

Enhancing Customer Trust in Indonesian Digital Banking: The Moderating Role of Data Privacy Disclosure on AI-Driven Interactions

Natalia Ayu Hapsari^{1*} , Erny Sulistyaningsih² , Basneldi³ , Bakti Setiadi⁴ , Tri Susilowati⁵ 

^{1*,2}Faculty of Management and Business, Trisakti Institute of Transportation and Logistics, Indonesia

^{3,4,5}Sekolah Tinggi Penerbangan Aviassi Jakarta, Indonesia

*Corresponding Author Email: nataliaayu2812@gmail.com

Article History

Received: 07-05-2026

Revised: 12-06-2026

Published: 9-07-2026

Key Words:

AI-enabled interaction; Customer Trust; Data Privacy Disclosure; Digital Banking; Seabank; Moderated Regression; Indonesia

Abstract: Purpose: This study examines how AI-enabled banking interactions influence customer trust and whether data privacy disclosure strengthens this relationship among SeaBank users in DKI Jakarta, Indonesia. Design/methodology/approach: Drawing on the Stimulus-Organism-Response (S-O-R) framework and Social Identity Theory, the study employed an explanatory quantitative design. Data were collected through a structured online questionnaire from 180 active SeaBank depositors aged 18-35 years who had used AI-supported banking features at least three times in the previous three months. The data were analyzed using Ordinary Least Squares (OLS) regression and Moderated Regression Analysis (MRA). Findings: The results demonstrate that AI-enabled interaction has a positive and significant effect on customer trust, while data privacy disclosure also directly enhances trust. More importantly, the interaction term is positive and significant, indicating that transparent privacy disclosure strengthens the relationship between AI-enabled interaction and customer trust. The moderated model explains 56.4% of the variance in customer trust, with the interaction term adding 8.2% incremental explanatory power. Originality/value: This study advances digital banking trust literature by showing that AI-enabled service quality alone is insufficient to generate trust. In an emerging-market context, algorithmic convenience must be accompanied by visible, understandable, and controllable privacy disclosure. The findings extend the S-O-R framework by conceptualizing privacy disclosure as a trust-enabling boundary condition and offer actionable guidance for digital banks seeking to transform privacy governance into a competitive advantage.

How to Cite: Ayu, N., Sulistyaningsi, E., Basneldi, Setiadi, B., & Susilowati, T. (2026). Enhancing Customer Trust in Indonesian Digital Banking: The Moderating Role of Data Privacy Disclosure on AI-Driven Interactions . *JMET: Journal of Management Entrepreneurship and Tourism*, 4(2), 104–114. <https://doi.org/10.61277/jmet.v4i2.306>

 <https://doi.org/10.61277/jmet.v4i2.306>

This is an open-access article under the [CC-BY-SA License](#).



1. Introduction

Artificial intelligence (AI) is reshaping financial services by enabling banks to deliver more personalized, responsive, and automated customer experiences. In digital banking, AI-supported interfaces such as chatbots, robo-advisory tools, automated risk alerts, and personalized financial recommendations are increasingly embedded into everyday customer journeys. These technologies can reduce service friction and improve perceived convenience, but they also intensify questions about algorithmic opacity, personal data use, and institutional responsibility. Consumer research on AI emphasizes that customers do not experience AI merely as a technological tool; they also experience data capture, classification, delegation, and social interaction, all of which can produce both value and psychological tension (Puntoni et al., 2021). Therefore, digital banking

JMET Vol. 4, No.2 (July 2026)

trust should be understood not only as a function of technological efficiency but also as an outcome of how customers interpret the fairness, transparency, and safety of AI-mediated interactions.

The Indonesian digital banking market provides a particularly relevant context for examining this issue. Indonesia is one of Southeast Asia's most dynamic digital economies, and digital financial services have become part of daily life for urban consumers. Populix reported strong growth in Indonesia's digital banking ecosystem and noted that Bank Indonesia recorded digital banking transaction value of Rp5,570.49 trillion in May 2024, representing a 10.82% year-on-year increase (Populix, 2024). In a 2025 consumer insight article, Populix also identified SeaBank, Jago, and Blu by BCA Digital as the three most frequently selected digital banks for daily transactions, with SeaBank ranked first among the listed options (Populix, 2025). This market growth makes SeaBank an important empirical setting for understanding how AI-enabled interactions and privacy communication jointly influence customer trust.

Customer trust is central to digital banking because financial services require customers to rely on institutions that manage sensitive personal, behavioral, and transactional data. In AI-enabled banking, trust is more complex because users interact with automated systems that can personalize recommendations and support decisions but may also collect and infer data beyond what users fully understand. Previous studies in AI-enabled banking show that trust, security, awareness, and perceived usefulness are significant determinants of customer acceptance and satisfaction (Bharti et al., 2023; Ikhsan et al., 2025). However, a key challenge remains: the same personalization that improves service relevance may also trigger privacy concerns when users believe that banks collect, process, or share their data without sufficient transparency and control.

This tension is consistent with the broader data privacy literature. Martin et al. (2017) show that access to customer data can heighten perceived vulnerability and reduce trust, whereas transparency and control can suppress negative reactions to data use. Similarly, Martin and Murphy (2017) argue that privacy management is a strategic marketing issue rather than a merely legal or technical function. In digital banking, privacy disclosure therefore plays a dual role. It informs users about how data are collected and processed, and it also signals whether the institution respects users' autonomy, protects sensitive information, and aligns with ethical expectations. This makes data privacy disclosure a potentially important boundary condition in the relationship between AI-enabled interaction and customer trust.

The Stimulus-Organism-Response (S-O-R) framework offers a useful theoretical lens for explaining this mechanism. In this study, AI-enabled interaction and data privacy disclosure are treated as environmental stimuli that shape customers' internal cognitive and affective states. The organismic state is represented by customer trust, which reflects competence, benevolence, and integrity perceptions. A high-quality AI interface may signal competence through speed, relevance, and responsiveness. At the same time, visible privacy disclosure may reduce perceived vulnerability by increasing transparency, control, and security assurance. When these stimuli are aligned, customers are more likely to interpret AI-enabled banking as helpful rather than intrusive.

Social Identity Theory complements the S-O-R framework by explaining why digital banking choices may also carry symbolic meaning among young urban consumers. Millennial and Generation Z users in metropolitan areas often adopt digital platforms not only for functional benefits but also because these platforms reflect lifestyle, technological orientation, and perceived modernity. In such contexts, trust is shaped by both instrumental evaluations and identity-related judgments. Customers may trust a digital bank when it performs efficiently and when its data practices correspond to the ethical standards expected from a modern, reputable financial institution.

Despite growing interest in AI, privacy, and digital banking, three research gaps remain. First, many digital banking studies still conceptualize technological stimuli through conventional usability or service quality attributes, leaving limited empirical evidence on AI-enabled interaction as a distinct stimulus. Second, AI capability and privacy governance are often examined as separate predictors, whereas fewer studies investigate whether privacy disclosure conditions the trust-building effect of AI-enabled interaction. Third, most AI-banking trust studies are conducted in mature markets or generalized digital contexts, while empirical

JMET Vol. 4, No.2 (July 2026)

evidence from Indonesian urban banking customers remains limited. These gaps restrict understanding of how AI and privacy jointly shape trust in emerging-market digital banking ecosystems.

To address these gaps, this study develops and tests a moderated model in which data privacy disclosure strengthens the relationship between AI-enabled interaction and customer trust among SeaBank users in DKI Jakarta. The study contributes to the literature in three ways. First, it extends the S-O-R framework by positioning AI-enabled interaction as a technology stimulus and privacy disclosure as a boundary condition. Second, it integrates Social Identity Theory to explain why trust in digital banking reflects both cognitive risk evaluation and identity-related expectations. Third, it offers managerial implications for digital banks by showing that privacy communication should be designed as an active trust-building mechanism, not merely as a compliance document.

2. Literature Review and Hypothesis Development

2.1 AI-Enabled Interaction in Digital Banking

AI-enabled interaction refers to customer-facing digital service encounters in which intelligent systems assist customers through personalization, responsiveness, conversational support, automated recommendations, risk alerts, or data-driven financial guidance. In banking, such interaction is different from conventional digital service quality because customers do not merely use a static interface; they interact with algorithmic systems that classify needs, anticipate preferences, and sometimes simulate human-like communication. Hentzen et al. (2022) argue that artificial intelligence in customer-facing financial services has become a critical research domain because it changes how customers evaluate service quality, advice, convenience, and institutional competence. Similarly, Puntoni et al. (2021) explain that consumer experiences with AI involve data capture, classification, delegation, and social interaction, meaning that AI creates both functional value and psychological tension.

The literature on AI-based chatbots and digital services shows that customers respond positively when automated systems provide fast, relevant, and understandable assistance. Adam et al. (2021) demonstrate that chatbot design influences user responses in customer service encounters, suggesting that conversational cues, perceived intelligence, and interaction quality can shape compliance and acceptance. In digital banking, AI-enabled interaction may strengthen trust because it reduces service friction, provides real-time support, personalizes financial information, and signals the bank's technological capability. Recent evidence from Indonesia also indicates that perceived trust, perceived risk, awareness, and usefulness are central to customers' continued acceptance of AI in banking services (Ikhsan et al., 2025). Therefore, AI-enabled interaction can be conceptualized as a technological stimulus that shapes customers' cognitive evaluation of the bank.

From the Stimulus-Organism-Response (S-O-R) perspective, AI-enabled interaction functions as an external service stimulus that affects the internal organismic state of the customer. In this study, that organismic state is customer trust. When AI features are perceived as personalized, responsive, accurate, and easy to communicate with, customers are more likely to infer that the bank is competent and reliable. This reasoning is consistent with the view that technology-enabled service encounters influence trust not only through performance outcomes but also through the quality of interaction experienced during the service process. Accordingly, the first hypothesis is proposed as follows:

H1: AI-enabled interaction has a positive effect on customer trust in digital banking.

2.2 Data Privacy Disclosure as a Governance and Risk-Reduction Signal

Data privacy disclosure refers to the extent to which a digital bank clearly communicates how customer data are collected, processed, protected, shared, and controlled. In AI-enabled banking, privacy disclosure becomes especially important because intelligent systems rely on large volumes of behavioral, transactional, and personal data. While these data enable personalization and automation, they may also increase perceived vulnerability when customers are unsure about how their information is used. Martin et al. (2017) show that customer data access can increase feelings of vulnerability and reduce trust, but transparency and control can

JMET Vol. 4, No.2 (July 2026)

reduce negative reactions to data use. Martin and Murphy (2017) further argue that privacy is a strategic marketing and governance issue rather than merely a legal compliance requirement.

In the banking sector, data privacy disclosure also operates as an institutional signal. Customers are more likely to trust a digital bank when privacy communication is visible, comprehensible, and linked to security assurance. Wang et al. (2024) emphasize that data privacy and cybersecurity are central challenges in banking digital transformation because banks must protect sensitive customer information while adopting technologies such as AI, cloud computing, big data analytics, and blockchain. Their findings indicate that banks perceive strong data privacy and cybersecurity as essential for regulatory compliance, competitive advantage, and customer trust. This is particularly relevant for digital banks because customers may not physically meet bank employees and must rely on app-based cues to evaluate the safety and integrity of the institution.

Privacy disclosure is therefore expected to strengthen customer trust through three mechanisms. First, transparency reduces uncertainty by explaining what data are collected and why. Second, control reduces perceived power asymmetry by allowing customers to manage or revoke permissions. Third, security assurance signals that the bank has technical and organizational safeguards to protect sensitive information. In this sense, data privacy disclosure is not a passive legal statement; it is an active trust-building mechanism embedded in customer experience. Accordingly, the second hypothesis is formulated as follows:

H2: Data privacy disclosure has a positive effect on customer trust in digital banking.

2.3 Customer Trust in AI-Mediated Digital Banking

Customer trust is a central construct in digital banking because banking services require customers to accept vulnerability in relation to institutions that manage financial assets and sensitive personal information. Trust is commonly understood as the willingness to rely on another party based on expectations of competence, benevolence, and integrity (Mayer et al., 1995). In AI-mediated banking, these dimensions become more complex. Competence refers to the bank's ability to provide accurate, responsive, and technically reliable AI-supported services. Benevolence reflects the perception that the bank considers customer welfare and does not exploit data asymmetries. Integrity refers to the belief that the bank follows ethical, transparent, and consistent data practices.

The digital banking context amplifies the importance of trust because customers evaluate both the bank and the technological systems that represent it. AI may increase trust when it delivers convenience, speed, personalization, and problem-solving capability. However, AI may also undermine trust when customers perceive algorithmic opacity, excessive automation, intrusive personalization, or insufficient human accountability. Hentzen et al. (2022) note that customer-facing AI in financial services requires further investigation because its benefits depend on how customers interpret risk, advice, personalization, and automation. Thus, trust in AI-enabled banking is not produced by technological sophistication alone; it depends on whether customers perceive the technology as useful, safe, ethical, and aligned with their interests. Social Identity Theory provides an additional explanation for why trust is salient among young urban digital bank users. Millennial and Generation Z customers may evaluate digital banks not only as financial service providers but also as symbols of modernity, efficiency, and digital lifestyle. When a digital bank demonstrates sophisticated AI features and responsible data governance, customers may perceive it as consistent with the identity of a modern and trustworthy financial platform. Conversely, unclear privacy practices may create identity dissonance because users expect technologically advanced banks to also uphold high standards of data ethics and security.

2.4 The Moderating Role of Data Privacy Disclosure

The relationship between AI-enabled interaction and customer trust is unlikely to be uniform across all customers and service conditions. AI interaction may increase trust when users perceive the service as helpful, responsive, and personalized. However, the same AI interaction may also raise privacy concerns because personalization depends on the collection and interpretation of personal data. This creates an AI trust paradox: algorithmic convenience may generate value, but it may also intensify concerns about surveillance, profiling, and loss of control. Puntoni et al. (2021) highlight that consumers experience AI through data capture and

JMET Vol. 4, No.2 (July 2026)

classification processes, which can create discomfort when customers do not understand how data are used. Therefore, privacy disclosure is theoretically relevant as a boundary condition that shapes whether AI interaction is interpreted as helpful or intrusive.

Data privacy disclosure can strengthen the trust-building effect of AI-enabled interaction by transforming algorithmic personalization into a more transparent and controllable experience. When users receive clear explanations about data use, security safeguards, and permission control, they are more likely to interpret AI recommendations as legitimate and customer-oriented. Recent e-banking research also shows that AI-related privacy concerns influence customers' willingness to disclose personal information, especially when fear of AI is present (de Matos et al., 2026). This implies that AI-enabled interaction alone is insufficient; privacy governance must accompany AI innovation to convert technological usefulness into trust.

From the S-O-R perspective, AI-enabled interaction represents a technological stimulus, while data privacy disclosure represents a governance stimulus that conditions the psychological interpretation of the technological stimulus. When privacy disclosure is strong, customers may perceive AI interaction as competent, responsible, and safe, resulting in stronger trust. When privacy disclosure is weak, even high-quality AI interaction may produce suspicion because customers may question how their data are being used. Based on this reasoning, the third hypothesis is proposed as follows:

H3: Data privacy disclosure positively moderates the relationship between AI-enabled interaction and customer trust, such that the relationship is stronger when data privacy disclosure is higher.

3. Research Method

This study employed an explanatory quantitative research design to test the direct and moderating relationships among AI-enabled interaction, data privacy disclosure, and customer trust. The research design was appropriate because the study aimed to evaluate statistically specified relationships among latent constructs and to determine whether data privacy disclosure changes the strength of the relationship between AI-enabled interaction and customer trust.

The population comprised active SeaBank digital banking users residing in DKI Jakarta, Indonesia. The sample consisted of 180 respondents from Millennial and Generation Z cohorts aged 18-35 years. Respondents were selected using purposive sampling because the study required participants who had direct experience with SeaBank's AI-supported banking features. The inclusion criteria were: (1) being an active SeaBank depositor, (2) residing in DKI Jakarta, (3) having used SeaBank for digital banking transactions, and (4) having interacted with AI-supported features such as conversational customer service, robo-advisory functions, dynamic promotions, or automated budget-tracking interfaces at least three times during the previous three months.

The sample size was considered adequate for OLS regression and moderated regression analysis. Following the rule of thumb proposed by Hair et al. (2019), a minimum ratio of five to ten observations per measurement item is acceptable for multivariate analysis. This study used 18 measurement items; therefore, 180 respondents provided a 10:1 ratio, which supports sufficient statistical power and stable parameter estimation.

Data were collected using a structured online questionnaire. All indicators were measured using a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The questionnaire measured three constructs: AI-enabled interaction, data privacy disclosure, and customer trust. AI-enabled interaction was operationalized through personalization, responsiveness, and anthropomorphism. Data privacy disclosure was measured through transparency, control, and security assurance. Customer trust was measured through competence, benevolence, and integrity. The items were adapted from prior studies on AI-enabled banking, AI trust, data privacy, and digital service trust.

Before hypothesis testing, the measurement quality was examined through corrected item-total correlations, Cronbach's alpha, and split-half reliability. Classical assumption tests were then conducted to verify normality, multicollinearity, and heteroskedasticity. The direct effects were tested using OLS multiple

JMET Vol. 4, No.2 (July 2026)

regression, while the moderating effect was examined using Moderated Regression Analysis (MRA). The interaction model was specified as follows: Customer Trust = $\beta_0 + \beta_1(\text{AI-enabled Interaction}) + \beta_2(\text{Data Privacy Disclosure}) + \beta_3(\text{AI-enabled Interaction} \times \text{Data Privacy Disclosure}) + \text{error}$.

Ethical considerations were addressed by informing respondents about the academic purpose of the study, the voluntary nature of participation, and the confidentiality of responses. No personally identifying financial data were collected. Respondents were asked only about their perceptions and experiences with digital banking services.

Table 1. Demographic and Behavioral Profile of Respondents

Category	Sub-category	Frequency	Percentage
Gender	Male	84	46.7%
Gender	Female	96	53.3%
Age	18-25 years (Gen Z)	105	58.3%
Age	26-35 years (Millennials)	75	41.7%
Product used*	High-yield savings account	180	100.0%
Product used*	Digital payments and QRIS	115	63.9%
Product used*	Time deposits	69	38.3%
Product used*	E-commerce lending / PayLater	40	22.2%
Monthly transactions	Low (< 5 transactions)	22	12.2%
Monthly transactions	Moderate (5-15 transactions)	58	32.2%
Monthly transactions	High (> 15 transactions)	100	55.6%
Main AI channel	Conversational chatbot	85	47.2%
Main AI channel	Robo-advisory and wealth engine	60	33.3%
Main AI channel	Dynamic promotion and budget tracking	35	19.5%

*Multiple responses were allowed for product categories.

Table 2. Operationalization of Research Constructs

Construct	Dimension	Measurement focus	Key references
AI-enabled interaction	Personalization	Customized recommendations and anticipation of financial needs based on user activity.	Adam et al. (2021); Bharti et al. (2023); Puntoni et al. (2021)
AI-enabled interaction	Responsiveness	Speed, accuracy, and fluidity of automated support in resolving customer needs.	Adam et al. (2021); Ikhsan et al. (2025)
AI-enabled interaction	Anthropomorphism	Natural, conversational, and empathetic qualities of AI-supported banking interaction.	Adam et al. (2021); Puntoni et al. (2021)
Data privacy disclosure	Transparency	Clarity, visibility, and comprehensibility of data-use explanations.	Martin et al. (2017); Martin & Murphy (2017)
Data privacy disclosure	Control	User ability to manage, modify, or revoke permissions related to personal data use.	Martin et al. (2017); de Matos et al. (2026)
Data privacy disclosure	Security assurance	Visible assurances that sensitive data are protected through robust information-security practices.	SeaBank Indonesia (2023); de Matos et al. (2026)

JMET Vol. 4, No.2 (July 2026)

Customer trust	Competence	Perceived technical capability and institutional reliability of the digital bank.	Bharti et al. (2023); Ikhsan et al. (2025)
Customer trust	Benevolence	Perceived concern for customer welfare and reduction of user vulnerability.	Martin et al. (2017); Martin & Murphy (2017)
Customer trust	Integrity	Perceived honesty, ethical alignment, and credibility of data and service practices.	de Matos et al. (2026); Puntoni et al. (2021)

4. Results and Discussion

4.1 Results

The descriptive analysis indicates that the respondents represented an active digitally native customer group. The dataset was slightly dominated by female respondents (53.3%) and by Generation Z users aged 18-25 years (58.3%). More than half of the respondents reported high monthly transaction intensity, with 55.6% conducting more than 15 digital banking transactions per month. Conversational chatbot interaction was the most frequently reported AI-supported channel (47.2%), followed by robo-advisory and wealth-engine features (33.3%) and dynamic promotion or budget-tracking interfaces (19.5%). This profile confirms that the sample was appropriate for examining AI-enabled interaction and privacy-related trust in digital banking.

Table 3. Descriptive Statistics of Research Variables

Variable	Minimum	Maximum	Mean	Std. deviation	Interpretation
AI-enabled interaction	2.00	5.00	4.12	0.64	High
Data privacy disclosure	1.83	5.00	3.89	0.72	Moderate to high
Customer trust	2.17	5.00	4.05	0.58	High

The descriptive statistics show that AI-enabled interaction received the highest mean score ($M = 4.12$, $SD = 0.64$), indicating that respondents generally perceived SeaBank's AI-supported services as personalized, responsive, and easy to interact with. Customer trust was also high ($M = 4.05$, $SD = 0.58$), suggesting a generally favorable trust climate among the sampled users. Data privacy disclosure produced a slightly lower mean ($M = 3.89$) and the highest standard deviation ($SD = 0.72$), indicating that users' perceptions of privacy communication were more varied than their perceptions of AI service interaction and trust.

Table 4. Measurement Validity and Reliability

Construct	Items	Corrected item-total correlation	Cronbach alpha	Split-half reliability	Status
AI-enabled interaction	AI1-AI6	0.542-0.781	0.845	0.812	Valid and reliable
Data privacy disclosure	PRIV1-PRIV6	0.611-0.804	0.882	0.856	Valid and reliable
Customer trust	TRST1-TRST6	0.519-0.765	0.829	0.798	Valid and reliable

The measurement quality analysis confirms that all constructs met the required validity and reliability criteria. Corrected item-total correlation values exceeded the minimum threshold of 0.30, while Cronbach's

alpha and split-half reliability values were above 0.70. These results indicate that the measurement items were internally consistent and suitable for regression-based hypothesis testing.

Classical assumption testing supported the use of OLS regression. The Kolmogorov-Smirnov test produced an asymptotic significance value of 0.082, indicating that the residuals were normally distributed. The variance inflation factor (VIF) for the main predictors was 1.421, well below the conservative threshold of 5.00, indicating no serious multicollinearity problem. The Glejser test showed non-significant residual patterns ($p > 0.05$), indicating that heteroskedasticity was not detected.

Table 5. OLS and Moderated Regression Results

Predictor	Model 1: Direct OLS	Model 2: Moderated regression
Constant	1.241 (t = 4.150**)	0.892 (t = 2.915**)
AI-enabled interaction	0.425 (t = 6.843**)	0.214 (t = 3.124**)
Data privacy disclosure	0.318 (t = 4.922**)	0.152 (t = 2.212*)
AI-enabled interaction x data privacy disclosure	-	0.285 (t = 4.385**)
R-squared	0.482	0.564
Adjusted R-squared	0.476	0.557
Standard error of estimate	0.420	0.386
F-statistic	82.351**	76.124**
Incremental variance (Delta R-squared)	-	0.082
F-change	-	19.228**

Notes: * $p < 0.05$; ** $p < 0.01$.

Model 1 shows that AI-enabled interaction has a positive and significant effect on customer trust (beta = 0.425, $t = 6.843$, $p < 0.01$). Data privacy disclosure also has a positive and significant direct effect on customer trust (beta = 0.318, $t = 4.922$, $p < 0.01$). Together, these two predictors explain 48.2% of the variance in customer trust. Model 2 adds the interaction term between AI-enabled interaction and data privacy disclosure. The interaction effect is positive and significant (beta = 0.285, $t = 4.385$, $p < 0.01$), and the model explains 56.4% of the variance in customer trust. The increase in explained variance (Delta $R^2 = 0.082$) and the significant F-change value (19.228, $p < 0.01$) confirm that data privacy disclosure strengthens the relationship between AI-enabled interaction and customer trust.

4.2 Discussion

The first finding demonstrates that AI-enabled interaction significantly increases customer trust. This result supports the argument that digital banking customers evaluate AI not only according to its technical presence but also according to how effectively it reduces friction, provides relevant assistance, and creates a sense of institutional competence. In SeaBank's case, AI-supported interfaces such as chatbots, automated recommendations, and budget-tracking tools appear to serve as trust-relevant service cues. This finding is consistent with prior studies showing that AI-enabled banking acceptance is shaped by trust, awareness, security, and perceived usefulness (Bharti et al., 2023; Ikhsan et al., 2025). It also aligns with Adam et al. (2021), who emphasize that chatbot design affects customer responses in digital service encounters.

Theoretically, the result extends the S-O-R framework by confirming that AI-enabled interaction can function as a technological stimulus that shapes the organismic state of trust. When AI interaction is personalized and responsive, customers are more likely to perceive the bank as competent and reliable. From a managerial perspective, this means that digital banks should not treat AI as a back-end efficiency tool only. AI systems should be designed as customer-facing trust interfaces that communicate reliability, contextual understanding, and service empathy.

The second finding confirms that data privacy disclosure directly strengthens customer trust. This indicates that privacy communication is not a peripheral administrative requirement; it is a central part of digital banking value creation. Customers are more likely to trust a digital bank when they can understand how their data are collected, processed, protected, and controlled. This finding is consistent with Martin et al. (2017), who show that transparency and control can reduce the negative effects of data vulnerability on trust. It also supports the argument that privacy should be treated as a strategic marketing and governance issue (Martin & Murphy, 2017).

In practical terms, the finding suggests that digital banks should avoid hiding privacy information in complex legal documents. Privacy disclosure should be visible, concise, and actionable. SeaBank's public communication regarding ISO27001 certification signals a commitment to information security and customer data protection (SeaBank Indonesia, 2023). However, certification alone may not be sufficient if users do not clearly understand what data are collected, why they are collected, and how they can manage their data preferences. Therefore, privacy disclosure must be converted into a user-friendly communication experience within the application interface.

The most important contribution of this study is the significant moderating effect of data privacy disclosure. The finding shows that AI-enabled interaction generates stronger trust when customers perceive privacy disclosure as transparent, controllable, and secure. This result resolves an important trust paradox in AI-enabled banking: the same AI features that create convenience may also create privacy concerns because they rely on extensive user data. When privacy disclosure is strong, customers interpret AI interaction as helpful and responsible. When privacy disclosure is weak, AI interaction can be interpreted as intrusive or surveillance-oriented.

This finding is consistent with recent evidence from electronic banking research showing that AI-related privacy concerns and fear of AI shape customers' willingness to disclose personal information (de Matos et al., 2026). It also resonates with the AI consumer experience literature, which argues that data capture and classification can produce psychological tension if customers do not perceive sufficient transparency and agency (Puntoni et al., 2021). Therefore, the trust-building effect of AI depends on the institutional context in which AI is communicated and governed.

For digital banking executives, the implication is clear: AI innovation and privacy governance must be integrated rather than managed separately. Product teams responsible for AI personalization should work closely with compliance, cybersecurity, and customer-experience teams. A practical solution is to develop a centralized privacy dashboard that allows users to see what data are used by AI features, activate or deactivate specific data permissions, and access plain-language explanations of automated recommendations. Such a mechanism would transform privacy governance from a passive legal obligation into an active trust-building feature.

5. Conclusion

This study examined the effect of AI-enabled interaction on customer trust and tested data privacy disclosure as a moderating variable among SeaBank users in DKI Jakarta. The findings show that AI-enabled interaction has a positive and significant effect on customer trust, indicating that personalization, responsiveness, and conversational quality enhance customers' confidence in digital banking services. Data privacy disclosure also directly increases customer trust, confirming that transparency, control, and security assurance are essential for reducing perceived vulnerability in AI-enabled financial services. Most importantly, data privacy disclosure significantly strengthens the relationship between AI-enabled interaction and customer trust. This demonstrates that AI-enabled service innovation produces stronger trust when supported by visible and understandable privacy communication. Theoretically, the study extends the S-O-R framework by positioning privacy disclosure as a boundary condition that shapes the psychological effect of AI-enabled interaction. It also integrates Social Identity Theory by showing that customer trust in digital banking reflects both cognitive risk evaluation and identity-related expectations of modern, ethical, and secure financial

JMET Vol. 4, No.2 (July 2026)

platforms. Managerially, the findings suggest that digital banks should design AI systems and privacy communication as an integrated trust architecture. Despite these contributions, the study is limited by its cross-sectional design, purposive sampling approach, and focus on young urban users in DKI Jakarta. Future research should test the model across different regions, compare multiple digital banking platforms, examine older customer segments, and use longitudinal or experimental designs to capture changes in trust over time.

Recommendations

Digital banks should strengthen customer trust by integrating AI service innovation with transparent privacy governance. SeaBank and similar institutions should simplify privacy policies into plain-language summaries, provide visual explanations of AI-related data use, and offer a centralized privacy dashboard where users can manage data permissions. Regulators should encourage digital banks to move beyond minimum compliance by promoting privacy disclosure standards that are visible, understandable, and actionable for customers. Future studies should also examine whether digital literacy, AI awareness, or privacy concern further moderate the relationship between AI interaction and customer trust.

Data availability

The datasets generated and analyzed during the current study are not publicly available because they contain respondents' perceptions and banking-related service experiences. However, anonymized data may be made available from the corresponding author upon reasonable request, subject to confidentiality considerations and ethical restrictions.

Declaration of the use of artificial intelligence (AI)

During the preparation of this manuscript, AI-assisted language tools were used only to improve grammar, academic style, readability, and consistency of English expression. The authors reviewed, edited, and approved all AI-assisted outputs and take full responsibility for the accuracy, integrity, originality, interpretation, citations, and conclusions of the manuscript. AI tools were not used to generate empirical data, conduct statistical analysis, or make autonomous research decisions.

Funding

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

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors sincerely thank all respondents in DKI Jakarta who voluntarily participated in this study and shared their experiences with digital banking services. The authors also appreciate the academic support and constructive feedback provided by colleagues during the preparation of this manuscript.

References

- Adam, M., Wessel, M., & Benlian, A. (2021). AI-based chatbots in customer service and their effects on user compliance. *Electronic Markets*, 31(2), 427-445. <https://doi.org/10.1007/s12525-020-00414-7>
- Bharti, S. S., Prasad, K., Sudha, S., & Kumari, V. (2023). Customer acceptability towards AI-enabled digital banking: A PLS-SEM approach. *Journal of Financial Services Marketing*, 28(4), 779-793. <https://doi.org/10.1057/s41264-023-00241-9>

- de Matos, C. A., Rohden, S. F., & Lourenco Azevedo, A. B. (2026). AI-induced privacy concerns: Examining the moderating effect of AI fear on customer data sharing. *International Journal of Bank Marketing*, 44(6), 1271-1294. <https://doi.org/10.1108/IJBM-05-2025-0403>
- Geebren, A., & Jabbar, A. (2021). Factors that influence customer trust and satisfaction in mobile banking. *International Journal of E-Business Research*, 17(3), 1-20. <https://doi.org/10.4018/IJEER.2021070105>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate Data Analysis* (8th ed.). Cengage Learning.
- Hentzen, J. K., Hoffmann, A. O. I., Dolan, R., & Pala, E. (2022). Artificial intelligence in customer-facing financial services: A systematic literature review and agenda for future research. *International Journal of Bank Marketing*, 40(6), 1299-1336. <https://doi.org/10.1108/IJBM-09-2021-0417>
- Ikhsan, R. B., Fernando, Y., Prabowo, H., Yuniarty, Gui, A., & Kuncoro, E. A. (2025). An empirical study on the use of artificial intelligence in the banking sector of Indonesia by extending the TAM model and the moderating effect of perceived trust. *Digital Business*, 5(1), Article 100103. <https://doi.org/10.1016/j.digbus.2024.100103>
- Lappeman, J., Marlie, S., Johnson, T., & Poggenpoel, S. (2023). Trust and digital privacy: Willingness to disclose personal information to banking chatbot services. *Journal of Financial Services Marketing*, 28(2), 337-357. <https://doi.org/10.1057/s41264-022-00154-z>
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58. <https://doi.org/10.1509/jm.15.0497>
- Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, 45(2), 135-155. <https://doi.org/10.1007/s11747-016-0495-4>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709-734. <https://doi.org/10.5465/amr.1995.9508080335>
- Mehrabian, A., & Russell, J. A. (1974). *An approach to environmental psychology*. MIT Press.
- Populix. (2024). Analysis of the ecosystem and perception of digital banks in Indonesia. Populix Research Insight. <https://info.populix.co/data-hub/reports/digitalbanking2024>
- Populix. (2025). Layanan keuangan digital kian populer di 2025, apa alasannya? Populix. <https://info.populix.co/articles/layanan-keuangan-digital/>
- Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2021). Consumers and artificial intelligence: An experiential perspective. *Journal of Marketing*, 85(1), 131-151. <https://doi.org/10.1177/0022242920953847>
- SeaBank Indonesia. (2023). SeaBank Indonesia berhasil raih ISO27001, bentuk komitmen perlindungan keamanan data nasabah. <https://www.seabank.co.id/blog/seabank-indonesia-berhasil-raih-iso27001-bentuk-komitmen-perindungan-keamanan-data-nasabah>
- Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. In W. G. Austin & S. Worchel (Eds.), *The social psychology of intergroup relations* (pp. 33-47). Brooks/Cole.
- Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & Security*, 147, Article 104051. <https://doi.org/10.1016/j.cose.2024.104051>