception permitting temporary suspension of a suspected mule account, as distinct from disclosure of its holder's identity, would close the gap without touching the privacy interest the regime exists to defend.

Table 1. Mapping of OJK Regulation No. 44 of 2024 against a duty-of-care reconstruction

Provision	Normative content	Effect in a social engineering incident	Reconstruction
Art. 2(1)	Bank and affiliated parties must keep depositor information confidential.	Prevents the bank from identifying the beneficiary of a mule account to the victim without formal authorisation.	Confidentiality should be applied proportionately, so that it does not shield an account already the subject of a credible fraud report.
Art. 3	Exceptions, including civil proceedings and interbank information exchange.	Disclosure becomes available only once litigation or a criminal investigation is under way.	An emergency exception permitting temporary suspension on a verified victim report, without identity disclosure.

Art. 7(1) and 7(4)	OJK written authorisation for law enforcement; documentary requirements including the target bank and suspect identity.	Requires information the victim cannot supply at the moment when action would still be effective.	A secure, integrated inter-agency channel enabling verification within hours rather than weeks.
Art. 19(1)(b)	Directors must disclose a customer's financial position on written request of the court.	Provides a remedy only through litigation whose cost typically exceeds the individual loss.	Recognition of a duty to preserve the disputed balance pending resolution.
Art. 23(1) and 23(6)	Permits interbank information exchange for risk management; prohibits commercial use.	Enables, but does not require, a shared mule-account register.	Convert the permission into an obligation to participate in a centralised, supervised fraud register.
Arts. 5 and 26	Graduated administrative sanctions for unauthorised disclosure.	Encourages defensive conduct: staff hesitate to act without formal instruction.	A statutory safe harbour for good-faith temporary blocking on a credible report.

Source: authors' analysis of OJK Regulation No. 44 of 2024.

The anti-money-laundering architecture: Law No. 8 of 2010

Article 1(5) of Law No. 8 of 2010 defines a suspicious financial transaction to include a transaction that deviates from the profile, characteristics or usual transaction pattern of the service user concerned. Article 18(2) obliges providers of financial services to apply the know-your-service-user principle. Article 26 permits a provider to postpone a transaction where there are grounds for suspicion [28].

This provision is the analytical fulcrum of the present argument, and it has been consistently overlooked in the Indonesian literature on digital banking liability. Indonesian law already imposes on banks a duty to monitor transactions against a behavioural baseline, and already confers on them the power to halt a transaction unilaterally. The duty is publicly oriented, its object is the integrity of the financial system rather than the protection of any individual depositor, but the technical capability it presupposes is identical to the capability required to interdict a social engineering transfer.

The consequence for the private law analysis is direct. When a bank argues, as the industry informant in this study candidly did, that it cannot detect a manipulated instruction because its systems process technically valid commands and cannot read the customer's psychological state, the argument proves too much. The bank is not being asked to read the customer's mind. It is being asked to notice that an account which has never transferred more than five million rupiah, always to the same three beneficiaries, always from the same device, has just initiated four transfers to newly registered beneficiaries within eleven minutes. That is a pattern-recognition task the bank performs already, under statutory compulsion, for anti-money-laundering purposes. A capability that exists for one purpose cannot be declared non-existent for another.

Self-regulation: the 2023 Interbank By Laws

The Indonesian banking community has adopted a set of By Laws, agreed in 2023, governing the postponement of fund transfer transactions. Article 1(1) characterises postponement as an independent action grounded in Article 26 of Law No. 8 of 2010, taken on the initiative of the receiving bank. Article 5 requires the sending bank promptly to examine the reasonableness of a victim's report before transmitting a request to

hold the balance. Article 8(1) requires the receiving bank to execute the postponement on the same day, provided it is satisfied that the request is valid.

The significance of this instrument for the argument is evidential rather than normative. The industry has already built, voluntarily and at its own expense, the operational capability that the doctrinal case requires: same day interbank suspension on the strength of a victim complaint. Feasibility is therefore not in dispute. What the By Laws lack is enforceability in the direction that matters. They are a horizontal arrangement among banks, not a source of a subjective right in the customer. A bank that fails to act under them owes no private remedy to the victim, and the victim has no standing to insist on performance.

The reform task is accordingly narrower and more tractable than it first appears. It is not to invent a capability, procure a technology or impose an unfamiliar obligation. It is to convert an existing voluntary capability into a legal duty owed to the customer, and to attach a consequence to its breach.

Consumer protection: Law No. 8 of 1999 and OJK Regulation No. 22 of 2023

Article 18(1)(a) of Law No. 8 of 1999 prohibits a business actor from including in a standard-form agreement any clause transferring the business actor's responsibility to the consumer, and Article 18(3) declares any such clause null and void. OJK Regulation No. 22 of 2023, issued pursuant to Law No. 4 of 2023, strengthens the obligations of financial services business actors in relation to consumer data protection, information system security and cyber resilience, and confirms their responsibility for losses arising from the conduct of their employees and of third parties acting on their behalf [13], [14], [31].

The prohibition therefore already exists. It is under-enforced, and the reason is not that courts regard the clause as valid. It is that the clause is largely beside the point. Even where an exoneration clause is set aside, the court must still determine causation, and under the prevailing framing the answer is supplied by the customer's own act: the customer disclosed the OTP, and that disclosure is treated as an independent intervening cause severing the chain between any bank failure and the loss. Striking down the clause does not disturb that reasoning. Only an argument that reaches the characterisation of the customer's act, and the characterisation of the bank's omission, can disturb it. That is the work undertaken in the following two sections.

Table 2. Coverage of the existing regulatory framework and the residual gap

Instrument	What it regulates	What it does not resolve
Banking Law (Law No. 7/1992 as amended by Law No. 10/1998)	Prudential soundness, bank secrecy, supervision.	Allocation of loss where a third party manipulates the customer's will.
ITE Law (Law No. 11/2008 as amended by Law No. 19/2016 and Law No. 1/2024)	Validity and evidential status of electronic transactions and authentication.	Whether an authenticated instruction reflects a genuine will.
Consumer Protection Law (Law No. 8/1999)	Prohibited standard clauses; business actor liability; reversal of the burden of proving fault.	Application to banking disputes, which courts treat as purely contractual.
Anti Money Laundering Law (Law No. 8/2010)	Profile-based transaction monitoring; postponement powers.	Any private right in the customer to the exercise of those powers.

Personal Data Protection Law (Law No. 27/2022)	Obligations of the data controller; breach notification.	Consequence of an upstream leak for downstream transaction liability.
POJK 22/2023 and POJK 44/2024	Consumer protection standards; secrecy and its exceptions.	A loss allocation rule for seemingly authorised transactions.
By Laws 2023	Same-day interbank transaction postponement.	Enforceability by the customer; consequence of non-performance.

Source: authors' analysis.

Expert Perspectives: The Industry and the Academy

The industry perspective

The bank legal division informant located the validity of a digital transaction squarely in the technical code agreed between bank and customer in the terms of use of the mobile banking or electronic transfer service. On that basis, where the confidentiality of an authentication credential has been compromised through the customer's own conduct, the customer bears the transaction. The informant did not, however, assert an unqualified immunity. Liability was accepted without reservation for fraud demonstrated to have occurred within the bank's own system, and strict liability was acknowledged where an employee acts with intent, consistently with the OJK consumer protection regulation.

Three further points from that interview bear directly on the design of any reform. First, the informant posed the operational question openly: how is a bank to detect social engineering within its system, when the instruction originates from the customer's registered device and the customer performs the authorisation voluntarily? Second, the informant identified the systemic risk in an unbounded reversal of the burden of proof, observing that reverse proof in Indonesian law is presently confined to the money laundering and environmental statutes, and warning that automatic reimbursement on the strength of an unverified claim would create moral hazard and destabilise the industry. Third, and notably, the informant identified the interbank By Laws as the most effective instrument available outside formal regulation, precisely because they permit coordinated and immediate action across institutions.

The academic perspective

The academic informant framed the problem as one of integration. A bank offering a product is bound by the Banking Law; the same bank processing customer data is bound by the Personal Data Protection Law; and the interaction between the two regimes is not worked out. Regulatory synchronisation across the ITE Law, the Banking Law, the Consumer Protection Law and the Personal Data Protection Law was identified as the principal structural requirement.

On the measure of the standard of care, the informant preferred the *lex specialis* of OJK regulation over general civil law standards, on the ground that sectoral regulation reaches the technical detail of banking operations and provides an objective benchmark against which compliance can be assessed in court. The informant gave concrete content to the duty, identifying layered verification consisting of a combination of OTP, photographic verification and additional data matching as the kind of protection a bank should deploy. The informant also considered the OJK's consumer protection regulation an appropriate regulatory response, and accepted that risk-based liability could be applied where a bank is shown to have neglected its transaction supervision function.

At the same time, the informant maintained that where a bank has implemented rigorous security procedures and has provided adequate education, a customer who nevertheless discloses personal data to a third party may properly be regarded as having been negligent. That position is the mirror image of the industry's, and it defines the boundary the reconstruction must respect.

Synthesis

The two informants converge on three propositions and diverge on one. They converge in accepting that technical validity currently determines outcomes; that sectoral OJK regulation is the operative source of the applicable standard of care; and that statutory fragmentation across four principal statutes is the structural cause of the uncertainty. They diverge on the burden of proof.

The divergence, examined closely, is narrower than it appears. The industry objection is not to reversal as a matter of principle. It is to an unbounded reversal that would oblige a bank to reimburse on the strength of an unverified assertion, with no defence available and no consumer-conduct exception. That is a legitimate objection, and any reform that ignores it will not survive contact with the sector. It is also an objection that can be met without abandoning the customer, by three devices: a defined safe harbour that discharges the bank on proof of compliance in the specific transaction; a consumer standard of caution that returns the loss to a customer who acted with gross negligence or complicity; and a cap that limits exposure per claim. A reversal so bounded is not a systemic risk. It is an ordinary allocation of an evidentiary burden to the party holding the evidence. The model proposed in Part IV.G is constructed on that basis.

Qualifying Social Engineering as Vitiating Consent

Authentication verifies identity; it does not verify will

The doctrinal error at the centre of current practice is a conflation of two distinct questions. Authentication answers the question: is the person entering this credential the account holder? It does not answer, and is not designed to answer, the question: does the account holder intend this transfer, understanding what it is and to whom it goes? The first is a fact about the channel. The second is a fact about the mind. An OTP is evidence of the former and is silent as to the latter.

Indonesian law does not treat the two as equivalent anywhere else. Article 1320 Indonesia Civil Code requires consent as a substantive condition, and Article 1321 Indonesia Civil Code provides expressly that consent given by mistake or obtained by fraud is not valid consent. A signature on a paper instrument is likewise authentic and yet capable of being set aside where the will it purports to express was defective. There is no principled reason why the electronic equivalent of a signature should carry a greater conclusiveness than the manuscript original. The ITE Law confers evidential status on electronic authentication; it does not, and could not, convert a defective will into a valid one.

Mistake (dwaling) under Article 1322 Indonesia Civil Code

In a typical social engineering incident the victim forms an erroneous representation of two matters. The first is the identity of the counterparty: the victim believes he is dealing with a bank officer, a courier, a tax official or a police investigator, when he is dealing with an offender. The second is the nature and purpose of the act he is performing: the victim believes he is blocking a fraudulent transaction, paying a legitimate service charge, or verifying an account, when he is authorising a transfer of his own funds to a stranger.

Both errors go to the determining reason for the act. The victim would not have entered the credential had he known the true identity of the person requesting it, or the true effect of entering it. Article 1322 Indonesia Civil Code addresses mistake as to the essential quality of the subject matter and as to the person where that person's identity was determinative. Social engineering satisfies both limbs simultaneously, and does so by design: the entire technique consists in the deliberate manufacture of exactly those two errors.

Fraud (bedrog) under Article 1328

Article 1328 Indonesia Civil Code requires artifice and a series of falsehoods of such a character that, without them, the other party would not have contracted. Social engineering is, structurally, a series of falsehoods. The number is spoofed to display the bank's published contact line. The caller adopts an assumed identity and recites genuine personal data obtained from a prior leak in order to establish credibility. A fabricated emergency is introduced. Urgency is manufactured to suppress deliberation and to prevent the victim from verifying through an independent channel. The sequence is scripted, iterative and cumulative. It is difficult to imagine a factual pattern that answers more exactly to the statutory description.

The third-party objection and its answer

An objection must be confronted directly, because it is the strongest argument against the position advanced here and because it is not adequately addressed in the existing literature. Article 1328 Indonesia Civil Code addresses fraud practised by one contracting party upon the other. In social engineering the fraud is practised by a third party. The bank is not the deceiver, and on the face of the provision the customer cannot invoke the bank's fraud in order to annul the mandate.

Three responses are available, and together they are sufficient.

First, the analytical objective is not to annul the underlying account contract between bank and customer. It is to deny that the specific transfer instruction constitutes a valid expression of will capable of authorising the bank to debit the account. The relationship in which the bank executes a transfer is, in substance, one of mandate: the bank acts on the customer's instruction. Where the instruction is materially defective at its source, the question is not whether the contract survives but whether the mandate was validly conferred. It was not.

Second, a bank may of course rely in good faith on an apparently regular instruction, and ordinarily should be protected in doing so; commercial certainty requires it. But good faith is not a formal category. Article 1338(3) of the Indonesia Civil Code requires agreements to be performed in good faith, and good faith in the performance of a payment mandate imports an obligation not to rely mechanically on an instruction the bank had reason to doubt. A bank whose own systems flagged the transaction as anomalous, or would have flagged it had they been operating to the standard the bank applies for anti-money-laundering purposes, is not in the position of an innocent party misled along with the customer. Its reliance is not, in the relevant sense, in good faith at all.

Third, the doctrine of abuse of circumstances supplies an independent route. The manufactured panic in which the victim acts, combined with the pronounced asymmetry of technical expertise between the parties and the absence of any comparison mechanism within the application by which the victim might have tested the claim being made to him, constitutes precisely the exploitation of vulnerability at which the doctrine is aimed.

These three responses are not free-standing authorial construction; each is anchored in recognised authority. The doctrine of abuse of circumstances has been received into Indonesian law through a consistent line of Supreme Court jurisprudence, the Decision No. 1904 K/Sip/1982 of 28 January 1984, Decision No. 3431 K/Pdt/1985 of 4 March 1987 (Sri Setianingsih v. Ny. Boesono and R. Boesono), Decision No. 3641 K/Pdt/2001, and most recently Decision No. 3406 K/Pdt/2019, in which the Court annulled an agreement concluded by an elderly party who was ignorant of its substance and dependent on the counterparty and has been systematised in Indonesian doctrine as an autonomous, non-codified ground of defective will [19], [37]. Those decisions concern exploitation by the counterparty itself; the treatment of a defect procured by a third party is, however, settled in the legal family to which the Indonesian Civil Code belongs. Article 3:44(5) of the present Dutch Civil Code, the modern successor of the provisions from which Articles 1321 to 1328 descend, and a recognised source of doctrinal orientation where the old code is silent [37], provides that a declaration procured by threat, fraud or abuse of circumstances emanating from a third party cannot be avoided against a counterparty who neither knew nor ought to have known of the defect. The converse of that rule states the present argument exactly: against a counterparty who knew, or ought to have known, that the declaration was defectively formed, the defect can be invoked. A bank whose monitoring systems flagged the

instruction as anomalous, or would have flagged it had those systems been operated to the standard the bank already applies for anti-money-laundering purposes, is a counterparty that ought to have known. The third-party character of the deception therefore continues to protect the genuinely innocent bank, as commercial certainty requires but only the genuinely innocent bank.

The practical consequence of qualifying the instruction as defective is therefore not principally the formal remedy of annulment under Article 1454, useful though that may be in an appropriate case. It is that the defect deprives the bank of its central defence that the customer's own free act caused the loss and reopens the causation analysis. Once the customer's act is characterised as a manipulated act rather than a free one, the bank's omission is no longer displaced by an intervening cause. It becomes a concurrent cause, and the question shifts from whether the bank is liable at all to how the loss should be apportioned.

The Expanded Duty of Care of the Digital Bank

If the customer's act is a manipulated act, the analysis turns to the bank's conduct. Article 15 of the ITE Law requires every electronic system operator to operate its system reliably, securely and responsibly. Reliability in that provision cannot sensibly be read as uptime alone. A payment system that executes every syntactically valid instruction without regard to its substantive plausibility is available, but it is not reliable in any sense a depositor would recognise [7], [8].

The content of the expanded duty can be stated in four components, each of which is anchored in an existing Indonesian obligation rather than imported wholesale from another legal system.

Behavioural profiling and anomaly detection

The bank must maintain a behavioural baseline for each account device fingerprint, access location, transaction velocity, typical value, established beneficiaries and must evaluate instructions against it in real time. This is not a novel imposition. Article 1(5) of Law No. 8 of 2010 defines suspicion by reference to deviation from the service user's profile, and Article 18(2) requires the know your service user principle to be applied. The capability is mandated; what is proposed is that its output be used for the depositor's benefit as well as the system's.

Friction proportionate to risk

Where an instruction crosses a defined risk threshold, the system must impose additional verification before execution: step-up authentication, out-of-band confirmation through a channel distinct from the one in use, a short cooling-off period for first transfers to a newly registered beneficiary above a value threshold, or a specific in-application warning naming the scam typology detected. The academic informant in this study identified layered verification of exactly this kind, OTP combined with photographic verification and further data matching as the concrete content of the standard. The design question is calibration, not existence: friction imposed indiscriminately degrades the service, while friction imposed on the small proportion of transactions that deviate materially from the baseline is both tolerable and effective.

Responsiveness after the event

The bank must maintain a reachable reporting channel outside business hours and must act on a plausible victim report the same day, requesting suspension at the receiving institution. The 2023 By Laws establish that this is operationally achievable. What is proposed is that the obligation be owed to the customer and not merely between banks.

Upstream data integrity

A significant proportion of social engineering attempts succeed because the offender opens the conversation with accurate personal data, full name, account number, recent transaction, identity number, which establishes credibility before any request is made. Where that data originated in a leak at the controller, the bank's failure

is upstream of the customer's act, and cannot be answered by pointing at the downstream OTP. Law No. 27 of 2022 imposes the controller's obligations directly [29], [30]. A bank that leaks the material used to deceive its own customer, and then relies on the customer's deception to deny liability, occupies an untenable position.

From public-law monitoring duty to private-law standard of care

The reliance placed on Law No. 8 of 2010 in this argument requires a precise statement of the legal bridge, because a public law obligation does not translate automatically into private liability. The anti money laundering monitoring duty is owed to the state, and its protective purpose is the integrity of the financial system rather than the patrimony of any individual depositor. Under the doctrine of relativity (Schutznorm), which Indonesian scholarship on the unlawful act has received alongside the broad reading of unlawfulness [38], [39], the breach of a statutory duty grounds liability toward a claimant only where the norm breached serves, at least in part, to protect that claimant against the kind of loss suffered. The argument advanced here therefore does not proceed by treating a violation of Article 18(2) as, in itself, an unlawful act toward the customer.

The bridge runs instead through the second limb of the broadened unlawfulness standard received into Article 1365 Indonesia Civil Code: conduct contrary to the care that ought to be observed in society toward another person or property, measured against the conduct of a prudent professional in the defendant's position, possessing the defendant's knowledge and means [38], [39]. On that limb, the anti money laundering architecture is not the source of the duty; it is evidence of its content. What a bank can foreseeably and reasonably do for its depositor is demonstrated by what it already does under statutory compulsion: Article 1(5) and Article 18(2) of Law No. 8 of 2010 establish conclusively that real-time behavioural monitoring against a customer profile lies within the ordinary technical and operational competence of an Indonesian bank, and Article 26, read with the 2023 By Laws, establishes that acting on the output of that monitoring by postponing a transaction is both lawful and routinely practised. A capability the bank exercises daily at its own initiative cannot be characterised as unreasonable, infeasible or unforeseeable when the question becomes what care the same bank owed its own customer in the same transaction stream. Article 1366 Indonesia Civil Code completes the bridge on the side of the conduct, because it extends liability specifically to negligence and want of care, and therefore to the omission, the failure to query, to verify or to suspend, rather than only to a positive act.

Stated as a standard, the resulting duty is bounded in four respects, and the boundaries answer the operational objections fairly raised by the industry informant. First, proportionality: the duty is engaged only by a material deviation from the customer's established profile and its content is graduated friction and enquiry, not a guarantee of interdiction. Second, false positives: a bank that queries or briefly delays a transaction in good faith on defined risk triggers must not thereby incur liability toward the customer for the delay; the safe harbour proposed in Part IV.G gives that protection expressly, because a standard that penalised both inaction and precaution would be incoherent and would drive banks toward indiscriminate friction that degrades the service for all users. Third, operational feasibility: the benchmark is what risk-based monitoring of the kind already mandated would have flagged, assessed ex ante on the information available to the system at the moment of the instruction, not what hindsight reveals after the fraud has been reconstructed. Fourth, the negligence threshold: a failure to detect an anomalous transaction constitutes actionable negligence only where the transaction crossed the bank's own or the regulatory risk thresholds, where a feasible intervention step-up verification, out of band confirmation, a brief postponement was available and omitted, and where that intervention would more probably than not have prevented or reduced the loss. On this standard the bank is not the insurer of every manipulated customer; it answers for the losses that its own mandated vigilance, prudently operated, would have averted.

Breach and its legal characterisation

Failure at any of these levels is actionable. Article 1365 of the Indonesia Civil Code covers unlawful acts, and Indonesian doctrine has long accepted, following the reception of the broad reading of unlawfulness, that an act contrary to the standard of care owed in society is unlawful for this purpose [38], [39]. Article 1366

Indonesia Civil Code extends liability to loss caused by negligence or want of care, and therefore captures omissions specifically the failure to detect, the failure to query, the failure to suspend [11]. Where the failure is a departure from a service standard the bank has itself represented to the market, the same facts also sustain a claim in default of contractual performance.

Two features of the standard should be emphasised. It is dynamic: it tracks the state of available technology and the evolving *modus operandi* of offenders, so that compliance with a regulatory floor set several years earlier is evidence of diligence but is not conclusive of it. And it is internally benchmarked: the standard a bank must meet in protecting its customer is at least the standard it already meets in protecting the financial system from money laundering, because the two tasks draw on the same data and the same detection logic.

Exoneration Clauses and the Case for Risk-Based Liability

Article 18(1)(a) of the Consumer Protection Law prohibits standard clauses transferring the business actor's responsibility to the consumer, and Article 18(3) renders them void. The difficulty, as observed above, is that invalidating the clause does not by itself change the outcome, because the decisive reasoning operates at the level of causation rather than contract. The combined effect of Parts IV.C and IV.D is to dislodge that reasoning: the customer's act is characterised as manipulated rather than free, and the bank's omission is characterised as a concurrent cause rather than a background condition.

What replaces it should be a risk-based allocation. The justification is not that banks are blameworthy. It is that the bank designs the architecture, selects the authentication method, sets the limits, controls the detection logic and captures the efficiency gains of digitalisation, while the customer controls none of these. The party that controls the source of a risk and profits from the activity that generates it is the party that can most cheaply reduce it, and the party that can absorb and spread whatever residual remains, through pricing, provisioning and insurance [12]. An individual depositor has no comparable mechanism; a single incident may consume a lifetime's savings, and the marginal disutility of that loss is incomparably greater than its marginal cost to an institution able to distribute it across a portfolio.

Burden of proof: application rather than creation

The most consequential finding of this study concerns the burden of proof, and it runs against the framing adopted by both informants and by much of the Indonesian literature. The debate is habitually conducted as though reversing the burden would require new legislation, on the model of the money laundering and environmental statutes. It would not.

Article 28 of Law No. 8 of 1999 provides that, in a claim for compensation brought under Articles 19, 22 and 23 of that Law, proof of the presence or absence of the element of fault is the burden and responsibility of the business actor. A reversal of the burden of proving fault already exists in Indonesian consumer law and has done since 1999. It is not applied to banking disputes for a reason that is characterisational rather than substantive: courts approach the bank–customer relationship through the law of contract and treat the customer as a contracting party rather than as a consumer of a financial service, notwithstanding that a depositor is a consumer of a service within the ordinary meaning of the statute and is expressly treated as such by OJK Regulation No. 22 of 2023 [13], [14], [23], [32].

This reframing materially reduces the reform burden. It is not necessary to persuade the legislature to create an unprecedented evidentiary rule for the financial sector. It is necessary to establish that a depositor is a consumer, that a digital banking service is a service, and that Article 28 therefore applies. That is an argument about the characterisation of an existing relationship, capable of being made in the ordinary course of litigation and capable of being confirmed by regulation without amendment to primary legislation.

The industry objection is answered on the same ground. Article 28 does not oblige a business actor to compensate on demand; it obliges the business actor to prove the absence of fault. A bank that has maintained a functioning detection system, applied step-up verification where its own rules required it, warned the customer specifically, and acted promptly on the report, will discharge that burden by producing its own

records. What Article 28 removes is the bank's ability to prevail through the customer's inability to see inside the system. That is not a systemic risk. It is the elimination of a windfall.

Comparative Benchmarks

Two jurisdictions have recently adopted dedicated regulatory frameworks in this precise area, and both abandoned the equation of authentication with consent. Neither solution is, strictly speaking, legislative: the United Kingdom mechanism takes the form of binding directions issued by a statutory regulator to payment service providers, while Singapore's takes the form of joint guidelines issued by two regulators. Their experience is instructive for Indonesia because they adopted structurally different solutions to the same problem, and because the regulatory rather than legislative form of both responses bears directly on what the OJK could enact within its existing authority.

The United Kingdom

The Payment Systems Regulator introduced a mandatory reimbursement requirement for authorised push payment fraud, in force from 7 October 2024, applying to payments made through the Faster Payments Scheme, with a parallel regime operated by the Bank of England for CHAPS. Authorised push payment fraud is defined as fraud in which a consumer is deceived into authorising a payment to an account outside his control, whether by deception as to the recipient or as to the purpose of the transfer. The sending payment service provider reimburses the victim, and the cost is shared equally between the sending and the receiving provider. Reimbursement is capped at £85,000 per claim, and providers may apply an excess of up to £100, which does not apply to vulnerable consumers. Reimbursement may be refused where the consumer acted with gross negligence, assessed against a defined consumer standard of caution which likewise does not apply to vulnerable consumers. Accompanying amendments to the payment services regulations permit a provider to delay execution by up to four business days where fraud is suspected [33].

Singapore

The Monetary Authority of Singapore and the Infocomm Media Development Authority introduced a Shared Responsibility Framework for phishing scams with effect from 16 December 2024. The Framework applies to seemingly authorised transactions, defined by reference to the impersonation of a legitimate business or government entity through a digital messaging channel. It assigns specified anti-scam duties to financial institutions and to telecommunications operators, and allocates loss through a waterfall: where a financial institution has breached a duty it bears the loss; where the institution has complied but a telecommunications operator has breached its own duty, the operator bears it; and only where both have discharged their duties does the consumer bear the loss. No liability cap is imposed, and full payout is expected where a duty has been breached. Investigation is subject to indicative timelines of twenty-one business days for straightforward cases and forty-five for complex ones, with recourse preserved to the Financial Industry Disputes Resolution Centre and to the courts [34].

Table 3. Comparative loss allocation models for manipulated but authenticated payments

Feature	United Kingdom (PSR, from 7 Oct 2024)	Singapore (MAS-IMDA SRF, from 16 Dec 2024)	Indonesia (current position)
Legal form	Binding regulatory directions.	Guidelines issued by the two regulators.	No instrument; contractual terms govern.
Trigger	Authorised push payment fraud on Faster Payments.	Seemingly authorised transaction arising from impersonation via a digital messaging channel.	Not defined.

Default allocation	Reimbursement by the sending provider, cost shared 50:50 with the receiving provider.	Waterfall: the party in breach of its duty bears the loss.	Customer bears the loss.
Consumer exception	Gross negligence against a consumer standard of caution; not applied to vulnerable consumers.	Consumer bears the loss only if both institution and operator discharged their duties.	Disclosure of credentials treated as decisive negligence.
Cap	£85,000 per claim; excess up to £100.	No cap; full payout expected on breach.	Not applicable.
Payment delay power	Up to four business days where fraud is suspected.	Duties include transaction surveillance and blocking.	Postponement available under Art. 26 of Law No. 8/2010 and the 2023 Bye Laws, but not owed to the customer.

Source: authors' compilation from the Payment Systems Regulator and MAS–IMDA materials cited at [33] and [34].

Lessons for Indonesia

Four points emerge. First, both jurisdictions abandoned the proposition that a valid authentication concludes the liability question, and neither found that abandonment destabilising. Second, both allocate loss by reference to the discharge of defined duties rather than by reference to who pressed the button, which converts the enquiry from an unprovable question about the customer's state of mind into a documentable question about institutional conduct. Third, both preserve a consumer-conduct exception, which answers the moral hazard objection without reinstating the default rule. Fourth, the United Kingdom model distributes cost across both ends of the payment chain, which is of particular relevance to Indonesia, since the mule account through which proceeds are laundered is opened at the receiving institution and its existence is itself evidence of a customer due diligence failure under Article 18(2) of Law No. 8 of 2010.

Of the two, the Singaporean structure is the closer fit for Indonesian institutional conditions. It operates through supervisory guidelines rather than primary legislation, which corresponds to the OJK's existing regulatory practice; it allocates loss by reference to enumerated duties, which is administratively simpler for a supervisor to assess than a case-by-case negligence enquiry; and it preserves ordinary civil recourse for cases falling outside its scope.

Neither model is available for direct transplantation, and the institutional differences that confine the comparison should be stated rather than assumed away. The United Kingdom mechanism presupposes a dedicated payment-systems regulator holding express statutory powers to issue directions binding on scheme participants, and a single dominant retail rail, the Faster Payments Scheme, to which a uniform reimbursement rule can be attached; Indonesian retail transfers run across several rails under the divided authority of Bank Indonesia over payment systems and the OJK over banks, so an equivalent rule would require coordinated instruments from two authorities rather than a single direction from one. The Singapore framework presupposes the joint jurisdiction of the financial and communications regulators, which allowed anti-scam duties to be imposed on telecommunications operators within the same instrument; in Indonesia the corresponding authority over telecommunications sits in a ministry outside the financial-sector architecture, so the telecommunications limb of the waterfall could not be replicated by OJK regulation alone and is deliberately not proposed here. Both jurisdictions also operate mature, well-resourced dispute-resolution

bodies capable of administering indicative timelines at volume. The proposal in Part IV.G accordingly borrows the structure of enumerated duties, safe harbour and consumer standard of caution, while confining the instrument to what the OJK can enact within its own authority and what the industry can operationalise on existing capability.

A Proposed Shared Responsibility Framework for Indonesia

Drawing the foregoing together, the following model is proposed. It is designed to be implementable through an OJK regulation issued under Law No. 4 of 2023, as amended by Law No. 4 of 2026, supported where necessary by a narrow amendment to the bank secrecy exception list, and it deliberately builds on capabilities Indonesian banks already possess.

The currency of that legal basis has been verified against the most recent amendments to the governing statutes. Law No. 1 of 2024, the second amendment to the ITE Law, refines the regime for electronic evidence, electronic certification, digital identity and international electronic contracts; it strengthens the attribution function of authentication without addressing the integrity of the will behind an authenticated instruction, and it therefore leaves intact both the gap identified in Part IV.A and the doctrinal argument of Part IV.C. Law No. 4 of 2026, amending Law No. 4 of 2023 with effect from 17 June 2026, is directed principally at institutional matters: the status, governance and budgeting of the Deposit Insurance Corporation; the extension of OJK supervision to commodity exchanges and other managers of public funds; the demutualisation of the stock exchange; and the refinement of investigation and restorative-justice mechanisms in the financial sector. It does not repeal or narrow the consumer-protection mandate under which OJK Regulation No. 22 of 2023 was issued, and it does not disturb the OJK's authority to regulate the conduct of banks toward financial consumers. Neither amendment therefore affects the substance of the proposed liability framework, the OJK's authority to adopt it, or the consumer-protection and enforcement provisions on which it rests; references throughout this article are to the statutes as most recently amended.

Scope. The framework applies to a seemingly authorised transaction, defined as a fund transfer authorised by the account holder using valid credentials, where the authorisation was procured by a third party impersonating a legitimate business, financial institution or government entity through a telephone, messaging or application channel.

Enumerated duties of the sending bank. Real-time evaluation of instructions against a behavioural baseline; step-up verification on defined risk triggers; a cooling-off interval for a first transfer to a newly registered beneficiary above a value threshold; a specific in-application warning where a known scam typology is detected; a reporting channel available outside business hours; and same-day transmission of a suspension request on a plausible victim report.

Enumerated duties of the receiving bank. Customer due diligence at account opening consistent with Article 18(2) of Law No. 8 of 2010; participation in a supervised shared register of accounts implicated in fraud reports, using the permission already granted by Article 23(1) of OJK Regulation No. 44 of 2024; and same-day execution of a valid suspension request, as already provided by the 2023 Bye Laws.

Allocation rule. Where a duty has been breached and the breach is causally connected to the loss, the bank in breach bears the loss. Where duties were breached at both ends, the loss is shared. Where the receiving account was opened in breach of customer due diligence obligations, a share is allocated to the receiving bank irrespective of the sending bank's conduct.

Safe harbour. A bank that evidences full compliance with its enumerated duties in respect of the specific transaction is discharged. Compliance is proved by the bank's own contemporaneous records, consistently with Article 28 of Law No. 8 of 1999.

Consumer standard of caution. The loss returns to the customer where the customer acted with gross negligence in particular, where the customer proceeded after receiving a specific in-application warning identifying the transaction as consistent with a known fraud typology, or after being informed by the bank that

the counterparty was fraudulent or where the customer was complicit. Vulnerability, including advanced age and disability, is a relevant consideration in applying the standard.

Cap and excess. A statutory cap per claim, indexed to a multiple of the deposit guarantee threshold, together with a modest excess, in order to preserve customer vigilance and bound institutional exposure.

Forum and timelines. First-instance determination through the Alternative Dispute Resolution Institution for the Financial Services Sector, within defined timelines, with ordinary civil recourse preserved.

Table 4. Proposed loss allocation matrix for seemingly authorised transactions

Sending bank	Receiving bank	Customer conduct	Allocation
Duties discharged	Duties discharged	Ordinary care	Customer bears the loss, subject to any recovery from the offender.
Duty breached	Duties discharged	Ordinary care	Sending bank bears the loss, up to the cap and net of the excess.
Duties discharged	Customer due diligence breached at account opening	Ordinary care	Receiving bank bears the loss.
Duty breached	Duty breached	Ordinary care	Loss shared between the two banks, presumptively in equal shares.
Any	Any	Gross negligence or complicity	Customer bears the loss; vulnerability taken into account.
Internal employee involvement established	Any	Any	Strict liability of the bank concerned, without cap.

Source: authors' proposal.

The model does not require Indonesian banks to acquire a capability they lack. Behavioural monitoring is already mandated for anti-money-laundering purposes; interbank suspension is already operational under the 2023 Bye Laws; reversal of the burden of proving fault already exists in Article 28 of the Consumer Protection Law; and interbank information exchange for fraud prevention is already permitted by Article 23(1) of OJK Regulation No. 44 of 2024. What is missing is the instrument that binds these elements into a duty owed to the customer, together with a defined consequence for breach.

CONCLUSION

The first research question asked whether the doctrine of vitiated consent can qualify a transfer instruction produced by social engineering as a legally defective agreement. It can. Such an instruction materially satisfies the elements of mistake under Article 1322 Indonesia Civil Code, because the victim is in error both as to the identity of the counterparty and as to the nature of the act being performed, and both errors are determinative. It satisfies the elements of fraud under Article 1328 Indonesia Civil Code, because the technique consists in a scripted series of falsehoods without which the authorisation would not have been given. Where the fraud is practised by a third party rather than by the bank, the analysis proceeds through the law of mandate and through

the good faith requirement of Article 1338(3) Indonesia Civil Code, a bank cannot claim the protection of good-faith reliance on an instruction that its own systems flagged, or would have flagged had they been operating to the standard the bank already applies for anti money laundering purposes. An authentication code verifies identity; it does not verify will, and it cannot be permitted to substitute for it.

The second question asked how the bank's civil liability should be expanded through the duty of care doctrine. The standard applicable to a bank as a professional operator of an electronic system extends beyond the delivery of a functioning system to encompass behavioural anomaly detection, risk-proportionate transactional friction, prompt post-incident responsiveness and upstream data integrity. Failure at any of these levels is an omission actionable under Articles 1365 Indonesia Civil Code and 1366 Indonesia Civil Code. The standard is dynamic and internally benchmarked: a bank must protect its depositor to at least the standard at which it protects the financial system, because the two tasks draw on the same data and the same detection logic.

The study's principal contribution lies in identifying that the components of a workable solution already exist within Indonesian positive law and industry practice, and are simply not joined. The monitoring capability is mandated by Article 18(2) of Law No. 8 of 2010. The suspension power is conferred by Article 26 of the same statute and is operationalised daily under the 2023 By Laws. The reversal of the burden of proving fault is enacted in Article 28 of Law No. 8 of 1999. The prohibition on exoneration clauses is enacted in Article 18 of the same statute. Interbank information exchange for fraud prevention is permitted by Article 23(1) of OJK Regulation No. 44 of 2024. What Indonesian law lacks is not capability, power or precedent, but a single instrument converting these into a duty owed to the customer with a defined consequence for its breach.

RECOMMENDATIONS

To the Financial Services Authority: issue a regulation, under the authority of Law No. 4 of 2023 as amended by Law No. 4 of 2026, establishing minimum fraud detection standards for digital banking and a loss allocation rule for seemingly authorised transactions along the lines set out in Part IV.G, together with a narrow amendment to the bank secrecy exception list permitting temporary suspension of a suspected recipient account on a verified victim report, without disclosure of the account holder's identity.

To the legislature: in any amendment to the Banking Law, or in a prospective umbrella statute on digital consumer protection, define the seemingly authorised transaction as a distinct legal category and allocate its loss expressly, so that the question ceases to depend on the characterisation of the customer's act.

To the courts: recognise the depositor as a consumer of a financial service and apply Article 28 of Law No. 8 of 1999 accordingly, so that proof of the absence of fault rests with the bank; and read Articles 1365 and 1366 as capable of encompassing a failure of anomaly detection, which is an omission rather than a positive act and is squarely within the scope of Article 1366.

To the banking industry: convert the commitments contained in the 2023 By Laws into customer facing service standards with published timelines, and disclose aggregate detection and interdiction metrics, both of which would improve the sector's evidentiary position under a safe harbour regime and reduce the incidence of disputes.

For further research: an empirical study of Indonesian court decisions in digital banking disputes, examining how first instance courts have in fact reasoned about causation and negligence, would test the doctrinal claims advanced here against judicial practice. A quantitative evaluation of detection efficacy across Indonesian banks would allow the standard of care to be specified with greater precision than a normative study permits.

LIMITATIONS OF THE STUDY

This is a normative legal study. Its empirical component consists of two expert interviews selected purposively, and no claim of statistical generalisability is made on that basis. The case approach applied in this study operates on Supreme Court jurisprudence concerning defective consent and abuse of circumstances and on documented institutional practice; it does not extend to decided Indonesian cases allocating social

engineering losses specifically, because reported decisions in that category remain scarce. The study also does not quantify the incidence of such losses or the recovery rate through litigation. The comparative material addresses two jurisdictions whose payment infrastructure and supervisory institutions differ materially from Indonesia's, and is offered as a source of design options rather than as a template for direct transposition.

Declarations

Ethical Approval

The study involved adult expert informants participating in their professional capacity. Informed consent was obtained from both informants prior to interview, and each consented to the attribution of statements made. No personal data of bank customers was collected, accessed or processed at any stage of the research.

Conflict of Interest

The authors declare that they have no conflict of interest.

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data Availability

All legislation and regulations analysed in this study are publicly available through the official databases of the Government of Indonesia and the Financial Services Authority. Interview transcripts are held by the authors and are available from the corresponding author on reasonable request, subject to the informants' consent.

Author Contributions

Both authors contributed to the conceptualisation and design of the study. The first author supervised the research, developed the theoretical framework and the comparative analysis, and revised the manuscript critically. The second author conducted the collection and analysis of legal materials and the expert interviews and prepared the initial draft. Both authors read and approved the final version.

REFERENCES

1. Nursetyo, A. (2019). Prinsip kehati-hatian bank dalam penyelenggaraan digital banking di Indonesia. *Jurnal Hukum & Pembangunan*, 49(2).
2. Sudarmono, N. M. (2023). Adaptasi regulasi persaingan usaha dalam bidang perbankan digital. *Jurnal Studia Legalia*, 4(1), 60–71. <https://doi.org/10.61084/jsl.v4i01.65>
3. Khumairok, M. (2023). Regulasi hukum perbankan dalam menghadapi tren inovasi fintech dan keberhasilan industri perbankan di era society 5.0. *Jurnal Multidisiplin Indonesia*, 2(7), 1719–1731. <https://doi.org/10.58344/jmi.v2i7.335>
4. Anjani, N. H. (2021). Kondisi keamanan siber di Indonesia. *Ringkasan Kebijakan*, 9, 1–12.
5. Muhammad, A. (1990). *Hukum perdata*. Citra Aditya Bakti.
6. Ramadanti, N., & Suwanto, H. (2023). Pertanggungjawaban perdata penyelenggara jasa perbankan digital atas kerugian nasabah akibat kebocoran data pribadi. *Jurnal Hukum Transnasional*, 7(1), 88–100.
7. Sjahdeini, S. R. (2020). *Hukum tata kelola teknologi informasi perbankan*. Pustaka Utama Grafiti.
8. Savitri, A. R. (2021). The duty of care of banks in digital banking transactions: A comparative perspective. *Indonesian Journal of International Law*, 18(4), 57–67.
9. Hadjon, P. M. (2007). *Perlindungan hukum bagi rakyat Indonesia: Sebuah studi tentang prinsip-prinsipnya, penanganannya oleh peradil dalam lingkungan peradil umum dan pembentukan peradil administrasi negara*. Peradaban.

10. Sitompul, Z. (2002). *Perlindungan dana nasabah bank: Suatu gagasan tentang pendirian lembaga penjamin simpanan di Indonesia*. Fakultas Hukum Universitas Indonesia.
11. Apriani, T. (2021). Konsep ganti rugi dalam perbuatan melawan hukum dan wanprestasi serta sistem pengaturannya dalam KUH Perdata. *Ganec Swara*, 15(1), 929. <https://doi.org/10.35327/gara.v15i1.193>
12. Widjaja, G. (2008). Risiko hukum dalam bisnis. *Forum Sahabat*.
13. Zulham. (2017). *Hukum perlindungan konsumen*. Kencana Prenada Media.
14. Sinaga, N. A. (2015). Pelaksanaan perlindungan konsumen di Indonesia. *Jurnal Ilmiah Hukum Dirgantara*, 5(2).
15. Subekti, R. (1995). *Aneka perjanjian*. Citra Aditya Bakti.
16. Setiawan, R. (2016). *Hukum perjanjian dan jaminan*. Kencana.
17. Thalib, A., & Aisyah, N. (2021). *Hukum perjanjian*. Rajawali Pers.
18. Fatimah Mediawati, N., & Purwaningsih, S. B. (2018). *Hukum kontrak dan perikatan*. Umsida Press.
19. Mertokusumo, S. (2019). *Mengenal hukum: Suatu pengantar*. Maha Karya Pustaka.
20. Ekawati, D. (2018). Perlindungan hukum terhadap nasabah bank yang dirugikan akibat kejahatan skimming ditinjau dari perspektif teknologi informasi dan perbankan. *UNES Law Review*, 1(2), 157–171. <https://doi.org/10.31933/law.v1i2.24>
21. Mahiswari, A. A. S., & Utama, I. M. A. (2020). Tanggung jawab bank terhadap kerugian nasabah akibat kegagalan sistem dalam transaksi mobile banking. *Jurnal Ilmu Hukum*, 8(8).
22. Setiyono, H. (2020). Rekonstruksi pertanggungjawaban pidana dan perdata dalam kejahatan perbankan di era teknologi informasi. *Jurnal Hukum Ius Quia Iustum*, 27(1).
23. Handayani, I. G. A. K. R. (2022). Legal protection for bank customers as consumers in electronic banking transactions. *Journal of Legal, Ethical and Regulatory Issues*, 23(5).
24. Marzuki, P. M. (2005). *Penelitian hukum (rev. ed.)*. Prenada Media Group.
25. Ali, Z. (2009). *Metode penelitian hukum*. Sinar Grafika.
26. Soekanto, S. (2014). *Pengantar penelitian hukum*. UI Press.
27. Idris, M. (2019). Kerahasiaan bank suatu tinjauan dalam aturan hukum perbankan syariah di Indonesia. *Al-Amwal: Journal of Islamic Economic Law*, 1(1), 1–29. <https://doi.org/10.24256/alw.v1i1.624>
28. Sutedi, A. (2010). *Hukum perbankan: Suatu tinjauan pencucian uang, merger, konsolidasi, dan akuisisi*. Sinar Grafika.
29. Dewi, S. (2016). Cyberlaw: Perlindungan privasi data pribadi dalam digital economy. *Socio-Humaniora*, 18(2).
30. Lingga Syailendra Arief, & Purwanto, R. (2025). Tinjauan yuridis Undang-Undang Perlindungan Data Pribadi Tahun 2022 dalam menangani kebocoran data pelanggan e-commerce. *Pemuliaan Keadilan*, 2(3), 85–102. <https://doi.org/10.62383/pk.v2i3.1019>
31. Fista, Y. L., Machmud, A., & Suartini. (2023). Perlindungan hukum konsumen dalam transaksi e-commerce ditinjau dari perspektif Undang-Undang Perlindungan Konsumen. *Binamulia Hukum*, 12(1), 177–189. <https://doi.org/10.37893/jbh.v12i1.599>
32. Harahap, Y. (2015). *Hukum acara perdata: Tentang gugatan, persidangan, penyitaan, pembuktian, dan putusan hakim*. Sinar Grafika.
33. Payment Systems Regulator. (2023). *Fighting authorised push payment scams: Final decision (Policy Statement PS23/4)*. Payment Systems Regulator.
34. Monetary Authority of Singapore & Infocomm Media Development Authority. (2024). *Guidelines on Shared Responsibility Framework*. Monetary Authority of Singapore.
35. Friedman, L. M. (2011). *Sistem hukum: Perspektif ilmu sosial*. Nusa Media.
36. Mathilda, F. (2012). Cyber crime dalam sistem hukum Indonesia. *SIGMA-Mu*, 2(2), 34–45.
37. Panggabean, H. P. (2010). Penyalahgunaan keadaan (misbruik van omstandigheden) sebagai alasan (baru) untuk pembatalan perjanjian: Berbagai perkembangan hukum di Belanda dan Indonesia. *Liberty*.
38. Agustina, R. (2003). *Perbuatan melawan hukum*. Program Pascasarjana Fakultas Hukum Universitas Indonesia.
39. Fuady, M. (2002). *Perbuatan melawan hukum: Pendekatan kontemporer*. Citra Aditya Bakti.
40. Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative data analysis: A methods sourcebook (3rd ed.)*. Sage Publications.

Legislation, Regulations and Industry Instruments

1. Kitab Undang-Undang Hukum Perdata (Burgerlijk Wetboek).
2. Law No. 7 Year 1992 on Banking, as amended by Law No. 10 Year 1998.
3. Law No. 8 Year 1999 on Consumer Protection.
4. Law No. 11 Year 2008 on Information and Electronic Transactions, as amended by Law No. 19 Year 2016 and by Law No. 1 Year 2024.
5. Law No. 8 Year 2010 on Prevention and Eradication of Money Laundering.
6. Law No. 27 Year 2022 on Personal Data Protection.
7. Law No. 4 Year 2023 on Development and Strengthening of the Financial Sector, as amended by Law No. 4 Year 2026.
8. Financial Services Authority Regulation Number 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector.
9. Financial Services Authority Regulation Number 44 of 2024 concerning Bank Secrecy.
10. 2023 Indonesian Banking Regulation regarding the Suspension of Fund Transfer Transactions.
11. Payment Systems Regulator (United Kingdom), Specific Directions 19, 20 and 21 (authorised push payment reimbursement), in force 7 October 2024.
12. Monetary Authority of Singapore and Infocomm Media Development Authority, Guidelines on Shared Responsibility Framework, in force 16 December 2024.

Court Decisions

1. Mahkamah Agung Republik Indonesia, Decision No. 1904 K/Sip/1982, 28 January 1984.
2. Mahkamah Agung Republik Indonesia, Decision No. 3431 K/Pdt/1985, 4 March 1987 (Sri Setianingsih v. Ny. Boesono and R. Boesono).
3. Mahkamah Agung Republik Indonesia, Decision No. 3641 K/Pdt/2001.
4. Mahkamah Agung Republik Indonesia, Decision No. 3406 K/Pdt/2019, 16 December 2019.