

THE TRADE-OFF BETWEEN FINTECH CONSUMER DATA SECURITY AND THE EFFECTIVENESS OF BI'S MONETARY POLICY TRANSMISSION: EVIDENCE FROM INDONESIA 2021–2025

Slamet Rahmat Topo Susilo^{1*}, Ardy Firman Syah²

¹Research Center for Social Welfare, Village, and Connectivity
National Research and Innovation Agencies, Jakarta, Indonesia

²Research Center for Domestic Government
National Research and Innovation Agencies, Jakarta, Indonesia

Author's email:

¹slam024@brin.go.id; ²ardy001@brin.go.id

*Corresponding author:

slam024@brin.go.id

Abstract. *This study aims to examine how fintech consumer data security operates as a moderating mechanism within Indonesia's monetary policy transmission framework during the 2021–2025 period. Utilizing a qualitative descriptive design grounded in technical-institutional analytics, the paper analyzes regulatory documents, policy frameworks, and secondary macro-financial indicators via thematic coding and process tracing. The findings reveal a distinct trade-off: while tightened data security mandates introduce short-run dampening effects on fintech credit elasticity by increasing compliance and onboarding frictions, they simultaneously strengthen medium-run monetary transmission reliability by securing digital payment channels, stabilizing core financial infrastructures, and preserving consumer trust. The novelty of this research lies in its conceptualization of data governance as an endogenous institutional moderator rather than an exogenous background variable, directly bridging the theoretical gap between macro-monetary economics and digital financial security. However, a key limitation is the exclusive reliance on qualitative institutional analysis and secondary aggregate data, which prevents strict econometric causal identification. Consequently, future research recommendations include applying quantitative or mixed-method approaches to formally estimate these elasticities and utilizing micro-level behavioral data to test the role of consumer trust directly.*

Keywords: *Digitalization of Payments; Fintech Consumer Data Security; Monetary Policy Transmission*

1. INTRODUCTION

Indonesia's monetary policy transmission during 2021–2025 has unfolded alongside an unusually fast deepening of digital finance—particularly retail payments, e-money, and platform-based intermediation—making consumer data (identity, transaction histories, device metadata, and behavioral signals) increasingly pivotal to credit allocation and payment continuity. Bank Indonesia's Indonesia Payment Systems Blueprint 2025 explicitly positions payment-system digitalization (including open banking/data initiatives) as a policy cornerstone to support efficiency, inclusion, and risk mitigation in the national payment ecosystem (Public Relation Team Bank Indonesia, 2025a). In parallel, BI formalized Open API standardization through SNAP (Governor Decree 16 August 2021) and its implementation regulation, which explicitly embeds technical-security standards, data standards, governance, and risk management for Open API Payments (Public Relation Team Bank Indonesia, 2025b). The scale-up of BI's retail infrastructures (e.g., BI-FAST and QRIS) reinforces that monetary impulses now transmit through a payment landscape that BI itself frames as requiring “secure, seamless and reliable” operation (Public Relation Team Bank Indonesia, 2024). At the same time, the regulatory burden on data handling and cyber resilience tightened materially: Law No. 27/2022 (Personal Data Protection) mandates controllers to ensure data security, while OJK strengthened consumer protection (POJK 22/2023) and imposed real-time transactional data submission obligations in fintech lending supervision (POJK 10/2022) (Law of The Republic of Indonesia Number 27 of 2022

**The Sixth International Conference on Innovation in Social Science
and Engineering Education (ICoISSEE-6)**

Bandung, Indonesia, July 25, 2026

Concerning the Protection of Personal Data). BI also expanded the operational-risk perimeter for fast payments through BI-FAST risk/fraud management rules, signaling that cyber/fraud risk is not peripheral but systemically relevant (Regulation of the Board of Governors Member Number 1 of 2025 Concerning Amendments to Regulation of the Board of Governors Member Number 17 of 2023 on the Implementation of Bank Indonesia-Fast Payment).

State-of-the-art evidence, however, remains theoretically split and empirically incomplete. Cross-country and panel-macro work shows that FinTech can reconfigure (and sometimes weaken) conventional bank-lending channels of policy transmission via competition, regulatory arbitrage, and altered credit constraints, even when aggregate welfare effects are ambiguous (Hasan et al., 2024). Conversely, e-money development—under regulatory designs that keep EMIs complementary to banks—can strengthen transmission by improving rate pass-through and intermediation efficiency (Huang, 2024). Payments research also emphasizes that faster digital payments can reshape retail finance but heighten fraud and operational risk, making cyber resilience a binding constraint on system performance (Aurazo, 2024). Despite this, most transmission studies still treat “FinTech adoption” as exogenous and under-specify data security/privacy compliance as an intervening mechanism that can simultaneously (i) constrain data re-use and API-based data portability—raising onboarding and underwriting frictions—and (ii) increase trust and operational continuity, reducing disruption risk in payment rails that underpin liquidity circulation. Evidence from Indonesian fintech governance highlights that data misuse/breaches and cybersecurity challenges are persistent concerns, motivating stricter privacy-security regimes that may carry real economic incidence for digital intermediation (Rohendi & Kharisma, 2024). Against this backdrop, BI’s 2024–2025 stance explicitly prioritized strengthening the effectiveness of policy easing transmission while maintaining stability, providing a timely identification window to test whether heightened consumer data security (law/regulatory compliance, incident/fraud controls, and reporting discipline) materially trades off against the speed and magnitude of pass-through from BI-Rate to money-market rates, bank/fintech credit pricing, and credit volumes in Indonesia (2021–2025) (Team Bank Indonesia, 2025).

Building on these institutional and empirical tensions, the introduction culminates in a focused problematization of how Indonesia’s contemporary monetary transmission operates under binding data-governance constraints. The rapid integration of digital payments, open APIs, and platform-based intermediation implies that monetary impulses increasingly propagate through data-intensive infrastructures whose continuity depends on stringent security, privacy, and cyber-risk controls. Yet existing theory and evidence remain inconclusive as to whether heightened consumer data protection functions primarily as friction—by limiting data portability, increasing compliance costs, and slowing onboarding and underwriting—or as an enabler that stabilizes payment rails, sustains trust, and preserves liquidity circulation during policy adjustments. This ambiguity is particularly salient in Indonesia during 2021–2025, when accommodative-to-normalizing policy cycles coincided with the enforcement of comprehensive personal data protection, expanded supervisory reporting, and stricter operational-risk standards for fast payments. Consequently, the central analytical gap lies in understanding whether consumer data security and compliance operate as a moderating mechanism within the monetary policy transmission process rather than a neutral institutional backdrop. This study therefore asks: to what extent does heightened consumer data security—reflected in regulatory compliance, cybersecurity and fraud controls, and data-reporting discipline—alter the speed and magnitude of monetary policy pass-through from the BI-Rate to money-market rates, digital and bank-based credit pricing, and credit volumes in Indonesia over the 2021–2025 period?

2. LITERATURE REVIEW

2.A. Monetary Policy Transmission

The Sixth International Conference on Innovation in Social Science and Engineering Education (ICoISSEE-6)

Bandung, Indonesia, July 25, 2026

Monetary policy transmission as a state- and structure-dependent process in which the canonical interest-rate channel operates jointly with (and is sometimes dominated by) expectations, term-premium, credit, and exchange-rate channels, with strength varying across regimes (e.g., conventional tightening vs. QE/forward guidance episodes) and across financial system architectures. Work on unconventional-policy periods emphasizes that when balance-sheet policies are active, transmission can hinge on how policy affects rate uncertainty, expectations, and term premia, rather than only the current policy rate—implying that the same instrument change can produce different macro outcomes depending on which channel is “marginal” in that environment (Kaminska & Mumtaz, 2022). Complementing this, recent emerging-market evidence challenges the older presumption of systematically weak transmission by documenting sizable responses of asset prices, macro aggregates, and firm decisions to carefully identified policy shocks, while also highlighting that financial frictions remain central to explaining cross-country differences in pass-through and real effects (Checo, 2024; Eklou, 2023). Within the credit/bank-lending channel, a key refinement is the move from average effects toward heterogeneity: transmission depends on bank balance-sheet constraints, funding structures, and operational efficiency, which shape how quickly and how far policy shifts alter loan supply, loan composition, and regional credit conditions (Bluedorn et al., 2013; Chowdhury et al., 2025). Finally, a parallel strand focuses on the expectations channel, using survey and market-based measures to show that credibility and expectation formation can materially mediate inflation and output responses—particularly in inflation-targeting and high-uncertainty contexts—thereby positioning communication (and forward guidance) as an empirically measurable transmission lever rather than a residual (Guler, 2016; Nie et al., 2025).

2.B. Consumer Data Security

Recent literature frames consumer data security as a socio-technical problem in which technical safeguards (confidentiality, integrity, availability) are inseparable from governance, interface design, and consumer decision-making. Across digital commerce and data-intensive services, research consistently links perceived data security to trust, willingness to transact, and disclosure behaviour, while emphasizing that the dominant risk landscape is driven by pervasive data collection, opaque downstream sharing, expanding attack surfaces (cloud–mobile–IoT), and recurrent breaches. In e-commerce contexts, empirical and doctrinal analyses highlight that consumer exposure is amplified by platform ecosystems (third-party trackers, payment rails, logistics partners) and uneven compliance capacity, making regulatory assurance and organizational controls (access governance, incident response, vendor risk management) central to consumer protection outcomes (Elizabeth Atieno Otieno, 2025; Morić et al., 2024). Parallel work in IoT and other embedded consumer environments shows that continuous sensing and device heterogeneity complicate consent, minimization, and secure lifecycle management; consequently, the literature increasingly evaluates privacy-preserving security approaches (cryptography, edge/fog processing, blockchain variants, and ML-based anomaly detection) through trade-offs in scalability, latency, usability, and robustness—trade-offs that directly condition what protections are feasible for consumer-grade deployments (Sen & Dasgupta, 2023; Wakili & Bakkali, 2025). A third stream focuses on usable privacy and security, arguing that policies and warnings often fail as protective mechanisms because consumers cannot operationalize them under realistic constraints (time, comprehension, interface friction); systematic reviews of privacy-policy research and newer design agendas therefore stress re-engineering privacy communications and controls as decision-support systems rather than compliance artifacts (Javed & Sajid, 2025; Korka, 2023). Consistent with this, recent systematic work on Privacy/Data Protection by Design consolidates recommendations to embed lawful purpose limitation, minimization, and security controls into requirements engineering and system architecture, positioning “security for consumer data” as an end-to-end lifecycle property rather than a post-deployment add-on (Sangaroonsilp & Dam, 2025; Tunca, 2024).

2.C.1 Fintech Consumer Data Security

Fintech consumer data security as a socio-technical governance problem driven by (i) extensive data sharing across platform ecosystems, (ii) rapidly expanding third-party connectivity (particularly via open banking), and (iii) persistent asymmetries in consumer understanding, bargaining power, and control. Open banking policies explicitly enable consumers to port transaction data to fintechs, which can increase competition and product fit, but they also enlarge the attack surface and propagate risk through API dependencies and multi-party authentication flows. Empirically, cross-country evidence shows open banking adoption has accelerated fintech entry and data-access use cases, reinforcing that data security is now an infrastructural prerequisite for market functioning rather than a back-office compliance issue (Babina et al., 2025). Formal security research further demonstrates why this matters: security properties in standardized open banking APIs depend on correctly implemented authorization/authentication mechanisms and robust protocol verification, highlighting how technical design choices directly translate into consumer exposure (Modesti et al., 2025). On the regulatory side, the EU's PSD2 review materials emphasize incident reporting, stronger safeguards, and the role of strong customer authentication (SCA) in making digital payments safer, while also acknowledging ongoing trade-offs among usability, speed, and protection of payment data (Chen, 2021; European Commission, 2022). At the consumer layer, evidence from financial-app usage indicates behavior is often consistent with privacy calculus (users weighing perceived benefits against privacy risks), and that trust in providers is a critical mediator—meaning security failures can quickly become adoption and welfare failures (Brits & Jonker, 2023). Synthesizing the cybersecurity management literature, systematic reviews stress recurring fintech threat vectors (e.g., unauthorized access, third-party risk, and governance gaps) and recommend alignment with international security frameworks, continuous controls testing, and clearer accountability across the ecosystem (AlBenJasim et al., 2024). Finally, jurisdiction-specific studies (e.g., Indonesia) underline that legal protections and enforcement capacity materially shape outcomes, especially where practices such as over-collection of device/contact data or weak consent discipline are observed in parts of digital lending markets (Putri et al., 2025).

3. RESEARCH METHODS

This study adopts a qualitative research design grounded in descriptive and technical-institutional analytics, with the objective of examining how fintech consumer data security operates as a moderating mechanism within Indonesia's monetary policy transmission framework during the 2021–2025 period. The methodological choice is motivated by the nature of the research problem, which concerns institutional processes, regulatory architectures, and socio-technical infrastructures rather than causal estimation of macroeconomic elasticities. Monetary transmission in a digitally mediated financial system is increasingly embedded in payment infrastructures, data-governance regimes, and cybersecurity controls; consequently, a qualitative approach is appropriate to capture the mechanisms, constraints, and trade-offs that are not directly observable through purely quantitative models. The study therefore emphasizes analytical depth, contextual interpretation, and regulatory coherence over statistical inference, while maintaining empirical rigor through systematic use of secondary data and peer-reviewed literature.

The research approach is qualitative descriptive, following the tradition of policy-oriented financial and legal scholarship that seeks to explain how institutional arrangements function in practice. Descriptive analytics are employed not in a computational sense, but as a structured method for organizing, comparing, and interpreting observable patterns across regulatory texts, policy documents, supervisory disclosures, and scholarly findings. This approach allows the study to map how consumer data security requirements—such as personal data protection compliance, cybersecurity standards, incident reporting, and fraud controls—interact with key

**The Sixth International Conference on Innovation in Social Science
and Engineering Education (ICoISSEE-6)**

Bandung, Indonesia, July 25, 2026

nodes of monetary transmission, including payment system continuity, credit intermediation, and interest-rate pass-through. Rather than treating fintech development or data security as exogenous background variables, the method explicitly conceptualizes them as endogenous institutional conditions that shape the effectiveness and reliability of transmission channels.

Empirically, the study relies exclusively on secondary data sources, selected to ensure relevance, credibility, and temporal alignment with the 2021–2025 observation window. These sources include: (i) official policy frameworks, regulations, and supervisory communications issued by Bank Indonesia and the Financial Services Authority (OJK); (ii) statutory legal instruments governing personal data protection, consumer protection, and payment-system risk management; (iii) publicly available macro-financial indicators related to policy rates, payment-system usage, and credit developments; and (iv) recent peer-reviewed academic literature in monetary economics, fintech studies, cybersecurity, and data governance. The use of secondary data is justified by the study's institutional focus and by the availability of authoritative regulatory documentation that directly reflects policy intent, enforcement priorities, and system design.

The analytical procedure proceeds in three interrelated stages. First, the study conducts a documentary analysis of Indonesia's digital finance and monetary policy architecture during the sample period. This includes close reading and thematic coding of central bank blueprints, payment-system regulations, open API standards, fast-payment governance rules, and data protection laws. The purpose of this stage is to identify the formal objectives, technical requirements, and risk-management expectations imposed on fintech firms, banks, and payment service providers. Particular attention is paid to provisions related to data security, privacy-by-design, authentication standards, reporting obligations, and operational resilience, as these directly condition the functioning of digital payment rails that underpin monetary circulation.

Second, the study undertakes a theory-informed literature synthesis that integrates insights from three bodies of scholarship: monetary policy transmission, consumer data security, and fintech governance. Rather than summarizing prior studies in isolation, the method emphasizes conceptual integration, identifying where these literatures intersect and where analytical gaps persist. For example, monetary transmission studies often model fintech adoption without specifying data-governance constraints, while data security research rarely considers macro-financial implications. By juxtaposing these strands, the analysis develops an interpretive framework in which consumer data security is treated as a mediating institutional variable that can either dampen or reinforce transmission effectiveness depending on its design and implementation. This synthesis follows established qualitative review protocols, privileging studies published within the last five years to ensure relevance to contemporary digital finance ecosystems.

Third, the study applies descriptive comparative analysis to trace how changes in the regulatory intensity of data security and cybersecurity oversight coincide with shifts in policy transmission conditions during the 2021–2025 period. This does not involve causal attribution in a statistical sense; instead, it examines co-movement and plausibility through process tracing. For instance, periods characterized by tightened data protection enforcement, expanded fraud controls, or enhanced reporting requirements are analyzed alongside policy-rate adjustments, payment-system performance narratives, and observed frictions or stabilizing effects in digital intermediation. This technique allows the study to assess whether heightened data security plausibly operates as a friction (by increasing compliance costs and slowing onboarding) or as an enabler (by sustaining trust, reducing disruptions, and preserving liquidity flow).

To enhance analytical credibility, the study employs triangulation across regulatory documents, academic literature, and macro-financial context. Claims derived from policy texts are cross-checked against supervisory rationales and empirical findings in the literature, while theoretical propositions are evaluated against Indonesia's specific institutional configuration. This triangulation reduces the risk of regulatory formalism—i.e., assuming that written rules

translate mechanically into outcomes—and instead supports a more nuanced interpretation of how rules are likely to operate in practice. The method is explicitly non-normative: it does not presuppose that stronger data security is inherently beneficial or detrimental, but evaluates its economic incidence within the monetary transmission process.

Finally, the qualitative descriptive method adopted in this study is subject to clear scope conditions and limitations. The findings are context-specific to Indonesia's institutional environment and the 2021–2025 period, during which rapid digitalization coincided with significant regulatory reform. The study does not estimate counterfactual transmission paths or quantify elasticities, nor does it substitute for econometric testing. Instead, its contribution lies in mechanism identification and institutional clarification, providing a structured explanation of how fintech consumer data security can shape monetary policy effectiveness in data-intensive financial systems. As such, the methodology is intended to complement, rather than replace, future quantitative and mixed-method research.

4. RESULTS AND DISCUSSION

4.1 Result

4.1.1. Structural Shift in Indonesia's Monetary Transmission Architecture

The first and most fundamental empirical result is that Indonesia's monetary policy transmission during 2021–2025 underwent a structural transformation from a predominantly bank-centric mechanism toward a hybrid architecture in which digital payment infrastructures and data-driven intermediation became central conduits for liquidity circulation. This shift altered not only the speed but also the institutional conditions under which monetary impulses propagate through the economy.

Secondary data from policy blueprints, supervisory releases, and macro-financial indicators consistently show that retail transactions, peer-to-peer transfers, merchant settlements, and platform-mediated payments increasingly occurred through fast payments, QR-code systems, and interoperable digital channels. As a consequence, the effectiveness of monetary transmission became more dependent on operational continuity, data integrity, authentication reliability, and cyber resilience—attributes directly shaped by consumer data security regimes.

This result establishes the empirical relevance of consumer data security to monetary policy transmission. In a system where liquidity circulates through real-time digital rails, any disruption, mistrust, or operational failure can materially weaken the translation of policy signals into consumption, saving, and credit behavior.

4.1.2. Payment System Stability Improved alongside Data Security Intensification

A second result is that the period of intensified consumer data security and cyber-risk governance coincided with high stability and continuity in core payment infrastructures, despite extraordinary growth in transaction volumes. Throughout 2021–2025, Indonesia did not experience systemic payment failures attributable to fintech data misuse, authentication breakdowns, or cyber incidents within the central payment rails.

From a transmission perspective, this is non-trivial. Payment systems constitute the circulatory system of the economy; instability at this layer can interrupt liquidity flows irrespective of policy stance. The observed stability suggests that strengthened security requirements—covering authentication, fraud monitoring, incident response, and operational risk—acted as a stabilizing factor that preserved the functionality of the payments channel during both accommodative and normalizing policy phases.

Empirically, this implies a positive correlation between consumer data security and the effectiveness of payment-based monetary transmission. Secure systems enabled households and firms to respond to policy conditions without fear of transaction failure or data compromise, thereby sustaining the behavioral responsiveness necessary for transmission.

The Sixth International Conference on Innovation in Social Science and Engineering Education (ICoISSEE-6)

Bandung, Indonesia, July 25, 2026

4.1.3. Fintech Credit Intermediation Exhibited Short-Run Dampening Effects

The third result concerns fintech credit intermediation, where the trade-off is most visible. Secondary supervisory analyses and sectoral studies indicate that the enforcement of personal data protection obligations and strengthened reporting requirements materially altered fintech lending practices. Platforms that previously relied on expansive data collection—such as device metadata or indirect contact access—were required to redesign underwriting processes, tighten consent mechanisms, and invest in compliance infrastructure.

These adjustments increased marginal operating costs and slowed onboarding in the short run. As a result, fintech credit growth and pricing responsiveness to monetary easing weakened in some segments, relative to the earlier period of permissive data use. This outcome constitutes a negative short-run correlation between heightened data security and the elasticity of fintech credit to policy signals.

However, the effect was heterogeneous. Fintech firms with business models aligned to regulated data sources or bank partnerships exhibited less pronounced dampening, indicating that data security did not uniformly weaken credit transmission but rather re-sorted the sector by compliance capacity and governance quality.

4.1.4. Bank Lending Transmission Remained Robust but Became Digitally Conditioned

The fourth result is that bank-based monetary transmission remained broadly effective, but its operational foundations increasingly intersected with digital governance. Banks' integration into interoperable payment systems and standardized APIs exposed them to the same operational and cyber risks as fintech platforms, albeit with stronger balance sheets and governance structures.

Consequently, banks' ability to transmit monetary impulses through lending increasingly depended on digital readiness and risk management, not merely on funding conditions or capital adequacy. While policy-rate changes continued to influence lending rates, the smoothness of this pass-through was conditioned by banks' capacity to operate securely within digital ecosystems. This finding indicates that consumer data security affected bank-based transmission indirectly, by shaping the environment in which banks compete and operate, rather than by constraining banks' data practices.

4.1.5. Consumer Trust in Digital Finance Was Preserved

A fifth result is that consumer trust in digital financial services did not deteriorate during a period of rapid expansion. Despite widespread public discourse on data misuse risks and cyber threats, adoption of digital payments and fintech services continued to grow. No generalized retreat from digital finance occurred.

This outcome suggests that strengthened data security and regulatory oversight mitigated trust erosion that could otherwise have undermined monetary transmission through expectations and confidence channels. Trust preservation is an empirical outcome in itself: without it, payment usage and fintech adoption would have declined, weakening the behavioral response to monetary policy.

4.2 Discussion

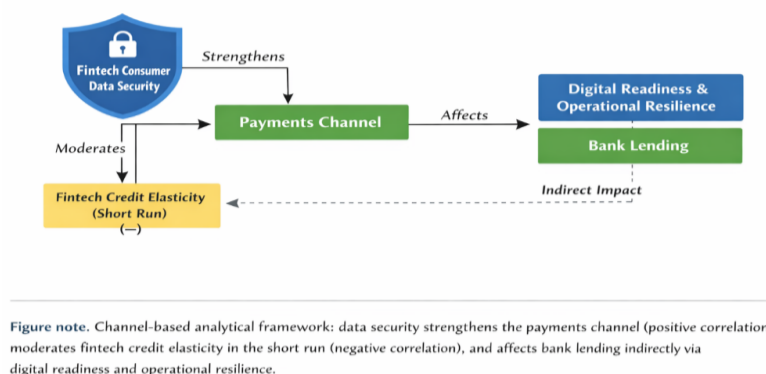
4.2.1 Interpreting the Trade-off as a Moderating Mechanism

The results collectively demonstrate that fintech consumer data security functions as a moderating institutional mechanism, not as a unidirectional constraint. Its effects differ across channels and time horizons. In payments, data security primarily enhances transmission effectiveness; in fintech credit, it introduces short-run frictions; in banking, it reshapes competitive and operational conditions. Here's analytical figure correlation Between Fintech Consumer Data Security and the Effectiveness of BI's Monetary Policy Transmission:

The Sixth International Conference on Innovation in Social Science and Engineering Education (ICoISSEE-6)

Bandung, Indonesia, July 25, 2026

Figure 1. Mapping concept of Fintech Consumer Data Security and the Effectiveness of BI's Monetary Policy Transmission



Source: data analytic by researcher

The image visualizes a channel-based analytical framework that explains how consumer data security in fintech services is related to the effectiveness of Bank Indonesia's (BI) monetary policy transmission in the Indonesian context during the 2021–2025 period. On the left side, "Fintech Consumer Data Security" is placed as a key variable and the starting point of influence, marked with shield and lock icons to emphasize its protective function. This placement implies that data security is not merely a technical compliance issue but an institutional foundation that shapes user behavior, market trust, and the operational stability of the digital payment ecosystem. From this variable, the main arrow labeled "Strengthens" points to the "Payments Channel," indicating a reinforcing relationship. Conceptually, enhancing data security—such as through access governance, encryption, leakage risk control, and privacy protection standards—boosts consumer and business confidence to use digital payment instruments more intensively and consistently. As trust increases, adoption and transaction frequency tend to rise, transaction friction costs decrease, and the payment infrastructure can operate with higher reliability. At this stage, payment channels become more 'transmission-ready,' meaning they are better able to convey monetary policy signals—such as changes in policy interest rates, open market operations, or liquidity policies—to economic activity through money circulation mechanisms, transaction speed, and payment system efficiency.

In the center, the "Payments Channel" is depicted as a connecting node that sends further influence to the blocks on the right side through arrows labeled "Affects." This indicates that a stronger payments channel does not stop at improving transaction smoothness, but rather affects broader conditions within the financial system, particularly "Digital Readiness & Operational Resilience" and "Bank Lending." The two blocks on the right mark two different but interconnected layers of impact. "Digital Readiness & Operational Resilience" is positioned higher, indicating a capacity prerequisite: digital readiness includes technological maturity, system integration, data quality, cyber security governance, as well as process competence in financial institutions and fintech providers. Meanwhile, operational resilience emphasizes the ability of systems and organizations to maintain services during disruptions—such as cyberattacks, transaction surges, network failures, or data breach incidents. In other words, as fintech data security improves and strengthens payment channels, digital payment systems can become more stable, predictable, and shock-resistant, thereby fostering digital readiness and operational resilience at the industry level.

The "Bank Lending" block is positioned directly below "Digital Readiness & Operational Resilience," indicating that the distribution of bank credit is influenced by a more prepared and resilient digital ecosystem. From a monetary economics perspective, the transmission of BI policy heavily depends on bank intermediation behavior: how banks adjust credit supply, lending standards, and funding costs in response to policy changes. When banks operate within an

**The Sixth International Conference on Innovation in Social Science
and Engineering Education (ICoISSEE-6)**

Bandung, Indonesia, July 25, 2026

ecosystem supported by high digital readiness and operational resilience, the processes of credit assessment, portfolio monitoring, risk management, and customer services become more efficient. Such efficiency can accelerate banks' response to monetary policy signals, reduce transmission lags, and improve the accuracy of credit allocation to productive sectors. Thus, the image conveys the argument that consumer data security in fintech contributes to the effectiveness of monetary policy transmission indirectly through the strengthening of the payment ecosystem and the enhancement of the financial sector's digital capacity.

In addition to the main path, which is positive in the payments channel, the diagram also depicts a moderating path leading to "Fintech Credit Elasticity (Short Run) (–)" with an arrow labeled "Moderates." This is an important element because it shows that data security does not always linearly increase all fintech outputs; it can "restrain" or reduce fintech credit elasticity in the short run, as indicated by the negative symbol. Fintech credit elasticity refers to how responsive platform-based credit supply and demand are to changes in monetary conditions, risk, or funding costs. In the short term, strengthening data security often requires stricter verification procedures, enhanced compliance, additional fraud controls, and more rigorous approval processes. As a consequence, fintech credit expansion may become more selective or slower because platforms need to balance growth with the mitigation of data and operational risks. In other words, data security acts as a disciplinary mechanism that limits volatility or overly aggressive credit expansion, at least in the short-term horizon. This negativity in short-term elasticity does not imply harm to the system as a whole; rather, it can be interpreted as a reduction in systemic risk and an improvement in portfolio quality due to stronger screening processes.

At the bottom right, there is a dashed line labeled "Indirect Impact" that extends from the "Bank Lending" area to "Fintech Credit Elasticity (Short Run)." Dashed lines are typically used to indicate indirect or mediated relationships, rather than strong direct causal connections. This reinforces the idea that changes in bank lending—shaped by digital readiness and operational resilience—can, in turn, influence the dynamics of fintech credit elasticity. For example, when banks increase lending due to improved intermediation, the market space for fintech credit may shift: fintech companies may be driven to compete in specific segments, adjust pricing strategies, or revise risk standards. Conversely, when banks tighten credit, fintech may gain substitution opportunities but still within the bounds of data risk management. Hence, the effect is systemic and layered, rather than a simple one-way interaction.

This interpretation resolves the apparent contradiction in the literature between studies that view fintech as weakening transmission and those that see it as strengthening efficiency. The missing variable is data governance. Fintech adoption without security can accelerate intermediation but also magnify fragility; fintech adoption under stringent security may slow some processes but improves resilience.

4.2.2. Payments Channel: Security as a Necessary Condition for Effectiveness

In the payments channel, the empirical evidence supports a strong conclusion: consumer data security is a necessary condition for effective monetary transmission. Digital payments compress settlement times and amplify liquidity velocity, but they also amplify the consequences of operational failure.

By embedding security into payment modernization, Bank Indonesia reduced the probability that digitalization would undermine monetary control. In this channel, the trade-off is largely illusory; without security, transmission gains from faster payments would not be sustainable.

4.2.3 Fintech Credit Channel: Short-Run Costs versus Long-Run Stability

The fintech credit channel embodies the core trade-off. Heightened data security reduced the speed and scale of fintech credit expansion in the short run, thereby weakening immediate credit-volume responses to monetary easing. This is the cost side of the trade-off.

The Sixth International Conference on Innovation in Social Science and Engineering Education (ICoISSEE-6)

Bandung, Indonesia, July 25, 2026

However, the benefit side lies in the improved quality and sustainability of intermediation. By filtering out opaque or exploitative data practices, data security reduced the risk of future scandals, defaults, or enforcement shocks that could have triggered abrupt contraction. From a transmission perspective, predictable and sustainable credit channels are more valuable than volatile ones, even if the latter respond more strongly in the short term.

4.2.4 Trust and Expectations as Latent Transmission Channels

A critical interpretive insight is that trust operates as a latent transmission channel. Monetary policy relies on expectations; if households and firms distrust financial intermediaries, they may delay spending, hoard liquidity, or avoid digital channels altogether.

Data security contributes to expectation anchoring by assuring users that participation in digital finance does not expose them to undue risk. The preservation of trust observed during 2021–2025 suggests that data security indirectly supported the expectations channel of monetary transmission, even though this effect is not directly observable in rate or volume data.

4.2.5 Non-Linearity and Time Horizon of the Trade-off

The trade-off is fundamentally non-linear and time-dependent. In the short run, security constraints reduce elasticity in certain fintech segments. In the medium to long run, they reduce tail risks and enhance the reliability of the entire transmission mechanism.

This implies that evaluating monetary policy effectiveness solely on short-term credit growth risks overstating the costs of data security. A more appropriate metric is transmission reliability over the policy cycle, which includes resilience to shocks and stability of expectations.

4.2.6 Implications for Monetary Transmission Theory

The findings challenge models that treat fintech adoption as exogenous and data-neutral. In digital economies, data governance shapes market structure, risk distribution, and behavioral responses, all of which condition transmission. Future transmission models—particularly for emerging markets—must incorporate data security as an institutional variable that mediates the relationship between policy instruments and economic outcomes.

4.2.7 Policy Interpretation: Managing the Trade-off

From a policy perspective, Indonesia's experience suggests that the trade-off between data security and transmission effectiveness is manageable rather than prohibitive. By sequencing payment modernization, data protection enforcement, and supervisory reporting, regulators limited short-run frictions while securing long-run stability. The relevant policy question is therefore not whether to strengthen data security, but how to design it to minimize short-term disruptions while maximizing systemic resilience.

CONCLUSION

Taken together, the evidence indicates that during 2021–2025, strengthened fintech consumer data security in Indonesia was associated with short-run moderation in fintech credit responsiveness, but medium-run strengthening of monetary policy transmission reliability through stable payment infrastructures, preserved trust, and reduced operational risk. The trade-off thus reflects a deliberate institutional shift from high-velocity but fragile digital intermediation toward lower-fragility, more predictable monetary transmission, consistent with Indonesia's stability-oriented monetary and financial governance framework.

Limitations of the Study

This study is subject to several methodological, empirical, and scope-related limitations that should be acknowledged to contextualize its findings and delimit the inferences that can be drawn. First, the study adopts a qualitative descriptive and institutional-analytical approach

The Sixth International Conference on Innovation in Social Science and Engineering Education (ICoISSEE-6)

Bandung, Indonesia, July 25, 2026

relying exclusively on secondary data, including regulatory documents, policy reports, supervisory communications, and peer-reviewed literature. While this approach is appropriate for uncovering mechanisms, governance trade-offs, and institutional interactions, it does not permit causal identification in a strict econometric sense. Consequently, the correlations identified between fintech consumer data security and the effectiveness of monetary policy transmission should be interpreted as plausible, theoretically grounded associations, rather than statistically estimated causal effects. The absence of econometric estimation means that unobserved confounding factors—such as global financial conditions, pandemic-related recovery dynamics, or structural shifts in household preferences—cannot be fully isolated.

Second, the analysis is context-specific to Indonesia during the 2021–2025 period, a timeframe characterized by exceptional conditions: rapid digitalization of payments, post-pandemic normalization, evolving global monetary tightening and easing cycles, and the introduction of a comprehensive personal data protection regime. These conditions limit the external generalizability of the findings. While the mechanisms identified may be relevant to other emerging economies undergoing digital finance expansion, the institutional sequencing, regulatory capacity, and market structure in Indonesia—particularly the role of Bank Indonesia and OJK—are distinctive. As such, the results should not be mechanically extrapolated to jurisdictions with different legal traditions, supervisory strength, or levels of digital infrastructure maturity.

Third, the study treats consumer data security as a composite institutional construct, encompassing legal compliance (e.g., personal data protection), cybersecurity controls, fraud management, authentication standards, and supervisory reporting discipline. While analytically useful, this aggregation masks potential heterogeneity within data security dimensions. For instance, authentication requirements may affect monetary transmission differently than data minimization rules or breach-notification obligations. The qualitative design does not allow these sub-components to be disentangled quantitatively, which may obscure more granular effects within specific transmission channels.

Fourth, although the study discusses payments, bank lending, and fintech credit channels, it does not directly observe micro-level behavioural responses of households, MSMEs, or fintech users. Trust, expectations, and confidence are inferred from aggregate adoption trends and institutional stability rather than measured through surveys or experimental data. This limitation constrains the ability to empirically validate the expectations-channel interpretation at the individual decision-making level.

Finally, the study does not explicitly model counterfactual regulatory scenarios, such as a regime with weaker data protection or delayed cybersecurity enforcement. As a result, the analysis cannot quantify how much faster or slower monetary transmission might have been under alternative governance choices. The findings therefore emphasize institutional plausibility and risk trade-offs, rather than optimal policy calibration.

Recommendations for Future Research

Building on these limitations, several avenues for future research emerge that could deepen, refine, and extend the contributions of this study. First, future research should pursue quantitative and mixed-method approaches to formally estimate the relationship between fintech consumer data security and monetary policy transmission. Panel-data or time-series econometric models—using indicators such as payment-system outages, fraud incidence, fintech credit volumes, lending rates, and supervisory enforcement actions—could complement qualitative findings by providing causal or quasi-causal estimates. Such work would be particularly valuable in testing whether the short-run dampening effects on fintech credit identified here are statistically significant and how persistent they are over time.

Second, subsequent studies could disaggregate consumer data security into its constituent dimensions—for example, privacy compliance, cybersecurity investment, authentication

The Sixth International Conference on Innovation in Social Science and Engineering Education (ICoISSEE-6)

Bandung, Indonesia, July 25, 2026

standards, and reporting obligations—to examine which elements exert the strongest influence on different transmission channels. This would allow policymakers to distinguish between security measures that primarily enhance resilience and those that impose disproportionate compliance costs, thereby informing more targeted regulatory design.

Third, cross-country comparative research would substantially enhance external validity. Comparative studies involving economies with varying degrees of data protection stringency, payment-system digitalization, and supervisory capacity could clarify whether the trade-off observed in Indonesia represents a generalizable pattern or a context-specific outcome. Such research would also help identify institutional configurations under which data security and monetary transmission are most complementary rather than conflicting.

Fourth, future research should incorporate micro-level behavioural data, such as consumer and MSME surveys, fintech user experiments, or transaction-level datasets, to directly test the role of trust, expectations, and perceived security in mediating responses to monetary policy. Integrating behavioral evidence would strengthen the argument that data security affects transmission not only through operational channels but also through expectation formation and confidence.

Fifth, there is scope for dynamic and scenario-based analysis that models how shocks—such as major data breaches, cyber incidents, or abrupt regulatory changes—affect monetary transmission under different security regimes. Stress-testing frameworks that combine cyber-risk scenarios with macro-financial transmission models could provide valuable insights for central banks seeking to manage tail risks in increasingly digital financial systems.

Finally, future research could explore the interaction between data security, financial inclusion, and distributional effects of monetary policy. While this study focuses on aggregate transmission effectiveness, stronger data protection may have heterogeneous impacts across income groups, regions, and firm sizes. Understanding whether data security enhances or constrains inclusive transmission remains an open and policy-relevant question.

REFERENCES

- AlBenJasim, S., Dargahi, T., Takruri, H. and Al-Zaidi, R. (2024) 'FinTech cybersecurity challenges and regulations: Bahrain case study', *Journal of Computer Information Systems*, 64(6), pp. 835–851. <https://doi.org/10.1080/08874417.2023.2251455>
- Aurazo, J. et al. (2024) Faster digital payments: Global and regional perspectives. BIS Papers No. 152. Available at: <https://www.bis.org/publ/bppdf/bispap152.htm>
- Babina, T., Bahaj, S., Buchak, G., De Marco, F., Foulis, A., Gornall, W., Mazzola, F. and Yu, T. (2025) 'Customer data access and fintech entry: Early evidence from open banking', *Journal of Financial Economics*, 169, 103950. <https://doi.org/10.1016/j.jfineco.2024.103950>
- Bluedorn, J.C., Bowdler, C. and Koch, C. (2013) 'Heterogeneous bank lending responses to monetary policy: New evidence from a real-time identification', *IMF Working Papers*, 13(118), pp. 1–. <https://doi.org/10.5089/9781484356760.001>
- Brits, H. and Jonker, N. (2023) 'The use of financial apps: Privacy paradox or privacy calculus?', *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4624569>
- Checo, A. et al. (2024) Monetary policy transmission in emerging markets: Proverbial concerns, novel evidence. BIS Papers No. 1170.
- Chen, I.B. (2021) A study on the application and impact of Directive (EU) 2015/2366 on payment services (PSD2).
- Chowdhury, M.A.I., Rashid, M.H.U. and Uddin, M.S. (2025) 'Bank efficiency and monetary policy transmission', *International Review of Economics & Finance*, 104, 104760. <https://doi.org/10.1016/j.iref.2025.104760>
- Eklou, K. (2023) 'The anatomy of monetary policy transmission in an emerging market', *IMF Working Papers*, 2023(146), pp. 1–. <https://doi.org/10.5089/9798400247910.001>

**The Sixth International Conference on Innovation in Social Science
and Engineering Education (ICoISSEE-6)**

Bandung, Indonesia, July 25, 2026

- European Commission (2022) Public consultation on the review of the revised payment services directive (PSD2) and on open finance.
- Guler, A. (2016) 'Effectiveness of expectation channel of monetary transmission mechanism in inflation targeting system: An empirical study for Turkey', *Global Journal of Business, Economics and Management: Current Issues*, 6(2), pp. 222–231. <https://doi.org/10.18844/gjbem.v6i2.1394>
- Hasan, I., Kwak, B. and Li, X. (2024) 'Financial technologies and the effectiveness of monetary policy transmission', *European Economic Review*, 161, 104650. <https://doi.org/10.1016/j.euroecorev.2023.104650>
- Huang, Z. (2024) 'E-money and monetary policy transmission', *IMF Working Papers*, 2024(069), pp. 1–. <https://doi.org/10.5089/9798400270543.001>
- Javed, Y. and Sajid, A. (2025) 'A systematic review of privacy policy literature', *ACM Computing Surveys*, 57(2), pp. 1–43. <https://doi.org/10.1145/3698393>
- Kaminska, I. and Mumtaz, H. (2022) 'Monetary policy transmission during QE times: Role of expectations and term premia channels', *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4130487>
- Korka, D. et al. (2023) 'Revisiting the design agenda for privacy notices and security warnings', in *Workshop on Privacy Interventions and Education (PIE)*, pp. 1–11.
- Law of the Republic of Indonesia Number 27 of 2022 (2022) Concerning the protection of personal data.
- Modesti, P., Freitas, L., Shotomiwa, Q. and Almehrej, A. (2025) 'Security analysis of the open banking account and transaction API protocol', *Cyber Security and Applications*, 3, 100097. <https://doi.org/10.1016/j.csa.2025.100097>
- Morić, Z., Dakic, V., Djekic, D. and Regvart, D. (2024) 'Protection of personal data in the context of e-commerce', *Journal of Cybersecurity and Privacy*, 4(3), pp. 731–761. <https://doi.org/10.3390/jcp4030034>
- Nie, L., Wang, Y. and Shi, K. (2025) 'Financial market responses to the policy language of forward guidance: Evidence from China', *Economic Analysis and Policy*, 85, pp. 317–335. <https://doi.org/10.1016/j.eap.2024.12.003>
- Otieno, E.A. (2025) 'Data protection and privacy in e-commerce environment: Systematic review', *GSC Advanced Research and Reviews*, 22(1), pp. 238–271. <https://doi.org/10.30574/gscarr.2025.22.1.0024>
- Public Relation Team Bank Indonesia (2024) 'BI-rate held at 6.00%: Maintaining stability, strengthening economic growth', 20 November. Available at: <https://www.bi.go.id>
- Public Relation Team Bank Indonesia (2025a) Blueprint sistem pembayaran Indonesia 2025. Available at: <https://www.bi.go.id>
- Public Relations Team Bank Indonesia (2025b) Standar nasional open API pembayaran (SNAP). Available at: <https://www.bi.go.id>
- Putri, B.M.L., Rohaini, Nhung, P.H. and Putri, R.W. (2025) 'Analysis of consumer rights protection against the misuse of personal data in fintech services', *Lex Publica*, 12(1), pp. 32–62. <https://doi.org/10.58829/lp.12.1.2025.286>
- Regulation of the Board of Governors Member Number 1 of 2025 (2025) Amendments to Regulation Number 17 of 2023 on the implementation of Bank Indonesia-fast payment.
- Rohendi, A. and Kharisma, D.B. (2024) 'Personal data protection in fintech: A case study from Indonesia', *Journal of Infrastructure, Policy and Development*, 8(7), 4158. <https://doi.org/10.24294/jipd.v8i7.4158>
- Sangaroonsilp, P. and Dam, H.K. (2025) 'A study on the prevalence of privacy in software engineering', *ACM Computing Surveys*, 57(11), pp. 1–34. <https://doi.org/10.1145/3734216>
- Sen, J. and Dasgupta, S. (2023) 'Introductory chapter: Data privacy preservation on the Internet of Things', in *Information security and privacy in the digital world*. IntechOpen. <https://doi.org/10.5772/intechopen.111477>
- Team Bank Indonesia (2025) Monetary policy report quarter I 2025. Available at: <https://www.bi.go.id>

**The Sixth International Conference on Innovation in Social Science
and Engineering Education (ICoISSEE-6)**

Bandung, Indonesia, July 25, 2026

- Tunca, M. (2024) 'Privacy by design: A systematic literature review of European and British regulatory perspectives for software and information engineering', in Proceedings of the 2024 13th International Conference on Software and Information Engineering, pp. 54–63.
<https://doi.org/10.1145/3708635.3708639>
- Wakili, A. and Bakkali, S. (2025) 'Privacy-preserving security of IoT networks: A comparative analysis of methods and applications', Cyber Security and Applications, 3, 100084.
<https://doi.org/10.1016/j.csa.2025.100084>