Jurnal Pustaka Cendekia Hukum dan Ilmu Sosial
Volume 3, No. 3, October 2025 - January 2026, pp. 404-412
E-ISSN: 2987-4475
https://pchukumsosial.org/index.php/pchs

Analisis Normatif Atas Keterbatasan Pengaturan OJK Terkait Perlindungan Nasabah dalam Menghadapi Ancaman Risiko Social Engineering

Mika Anwarita Pakpahan[1]*, Yuniar Pamadya Astuti[2]

[1,2]Universitas Esa Unggul, Jl. Harapan Indah Boulevard No.2, Pusaka Rakyat, Kec. Tarumajaya, Kabupaten Bekasi, Jawa Barat, Indonesia.
Mikaanwarita@student.esaunggul.ac.id

Abstract

This article analyzes the effectiveness of customer protection regulations in digital banking services against the threat of social engineering, a form of modern financial risk. This research uses normative legal methods by examining regulations, legal literature, and empirical research findings related to digital crime in the banking sector. The results show that although the regulatory framework addresses the principles of consumer protection, system security, and risk management, these regulations do not specifically address the complexity of social engineering, which is rooted in psychological manipulation and low customer digital literacy. The absence of investigative standards, limits of liability, and independent evidentiary mechanisms leaves customers in a very vulnerable position when funds are lost. This article concludes that more detailed and adaptive regulatory updates are needed, including a strengthened accountability model, transparent investigation procedures, and increased digital security education to strengthen legal protection for customers in the digital banking ecosystem.
Keywords: Customer Protection, Social Engineering, Digital Banking, Modern Financial Risks, Financial Services Regulation.

Abstrak

Artikel ini menganalisis efektivitas pengaturan perlindungan nasabah dalam layanan digital perbankan terhadap ancaman social engineering sebagai salah satu bentuk risiko keuangan modern. Penelitian ini menggunakan metode hukum normatif dengan menelaah regulasi, literatur hukum, dan hasil penelitian empiris terkait kejahatan digital pada sektor perbankan. Hasil penelitian menunjukkan bahwa meskipun kerangka regulasi telah mengatur prinsip perlindungan konsumen, keamanan sistem, dan manajemen risiko, pengaturan tersebut belum secara spesifik menjawab kompleksitas social engineering yang berakar pada manipulasi psikologis dan rendahnya literasi digital nasabah. Ketiadaan standar investigasi, batas tanggung jawab, dan mekanisme pembuktian independen menyebabkan posisi nasabah sangat lemah ketika terjadi kehilangan dana. Artikel ini menyimpulkan bahwa diperlukan pembaruan regulasi yang lebih rinci dan adaptif, termasuk penegasan model pertanggungjawaban, prosedur investigasi transparan, serta peningkatan edukasi keamanan digital untuk memperkuat perlindungan hukum bagi nasabah dalam ekosistem perbankan digital.
Kata Kunci: Perlindungan Nasabah, Social Engineering, Perbankan Digital, Risiko Keuangan Modern, Regulasi Jasa Keuangan

✉Corresponding author: Mika Anwarita Pakpahan
Email Address: Mikaanwarita@student.esaunggul.ac.id (Jl. Harapan Indah Boulevard No.2, Kab. Bekasi, Jabar)
Received 05 January 2026, Accepted 11 January 2026, Published 17 January 2026

PENDAHULUAN

Perbankan Indonesia telah mengalami percepatan digitalisasi melalui pengembangan layanan seperti mobile banking dan internet banking yang memungkinkan masyarakat melakukan transaksi tanpa harus hadir secara fisik di kantor cabang. Transformasi ini menjadikan transaksi keuangan lebih cepat, mudah, dan inklusif bagi berbagai kelompok masyarakat (Anggraeni, 2023).

Namun, percepatan digitalisasi tersebut juga melahirkan risiko baru yang tidak muncul dalam transaksi perbankan konvensional. Risiko ini terutama berkaitan dengan kerentanan teknologi dan pola interaksi manusia dengan perangkat digital yang belum sepenuhnya aman (Bank Indonesia, 2025).

Salah satu risiko digital paling signifikan adalah social engineering, yakni manipulasi psikologis yang mendorong korban untuk menyerahkan akses terhadap akun perbankan digitalnya. Social engineering terbukti menjadi modus yang paling banyak menyebabkan kehilangan dana pada nasabah perbankan digital dalam dua tahun terakhir (Chairunnisa et al., 2024).

Peningkatan kasus social engineering tidak hanya disebabkan oleh kecanggihan pelaku, tetapi juga oleh tingginya ketergantungan layanan digital pada data kredensial pengguna seperti OTP, PIN, dan password. Ketika nasabah terpengaruh manipulasi, akses ke rekening dapat dibobol dengan sangat mudah, meski sistem keamanan bank tetap berjalan normal (Ibrahim et al., 2024).

Di Indonesia, kasus-kasus kehilangan dana akibat social engineering terus muncul dalam pemberitaan dan laporan publik, menunjukkan pola yang serupa: pelaku meniru identitas bank atau pihak resmi untuk mengelabui korban. Kejadian ini memicu keresahan masyarakat serta menunjukkan perlunya peningkatan sistem perlindungan nasabah dalam menghadapi risiko keuangan modern (Ekayani et al., 2023).

Di sisi regulasi, Otoritas Jasa Keuangan (OJK) telah mengeluarkan beberapa aturan mengenai perlindungan konsumen serta pengelolaan risiko oleh lembaga jasa keuangan. Namun, sejumlah penelitian menilai bahwa regulasi tersebut masih bersifat normatif dan belum memberikan mekanisme teknis yang spesifik untuk menangani kasus social engineering.

Keterbatasan ini terlihat dari tidak adanya pengaturan yang secara tegas mengatur standar pertanggungjawaban bank apabila nasabah menjadi korban manipulasi digital. Akibatnya, penyelesaian kasus sering bergantung pada interpretasi internal bank, sementara nasabah tidak memiliki posisi tawar maupun akses terhadap bukti teknis pemeriksaan transaksi (Hakim & Putra, 2025).

Kondisi tersebut menimbulkan ketidakpastian hukum dan berpotensi merugikan nasabah, terutama karena sebagian besar nasabah tidak memahami aspek teknis keamanan digital. Oleh karena itu, diperlukan kajian hukum normatif untuk menilai apakah pengaturan OJK saat ini telah memadai dalam merespons ancaman risiko keuangan modern, khususnya social engineering.

Penelitian ini menjadi penting karena memberikan analisis atas kekosongan dan kelemahan regulasi yang ada, sekaligus menawarkan rekomendasi model perlindungan yang lebih adaptif terhadap perkembangan teknologi perbankan digital. Kajian ini diharapkan dapat mendorong peningkatan standar keamanan serta mekanisme penyelesaian sengketa yang lebih adil bagi nasabah di era digital (Waliullah et al., 2025).

METODE

Penelitian ini menggunakan pendekatan hukum normatif dengan menelaah peraturan perundang-undangan, kebijakan OJK, serta literatur hukum yang relevan mengenai perlindungan konsumen jasa keuangan. Pendekatan ini digunakan untuk menganalisis kecukupan dan efektivitas norma dalam mengatur perlindungan nasabah terhadap risiko social engineering pada layanan digital perbankan (Ekayani et al., 2023). Penelitian memanfaatkan data sekunder berupa hasil penelitian,

laporan otoritas keuangan, dan publikasi resmi yang menggambarkan fenomena kejahatan digital yang berkembang di sektor perbankan.

Analisis dilakukan secara kualitatif melalui interpretasi sistematis terhadap norma yang mengatur kewajiban lembaga jasa keuangan serta hak-hak nasabah. Pendekatan normatif memungkinkan identifikasi celah pengaturan, ketidakpastian standar perlindungan, atau kekosongan hukum yang tidak menjawab ancaman risiko keuangan modern seperti social engineering (Hakim & Putra, 2025). Dengan metode ini, penelitian diharapkan mampu memberikan argumentasi hukum yang komprehensif mengenai perlunya pembaruan pengaturan dan penguatan perlindungan nasabah pada era digital.

HASIL DAN DISKUSI

Pengaturan Otoritas Jasa Keuangan (OJK) Mengatur Perlindungan Nasabah dalam Layanan Digital Perbankan Terhadap Ancaman Social Engineering

Perkembangan layanan digital dalam industri perbankan mendorong lembaga jasa keuangan untuk mengimplementasikan standar keamanan yang lebih kuat dalam setiap aktivitas elektronik. Digitalisasi ini memperbesar eksposur nasabah terhadap serangan manipulatif seperti social engineering, sehingga bank diwajibkan membangun sistem pengamanan yang memadai untuk menjaga kerahasiaan dan integritas data nasabah (Anggraeni, 2023). Regulasi terkait layanan keuangan secara umum telah mengatur perlunya kontrol keamanan informasi dan penerapan prinsip kehati-hatian, khususnya dalam transaksi yang melibatkan autentikasi berbasis data pribadi atau kredensial digital (Sianturi et al., 2024).

Sebagai bagian dari perlindungan konsumen, bank diwajibkan menyediakan informasi yang akurat, jelas, dan tidak menyesatkan kepada masyarakat pengguna layanan digital. Edukasi ini menjadi sangat penting karena mayoritas kasus social engineering terjadi akibat rendahnya pemahaman nasabah mengenai pola serangan, sehingga pelaku dapat dengan mudah memperoleh akses melalui bujukan atau penyamaran digital. Studi terkini menegaskan bahwa literasi keamanan digital merupakan variabel penting yang menentukan keberhasilan mitigasi risiko dan perlindungan terhadap akun nasabah (Furqon, 2025).

Pengaturan mengenai manajemen risiko teknologi informasi juga mewajibkan bank untuk menerapkan pengamanan yang meliputi verifikasi ganda, pengendalian akses, dan sistem deteksi transaksi mencurigakan. Ketentuan ini diarahkan untuk memastikan bahwa setiap aktivitas digital dapat dimonitor, sehingga potensi fraud dapat dikenali sebelum menimbulkan kerugian besar bagi pengguna. Analisis efektivitas pengamanan perbankan digital menunjukkan bahwa sistem pemantauan berbasis perilaku transaksi menjadi instrumen yang semakin penting dalam memitigasi ancaman manipulasi digital (Alia et al., 2024).

Selain aspek keamanan teknis, bank diwajibkan menyediakan mekanisme pengaduan yang cepat dan responsif sebagai saluran remedial ketika nasabah mengalami kehilangan dana. Namun, temuan penelitian menunjukkan bahwa tidak adanya standar investigasi yang seragam membuat penyelesaian

kasus kehilangan dana sering bergantung pada kebijakan internal masing-masing bank, sehingga menimbulkan ketidakpastian bagi nasabah yang berada pada posisi lemah dalam pembuktian (Ibrahim et al., 2024). Ketidakselarasan ini membuat perlindungan yang diberikan regulasi cenderung bersifat deklaratif dan belum memberikan kepastian mengenai bagaimana kasus serangan sosial harus ditangani secara objektif.

Regulasi anti-fraud yang lebih baru mengharuskan lembaga perbankan memperkuat kemampuan sistem dalam mengenali pola penipuan dan menetapkan intervensi otomatis ketika terdapat indikasi aktivitas tidak wajar. Sistem ini dirancang untuk memberikan perlindungan preventif, karena modus social engineering sering memanfaatkan momen ketika nasabah terburu-buru atau kurang berhati-hati dalam menanggapi pesan atau panggilan yang tampak resmi. Studi telekomunikasi dan keamanan digital menunjukkan bahwa pendekatan ini efektif menurunkan risiko apabila disertai edukasi konsumen yang berkelanjutan (Putri et al., 2024).

Meski demikian, sejumlah penelitian hukum menunjukkan bahwa pengaturan yang berlaku belum secara khusus mengatur tata cara penanganan kasus social engineering. Tidak terdapat aturan yang menjelaskan batas kewajiban bank, standar pembuktian, ataupun prosedur verifikasi independen ketika terjadi kehilangan dana. Kekosongan ini menyebabkan tanggung jawab bank dalam banyak kasus menjadi bias pada klaim "kelalaian nasabah," sementara nasabah sendiri tidak memiliki kemampuan teknis untuk membantah hasil investigasi internal yang dilakukan bank (Ekawati & Herdiana, 2025).

Kurangnya pengaturan spesifik tersebut berdampak pada rendahnya perlindungan hukum terhadap nasabah yang menjadi korban kejahatan manipulatif. Penelitian literatur hukum digital menegaskan bahwa social engineering merupakan risiko keuangan modern yang tidak dapat diselesaikan hanya dengan pendekatan keamanan teknis dan edukasi nasabah. Diperlukan kerangka pengaturan yang menyediakan batas tanggung jawab yang jelas, prosedur investigasi yang transparan, dan mekanisme penyelesaian sengketa yang setara bagi nasabah (Waliullah et al., 2025).

Dengan demikian, meskipun kerangka regulasi yang ada telah memuat prinsip umum perlindungan konsumen, penerapan keamanan TI, dan mitigasi risiko, efektivitasnya dalam menghadapi ancaman manipulasi digital masih terbatas. Risiko social engineering memiliki karakteristik unik yang menempatkan nasabah dalam posisi sangat rentan, sehingga pengaturan yang lebih komprehensif, spesifik, dan responsif terhadap perkembangan modus kejahatan digital diperlukan untuk memastikan perlindungan hukum yang optimal bagi masyarakat pengguna layanan digital perbankan (Tarumanagara University researchers, 2025).

Keterbatasan Normatif dalam Pengaturan OJK Menyebabkan Belum Optimalnya Perlindungan Hukum Bagi Nasabah yang Menjadi Korban Social Engineering

Secara normatif, Otoritas Jasa Keuangan (OJK) telah menerbitkan sejumlah regulasi yang berkaitan dengan perlindungan konsumen jasa keuangan dan manajemen risiko teknologi informasi pada lembaga perbankan, antara lain melalui Peraturan OJK mengenai Perlindungan Konsumen Sektor Jasa Keuangan dan Peraturan OJK mengenai Penyelenggaraan Teknologi Informasi oleh Bank Umum.

Regulasi tersebut mewajibkan bank untuk menerapkan prinsip transparansi, perlakuan yang adil, keandalan sistem, kerahasiaan dan keamanan data, serta penanganan pengaduan nasabah secara profesional.

Namun, apabila ditelaah lebih jauh, pengaturan yang ada masih bersifat umum dan belum secara khusus mengantisipasi karakteristik kejahatan social engineering yang berfokus pada manipulasi psikologis korban, bukan semata-mata pada kelemahan sistem elektronik. Dalam praktik, banyak bank mendasarkan penolakan klaim kerugian nasabah pada dalih "kelalaian nasabah" karena nasabah dianggap telah memberikan data otentikasi (OTP, PIN, password) kepada pihak lain, sehingga kerugian ditempatkan sebagai tanggung jawab pribadi nasabah. Pendekatan ini menunjukkan adanya bias penafsiran yang menempatkan beban risiko secara tidak proporsional kepada nasabah, padahal kerentanan tersebut muncul dalam ekosistem layanan digital yang dikendalikan dan dipasarkan oleh bank.

Kajian empiris menunjukkan bahwa kasus kehilangan dana pada rekening digital seringkali terjadi meskipun bank telah memenuhi standar keamanan teknis minimum, karena pelaku memanfaatkan celah pada perilaku dan literasi digital nasabah. Dalam konteks ini, social engineering seharusnya dipandang sebagai bagian dari risiko operasional yang inheren dalam penyelenggaraan layanan digital, sehingga tidak dapat sepenuhnya dialihkan sebagai kesalahan individu nasabah. Konstruksi normatif yang belum secara tegas mengakui social engineering sebagai risiko keuangan modern mengakibatkan tidak adanya standar pertanggungjawaban yang jelas ketika terjadi sengketa.

Keterbatasan lain tampak pada ketiadaan ketentuan eksplisit mengenai standar investigasi dan mekanisme pembuktian yang independen ketika nasabah melaporkan kehilangan dana. Regulasi yang ada umumnya hanya mewajibkan bank untuk menyediakan sarana pengaduan dan menyelesaikan pengaduan dalam jangka waktu tertentu, tanpa mengatur bagaimana proses investigasi teknis harus dilakukan, sejauh mana nasabah berhak mengakses hasil investigasi, serta bagaimana peran otoritas pengawas dalam menguji kebenaran laporan bank. Akibatnya, proses pembuktian cenderung didominasi oleh laporan internal bank yang bersifat sepihak, sementara nasabah berada pada posisi yang sangat lemah karena tidak memiliki kemampuan maupun akses terhadap bukti elektronik yang kompleks.

Dalam beberapa putusan dan kajian akademik, kerugian nasabah akibat kegagalan sistem atau kejahatan siber dikualifikasikan sebagai pelanggaran terhadap prinsip keandalan dan keamanan sistem elektronik yang diatur dalam Undang-Undang Informasi dan Transaksi Elektronik, Undang-Undang Perlindungan Konsumen, serta Undang-Undang Perbankan. Namun, pada level pengaturan sektoral, belum terdapat penghubung yang eksplisit antara kewajiban normatif tersebut dengan mekanisme kompensasi konkret bagi nasabah yang menjadi korban social engineering. Kekosongan pengaturan ini menimbulkan ketidakpastian mengenai apakah kerugian harus ditanggung penuh oleh nasabah, dibagi berdasarkan derajat kesalahan, atau menjadi tanggung jawab bank sebagai penyelenggara sistem.

Di sisi lain, sejumlah penelitian mutakhir menegaskan bahwa literasi keamanan digital memiliki peran signifikan dalam mengurangi keberhasilan serangan social engineering, sehingga edukasi yang efektif menjadi bagian integral dari perlindungan hukum terhadap nasabah. Meskipun regulasi OJK telah memuat kewajiban edukasi, belum ada standar normatif yang terukur mengenai kualitas, intensitas, dan evaluasi efektivitas program edukasi tersebut. Tanpa indikator yang jelas, kewajiban edukasi berpotensi berhenti pada kampanye sosialisasi yang bersifat formalistik, tanpa benar-benar meningkatkan kapasitas nasabah dalam mengenali dan mencegah modus penipuan.

Keterbatasan normatif juga terlihat pada belum optimalnya pengaturan mengenai koordinasi antarotoritas, khususnya antara OJK, Bank Indonesia, dan aparat penegak hukum, dalam penanganan kasus social engineering. Kejahatan ini sering melibatkan lintas platform (telekomunikasi, media sosial, dan sistem perbankan), sehingga penanganan yang terfragmentasi mengakibatkan proses pelacakan pelaku dan pemulihan kerugian berjalan lambat dan tidak terintegrasi. Ketiadaan protokol baku lintas lembaga menyebabkan banyak kasus berhenti pada pelaporan tanpa tindak lanjut yang memadai, sehingga menurunkan kepercayaan publik terhadap efektivitas perlindungan hukum.

Dengan demikian, dapat disimpulkan bahwa keterbatasan normatif dalam pengaturan OJK tercermin dalam beberapa aspek kunci:

1. Tidak adanya pengakuan eksplisit terhadap social engineering sebagai risiko keuangan modern yang harus dikelola sebagai bagian dari tanggung jawab operasional bank;
2. Ketiadaan standar pertanggungjawaban dan mekanisme kompensasi yang jelas bagi nasabah korban;
3. Belum diaturnya standar investigasi dan pembuktian yang independen dan transparan;
4. Lemahnya standar normatif mengenai edukasi literasi keamanan digital; serta
5. Belum optimalnya mekanisme koordinasi lintas otoritas dalam penanganan kasus.

Keterbatasan-keterbatasan ini secara kumulatif menyebabkan perlindungan hukum terhadap nasabah yang menjadi korban social engineering belum berjalan optimal, meskipun secara deklaratif prinsip perlindungan konsumen telah diakomodasi dalam regulasi sektor jasa keuangan.

KESIMPULAN

Digitalisasi perbankan telah menghadirkan kemudahan layanan, tetapi juga membuka ruang munculnya risiko keuangan modern, terutama social engineering yang memanfaatkan kelemahan psikologis dan literasi digital nasabah. Kajian terhadap pengaturan perlindungan nasabah menunjukkan bahwa kerangka regulasi yang berlaku pada dasarnya telah menyediakan prinsip umum perlindungan konsumen, kewajiban edukasi, keamanan teknologi, dan mekanisme pengaduan. Namun, regulasi tersebut belum mengatur secara spesifik model perlindungan terhadap serangan manipulatif yang tidak selalu melibatkan kelemahan sistem perbankan, tetapi justru bersumber dari rekayasa sosial yang membuat nasabah secara tidak sadar memberikan akses kepada pelaku.

Ketiadaan pengaturan rinci mengenai standar investigasi, batas tanggung jawab, dan prosedur verifikasi dalam kasus kehilangan dana menyebabkan nasabah berada pada posisi yang rentan. Banyak penyelesaian kasus masih bergantung pada penilaian internal lembaga perbankan, sehingga tidak semua nasabah mendapatkan perlindungan yang setara. Kondisi ini menunjukkan adanya celah normatif yang perlu diperkuat agar perlindungan hukum tidak hanya bersifat deklaratif, tetapi benar-benar memberikan kepastian dan keadilan bagi masyarakat pengguna layanan digital perbankan.

Dengan demikian, diperlukan pembaruan regulasi yang lebih komprehensif dan responsif terhadap risiko social engineering, termasuk pengaturan mengenai pembagian tanggung jawab, tata cara investigasi independen, mekanisme pembuktian yang objektif, serta peningkatan literasi keamanan digital. Pembaruan ini menjadi kunci untuk memastikan bahwa nasabah memperoleh perlindungan yang optimal di tengah perkembangan teknologi perbankan yang semakin kompleks dan dinamis.

Berdasarkan analisis terhadap kerangka pengaturan OJK dan praktik perlindungan nasabah dalam layanan perbankan digital, dapat disimpulkan bahwa keterbatasan normatif yang ada berkontribusi langsung terhadap belum optimalnya perlindungan hukum bagi nasabah yang menjadi korban social engineering. Regulasi OJK saat ini lebih menekankan pada prinsip umum perlindungan konsumen dan keamanan sistem, tetapi belum mengatur secara spesifik tanggung jawab bank, standar investigasi, serta mekanisme pemulihan kerugian dalam kasus manipulasi digital yang melibatkan interaksi kompleks antara teknologi dan perilaku manusia.`

Ketiadaan pengaturan yang eksplisit mengenai social engineering sebagai risiko operasional membuat bank cenderung menempatkan beban kesalahan pada nasabah dengan mendalilkan pelanggaran kewajiban merahasiakan data otentikasi. Padahal, dalam perspektif perlindungan konsumen dan manajemen risiko modern, social engineering merupakan konsekuensi yang tidak terpisahkan dari model layanan digital yang dipromosikan oleh bank, sehingga tanggung jawab atas pencegahan dan penanganannya tidak dapat sepenuhnya dialihkan kepada nasabah.

Di sisi lain, lemahnya pengaturan mengenai edukasi literasi keamanan digital, transparansi proses investigasi, dan koordinasi lintas otoritas menyebabkan nasabah tidak memperoleh jaminan perlindungan yang setara ketika menjadi korban. Nasabah tidak hanya mengalami kerugian finansial, tetapi juga menghadapi hambatan struktural dalam pembuktian dan pemulihan haknya. Hal ini menunjukkan bahwa perlindungan hukum yang tersedia masih bersifat deklaratif dan belum sepenuhnya terimplementasi dalam mekanisme operasional yang berpihak pada korban.

Oleh karena itu, untuk menjawab rumusan masalah kedua, diperlukan pembaruan regulasi OJK yang secara tegas mengakui social engineering sebagai risiko keuangan modern, menetapkan model pertanggungjawaban yang seimbang antara bank dan nasabah, mengatur standar investigasi dan pembuktian yang independen, serta memperkuat kewajiban edukasi dan koordinasi lintas otoritas. Pembaruan ini menjadi prasyarat agar perlindungan hukum terhadap nasabah dalam ekosistem perbankan digital tidak hanya berhenti pada tataran normatif, tetapi benar-benar menjamin keadilan, kepastian, dan keamanan bagi masyarakat pengguna layanan keuangan.

UCAPAN TERIMA KASIH

Penulis mengcapkan ribuan terima kasih kepada seluruh pihak yang telah berkontribusi dalam penelitian sekaligus penyusuuna artikel ini.

REFERENSI

Anggraeni, R. (2023, Agustus Senin). *Awas! Serangan Social Engineering Incar Data Pribadi Nasabah*. Bisnis.com. Retrieved Desember Rabu, 2025, from https://finansial.bisnis.com/read/20230821/90/1686735/awas-serangan-social-engineering-incar-data-pribadi-nasabah?

Al Fitara, I., & Fasa, M. I. (2025). Kemudahan dan Tantangan Green Banking di Era Digital dalam Penggunaan Marketplace. Jurnal Bersama Ilmu Ekonomi (EKONOM), 1(1), 30–39. https://doi.org/10.55123/ekonom.v1i1.34

Bank Indonesia. (2025). *Blueprint Sistem Pembayaran Indonesia 2025 Bank Indonesia: Menavigasi Sistem Pembayaran Nasional di Era Digital*. Bank Indonesia. https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/blueprint-2025/default.aspx

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024, Februari). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phisingdan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. *Jurnal Ilmu Hukum dan Sosial*, *2*, 01-16. https://doi.org/10.51903/hakim.v2i1.1535

Ekayani, L., Djanggih, H., & Suong, M. A. (2023, Juni). Perlindungan Hukum Nasabah Terhadap Kejahatan Pencurian Data Pribadi (Phising) Di Lingkungan Perbankan). *Journal of Philosophy (JLP)*, *4*(1), 22-40. Retrieved Desember Rabu, 2025, from https://www.researchgate.net/publication/383595518_Perlindungan_Hukum_Nasabah_Terhadap_Kejahatan_Pencurian_Data_Pribadi_Phising_Di_Lingkungan_Perbankan

Furqon, M. A. A. (2025). Digital Security Literacy of Bank and Fintech Customers: The Role of Educational Communication in Preventing Social Engineering. International Journal of Science and Society, 7(3), 20–32. https://doi.org/10.54783/ijsoc.v7i3.1475

Hakim, M. R., & Putra, M. R. S. (2025, Juni). Analysis of Digital Bank Customer Protection Against Loss of Funds in Accounts Reviewed According to Indonesian Positive Law. *JURNAL USM LAW REVIEW*, *8*(2), 813-824. Retrieved Desember Rabu, 2025, from https://www.researchgate.net/publication/392523669_Analysis_of_Digital_Bank_Customer_Protection_Against_Loss_of_Funds_in_Accounts_Reviewed_According_to_Indonesian_Positive_Law

Ibrahim, D. M., Hidayat, Y., & Wasitaatmadja, F. F. (2024, Juni). Legal Protection of Banking Customers Who Are Victims Of Information And Electronic Transaction Crimes. *Jurnal Ilmiah Penegakan Hukum*, *11*(1), 102-120. http://dx.doi.org/10.31289/jiph.v11i1.11099

Nguyen, T. T., et al. (2024). Digital literacy, online security behaviors and E-payment intention. Journal of High Technology Management Research, 35(1), 100123. https://doi.org/10.1016/j.hitech.2024.100123

Sihotang, D. J., Kamaludi, E., & Indriani, F. (2025). The Role of Digital Banking and Fintech in Advancing Financial Inclusion. Economic and Business Horizon, 4(2), 341–352. https://doi.org/10.54518/ebh.4.2.2025.678

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025, Februari). ASSESSING THE INFLUENCE OF CYBERSECURITY THREATS AND RISKS ON THE ADOPTION AND GROWTH OF DIGITAL BANKING: A SYSTEMATIC LITERATURE REVIEW. *American Journal of Advanced Technology and Engineering Solutions*, *01*(01), 226-257. Retrieved Desember Rabu, 2025, from https://www.researchgate.net/publication/390354819_Assessing_the_influence_of_cybersecurity_threats_and_risks_on_the_adoption_and_growth_of_digital_banking_a_systematic_literature_review

Zubaidi, K. S., & Yuliati, A. (2025). Pengaruh Literasi Keuangan, Persepsi Kegunaan, Keamanan, dan Fitur terhadap Minat Penggunaan Bank Digital: Studi pada Generasi Z di Surabaya Pengguna SeaBank. Jurnal Maneksi, 14(2), 839–852. https://doi.org/10.31959/jm.v14i2.3080