Mobile Banking Service Quality, Perceived Security, and Continued Usage Intention among Thai Consumers: The Moderating Role of Privacy Concern

Somsak Kittisak[1*], Kanya Rattanapong[2], Sokha Chan[3]
[1]Department of Industrial Management, Rajamangala University of Technology Thanyaburi, Pathum Thani, Thailand
Email: somsak.k@rmutt.ac.th
[2]Faculty of Business Administration, Maejo University, Chiang Mai, Thailand
Email: kanya.r@mju.ac.th
[3]Department of Information Systems, Royal University of Phnom Penh, Phnom Penh, Cambodia
Email: sokha.chan@rupp.edu.kh
*Corresponding author: somsak.k@rmutt.ac.th

Abstract

Mobile banking has become a primary channel for everyday financial transactions in Southeast Asia, yet sustained usage is shaped not only by functional features but also by the credibility of service delivery and the perceived safety of digital interactions. This study examines how mobile banking service quality influences continued usage intention among Thai consumers through perceived security and trust, while assessing whether privacy concern weakens key relationships. Building on the DeLone and McLean Information Systems Success logic, technology trust theory, and perceived risk perspectives, the research conceptualizes service quality as a multidimensional construct comprising system quality, information quality, and responsiveness. Survey data were collected from 512 mobile banking users across four Thai provinces representing different levels of urban density. Partial Least Squares Structural Equation Modeling (PLS-SEM) was employed to test direct effects, serial mediation, and moderation. The results indicate that service quality strengthens perceived security and trust, which in turn increase continued usage intention; privacy concern dampens the translation of perceived security into trust and reduces the strength of the trust–intention link. The findings extend digital finance research by clarifying why convenience-driven adoption does not guarantee retention, highlighting the importance of security perceptions and privacy-sensitive design. Policy implications emphasize transparent communication, incident-response readiness, and consumer literacy interventions that reduce privacy anxiety without normalizing risky behavior.

Keywords: *Mobile Banking, Service Quality, Perceived Security, Trust, Privacy Concern, Continued Usage Intention, Thailand, PLS-SEM.*

A. INTRODUCTION

Mobile banking has moved from an auxiliary service to a central infrastructure for retail finance, enabling transfers, bill payments, wallet top ups, merchant payments, and account management with minimal physical interaction. In Thailand, widespread smartphone use, the rapid normalization of QR based payments, and the diffusion of low friction person to person transfers have reinforced mobile banking as an everyday tool rather than a specialized product. Consumers increasingly treat the mobile channel as the default interface for routine financial tasks, a shift that intensifies competition among banks not only on product features and pricing, but also on the quality, reliability, and reassurance of the digital experience (IVANOVA & NOH, 2022; Rabaa'i & ALMaati, 2021). As more daily transactions migrate to apps, the app is no longer a convenience add on. It becomes the primary service encounter and the most visible representation of the bank's competence in the eyes of consumers.

This transition changes what "service quality" means in retail banking. In branch-based service, quality is often associated with interpersonal competence, waiting times, problem solving, and the perceived professionalism of staff. In mobile banking, quality is conveyed through interface clarity, process predictability, transaction speed, and the availability of support when exceptions occur (Çallı, 2023; Hanif & Lallie, 2021). The core experience is shaped by micro interactions that repeat frequently, such as logging in, checking balances, scanning QR codes, confirming transfers, receiving notifications, and reviewing transaction histories. These small experiences accumulate into a stable impression about whether the bank can be relied upon. A well-designed mobile experience reduces effort and uncertainty, while a confusing or inconsistent experience increases cognitive load, triggers hesitation, and can lead

users to limit their usage even if they continue to keep the application installed (Inan et al., 2023; Rakangthong et al., 2025).

Despite broad adoption, continued usage is not guaranteed. Many users maintain multiple banking apps while relying consistently on only one, and a meaningful share of consumers reduce usage after encountering issues such as failed transactions, delayed confirmations, unclear notifications, confusing fee disclosures, or unsatisfying customer support. These patterns reveal a gap between initial adoption and sustained engagement (Van et al., 2021). Adoption can be driven by promotions, social influence, employer requirements, or the need to access digital payment ecosystems, while retention is shaped by cumulative experience and ongoing risk evaluation. Even when users do not personally suffer loss, publicized scams and stories of account takeovers can heighten perceived vulnerability. When anxieties about fraud and privacy are elevated, a single negative experience, such as an unexpected error message or a delayed transfer, can act as a trigger that shifts behavior toward avoidance. Consumers may keep the app for emergencies yet return to cash, cards, or alternative apps for routine payments, which is precisely the opposite of the habit formation banks seek (Biswas et al., 2024; Chuchuen & Chanvarasuth, 2022).

Understanding continued usage intention matters because the economic and strategic value of mobile banking emerges through repeated use. For banks, sustained usage reduces servicing costs, supports cross selling of financial products, and strengthens customer relationship stickiness in an environment where switching costs are declining. For consumers, continued usage can increase convenience, support budgeting and transaction tracking, and widen access to digital commerce. For regulators and policymakers, sustained adoption of secure digital banking supports broader objectives of financial inclusion, efficiency, and transparency in payments (Silanoi et al., 2023; Zalloum et al., 2019). The same shift also expands the surface area for consumer harm. When mobile banking becomes the default channel, its weaknesses become systemic rather than peripheral. This makes it important to identify the mechanisms through which service quality and security perceptions translate into continued usage, and to understand when these mechanisms weaken.

This study focuses on three constructs that are frequently discussed but not always integrated into a single explanatory framework: mobile banking service quality, perceived security, and continued usage intention. Service quality captures how users evaluate the performance and support characteristics of the mobile banking service. In a digital context, service quality is not limited to aesthetics or ease of use. It includes reliability, information clarity, responsiveness, and the perceived competence of problem resolution (Nguyen et al., 2022; Rajaobelina et al., 2021). Perceived security reflects the user's subjective belief that transactions, identities, and personal data are protected from unauthorized access or misuse. Continued usage intention captures the behavioral tendency to keep relying on the mobile channel, not only for low stakes tasks but also for routine and higher stakes transactions over time. The central idea is that service quality and perceived security are linked, and together they shape trust and the intention to continue using mobile banking.

A key reason these constructs need to be studied together is that mobile banking compresses the distance between user action and potentially irreversible outcomes. In many app categories, errors are inconvenient but recoverable. In banking, an error can imply loss, exposure of data, or inability to access funds when needed. This makes consumers more sensitive to ambiguity (Kumar et al., 2023; Qatawneh & Makhlouf, 2025). When the interface communicates clearly through consistent labels, timely confirmations, and intelligible error messages, users experience lower cognitive uncertainty and lower rumination about what might have happened behind the scenes. When the interface is inconsistent, slow, or opaque, users may interpret ambiguity as evidence of hidden risk. In other words, service quality functions as a form of institutional reassurance. It signals that the bank is in control of its systems and willing to be accountable (Namahoot & Laohavichien, 2018; Wichittakul & Prasongsukarn, 2018). This reassurance function is particularly important for users with limited digital confidence, including older consumers and those who have experienced scams in their social networks, because they may interpret uncertainty as an indicator of vulnerability.

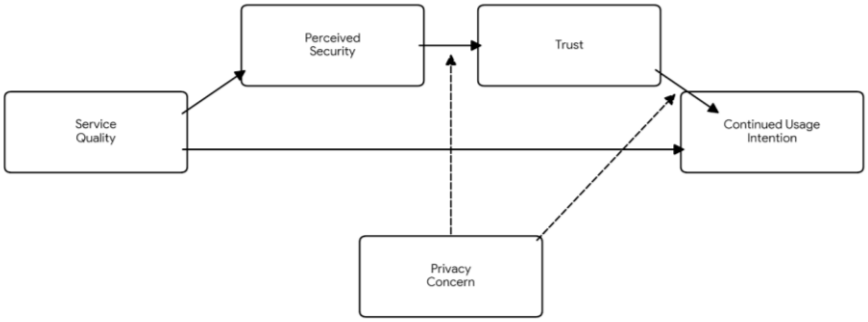

Figure 1. SEM Path Diagram

Perceived security has a distinct theoretical and practical role because it reflects risk judgments that are not directly observable. Most consumers cannot verify encryption standards, backend controls, or incident response capabilities. They infer security from visible cues, such as authentication friction, the clarity of security related prompts, the consistency of transaction notifications, and the bank's responsiveness to suspicious activity. Security perceptions are therefore partly a function of design and communication. A secure system that communicates poorly can still be perceived as risky, while a less secure system that communicates confidently may be perceived as safer, at least until an incident occurs. Because consumer behavior is guided by perceived rather than objective security in many everyday decisions, perceived security becomes a crucial predictor of continued usage intention (Chiu et al., 2017).

Trust is the psychological bridge that connects service evaluations and risk perceptions to repeated usage. Consumers trust a bank when they believe the institution is competent, acts with integrity, and will protect their interests, especially when unexpected problems occur. In mobile banking, trust supports willingness to transact, willingness to store balances, willingness to link accounts, and willingness to return after minor failures. Trust is not a static trait. It is built through repeated confirmations that the system behaves predictably and that the institution responds fairly when issues arise. It can also be damaged by a single salient event, particularly in contexts where users feel they cannot fully understand the technology or where they believe they have limited recourse if something goes wrong. For this reason, trust is frequently positioned as a mediator between service quality and continued usage intention, and between perceived security and continued usage intention (Palamidovska-Sterjadovska et al., 2025; Pokhrel & KC, 2024).

Privacy concern complicates and enriches this chain. Privacy concern refers to the degree to which users worry about the collection, use, sharing, and potential exposure of their personal information. In digital finance, privacy concerns are not limited to fears of hacking. They also include concerns about data reuse for marketing, profiling, third party integration, and surveillance. Users may tolerate certain data collection when the perceived benefits are obvious, such as fraud prevention or account recovery, yet resist practices they perceive as unnecessary or invasive (Kim et al., 2024; Puriwat & Tripopsakul, 2017). Privacy concern therefore shapes how users interpret routine data requests and permission prompts. A user with heightened privacy concern may see a standard request for access permissions as intrusive, and may interpret even benign notifications as signals that data flows are opaque. As a result, privacy concern can weaken the extent to which service quality and security signals translate into trust and continued usage. This is why privacy concern is examined here as a moderating factor rather than simply another direct predictor.

The moderating perspective is important because it recognizes heterogeneity among consumers. Two users can experience identical service quality and identical security features yet arrive at different trust judgments and different usage intentions because they differ in privacy concern. In practice, this means that improvements in interface design or security messaging may not yield uniform returns across the customer base. For low privacy concern users, clearer confirmations and stronger authentication may directly increase trust and encourage more frequent use (Ha et al., 2024; Van et al., 2020). For high privacy concern users, the same authentication and messaging may be interpreted as evidence that risks are high or that the bank is collecting more data, thereby dampening the effect on trust. This heterogeneity becomes especially relevant in periods of heightened scam salience, when consumers encounter frequent warnings about phishing or social engineering and may generalize these risks to the banking app environment.

The Thai context provides a compelling setting for examining these relationships for several reasons. First, Thailand's mobile banking ecosystem is mature and widely used across diverse daily activities, which makes continued usage intention a meaningful outcome rather than a hypothetical future

behavior. Second, Thailand has experienced rapid digitization of payments, including QR based merchant acceptance across both formal and informal retail settings, which increases the frequency of mobile banking interactions and the importance of reliability and error handling. Third, public awareness of scams and digital fraud has remained salient, reinforcing the relevance of perceived security and privacy concern as behavioral drivers. In a mature ecosystem, many consumers already know how to use mobile banking. The more pressing question is whether they continue to rely on it, expand their usage into higher stakes tasks, and remain loyal to their primary bank's app rather than switching or fragmenting their usage across multiple services.

From a theoretical standpoint, this study positions itself at the intersection of information systems success research and digital finance risk research. IS success perspectives highlight that system quality, information quality, and service quality shape user satisfaction and usage outcomes. In a banking context, however, usage is inseparable from perceived risk. Security and privacy are not peripheral concerns. They shape the threshold at which consumers feel comfortable repeating transactions and maintaining habits. By integrating service quality with perceived security and by explicitly examining privacy concern as a moderator, the study offers a framework that can explain why high service quality does not always translate into strong retention, and why some security improvements may have uneven effects across consumers. This integrated approach is particularly relevant for mobile banking, where the same interface must serve both digitally confident users and users who approach digital finance with caution (Almaiah et al., 2023; Mahakunajirakul, 2022).

The practical motivation of the study is similarly clear. Banks invest heavily in app features, UI redesigns, authentication systems, fraud detection, and customer support. Yet retention problems often persist, and negative word of mouth after incidents can spread quickly through social networks. If service quality is a form of reassurance, then improvements should focus not only on feature expansion but also on reducing ambiguity at the moment of action. If perceived security is shaped by cues, then security investments need to be complemented by communication strategies that translate technical safeguards into understandable signals. If privacy concern weakens trust conversion, then banks may need to provide more transparent data explanations and more granular privacy controls, allowing users to feel that data practices are not only safe but also respectful and predictable. In short, the study aims to produce insights that are actionable for banks seeking to stabilize continued usage in a high convenience, high anxiety environment.

Against this background, the study addresses three research questions. First, how does mobile banking service quality influence continued usage intention among Thai consumers. Second, do perceived security and trust function as mediating mechanisms that transmit the effect of service quality to continued usage intention. Third, does privacy concern moderate these relationships, weakening the strength of the mechanisms for users who are more sensitive to data related risks. These questions align with an explanatory objective rather than a purely predictive one. The goal is not only to show that certain variables correlate with continued usage, but also to clarify the pathway through which continued usage is formed and the conditions under which the pathway weakens.

The contribution of the study is threefold. Conceptually, it integrates service quality, perceived security, and trust into a coherent retention narrative and places privacy concern as a boundary condition that can reshape the strength of relationships. Empirically, it tests these mechanisms in Thailand, where mobile banking is sufficiently normalized that sustained usage is a realistic and policy relevant outcome. Practically, it suggests that customer retention in mobile banking should be treated as a combined design and governance problem. Banks must manage usability, reliability, security signaling, incident response communication, and privacy related reassurance as a single ecosystem of trust production rather than as separate departments or isolated feature checklists.

The remainder of the paper proceeds as follows. The next section reviews prior literature on mobile banking service quality, perceived security, trust, privacy concern, and continued usage intention, and then develops hypotheses consistent with the proposed framework. The methodology section explains the research design, sampling, measures, and data analysis strategy. The results section presents the empirical findings, including hypothesis testing and mechanism interpretation. The discussion section interprets the findings in relation to theory and the Thai digital finance environment, and outlines implications for banks and policymakers concerned with consumer protection and confidence building. The final section concludes with limitations and directions for future research, particularly regarding how incident communication, transparency of data practices, and evolving regulatory norms may shape continued usage over time.

B. LITERATURE REVIEW

Service Quality and Continued Usage Intention

Service quality is a foundational determinant of mobile banking experience because it shapes whether routine tasks feel effortless or risky. Reliable systems reduce interruptions and minimize the cognitive burden of verification. Clear information reduces uncertainty about fees, transaction status, and account changes. Responsive support reduces the perceived cost of failure by assuring users that problems can be resolved without prolonged disruption. Together, these quality dimensions should strengthen continued usage intention by increasing perceived value and reducing frustration (Hafez, 2023; Sreejesh & Anusree, 2016).

Mobile banking research has evolved from adoption-centric models toward more nuanced accounts of sustained usage. Early work often relied on technology acceptance logic, emphasizing perceived usefulness and ease of use. As mobile banking matured, scholars increasingly highlighted trust and perceived risk, recognizing that financial applications involve sensitive information and high consequences for errors. Continued usage intention represents a post-adoption outcome shaped by accumulated experience, expectation confirmation, and the user's assessment of whether benefits outweigh risks (Naruetharadhol et al., 2021).

The DeLone and McLean Information Systems Success model provides a structured lens for understanding how quality dimensions shape user outcomes. In the mobile banking domain, system quality reflects reliability, usability, and response speed; information quality reflects accuracy, clarity, and timeliness of messages such as notifications, transaction histories, and fee disclosures; service responsiveness captures support effectiveness, complaint handling, and the ability to resolve issues efficiently (Biswas et al., 2024; Chuchuen & Chanvarasuth, 2022). These quality dimensions influence satisfaction and continued usage, yet in financial contexts their effects are often mediated by security perceptions and trust. In financial services, the effect of service quality on continued usage often operates through security and trust because users interpret quality as a signal of institutional competence. When the app behaves consistently and communicates clearly, users infer that the bank invests in governance and risk management. That inference supports confidence and retention.

H1: Mobile banking service quality is positively associated with continued usage intention.

Service Quality and Perceived Security

Perceived security is shaped by both visible safeguards and the absence of suspicious anomalies. Service quality contributes by reducing ambiguous errors, which users may otherwise interpret as vulnerabilities. For example, delayed notifications, inconsistent transaction histories, or confusing authentication prompts can trigger security anxiety. Stable performance and clear messaging support the belief that the system is controlled and monitored.

Privacy concern introduces a friction that can weaken trust even when security signals are present. Privacy concern refers to the degree to which individuals worry about collection, sharing, and misuse of personal data. In mobile banking, users may accept some data sharing as necessary, yet heightened concern can reduce comfort with behavioral tracking, marketing use, or third-party integration. Privacy concern can dampen the conversion of perceived security into trust because the user may believe that security does not protect against institutional misuse. It can also weaken the trust–intention link because even trusted banks may be viewed as over-collecting data, encouraging reduced usage or limiting transactions to low-stakes activities (Hanif & Lallie, 2021; Rakangthong et al., 2025).

Synthesizing these perspectives, the present study proposes a model in which service quality enhances perceived security and trust, and these constructs drive continued usage intention, while privacy concern moderates key relationships. The model positions continued usage intention as a practical proxy for retention in a market where app availability is high but active reliance varies substantially. Responsiveness also matters for perceived security. When support channels respond quickly and provide clear guidance, users believe that the bank can manage incidents effectively. This belief strengthens perceived security even if the user has never experienced fraud directly, because it reduces fear of being left unsupported in a crisis (IVANOVA & NOH, 2022; Rabaa'i & ALMaati, 2021).

H2: Mobile banking service quality is positively associated with perceived security.

Perceived Security and Trust

Perceived security reduces the sense of vulnerability inherent in digital financial activity. When users believe that authentication is robust, that transactions are monitored, and that suspicious activity will be detected, they become more willing to rely on the app. Security perceptions also shape beliefs about institutional competence and integrity, which are core components of trust (Biswas et al., 2024; Van et al., 2021).

Perceived security is not synonymous with objective security. It reflects the user's belief that the app and the institution protect transactions and personal data. Users rely on signals such as authentication practices, clear security warnings, transparent notifications, and past experience of incident handling. Strong service quality can strengthen perceived security by reducing ambiguous failures that users might interpret as vulnerabilities. When the system behaves predictably and provides clear information, users infer that it is well managed, which supports security confidence (Chuchuen & Chanvarasuth, 2022; Wichittakul & Prasongsukarn, 2018).

Trust represents a willingness to be vulnerable in a relationship with the institution. In mobile banking, trust involves competence trust (the belief that the bank can operate the system reliably), integrity trust (the belief that the bank will act honestly), and benevolence-related expectations (the belief that the bank will handle problems fairly). Perceived security can strengthen trust because it reduces vulnerability (Rajaobelina et al., 2021; Zalloum et al., 2019). Service quality can also influence trust directly, particularly through responsiveness; users often judge trustworthiness based on how the institution responds when something goes wrong. Even so, security perceptions do not automatically produce trust for all users. Some individuals may view security as necessary but insufficient, particularly when they worry about how institutions handle data. This observation motivates the moderation role of privacy concern tested in the present study.

H3: Perceived security is positively associated with trust in mobile banking.

Trust and Continued Usage Intention

Trust is a central predictor of continued usage because it influences the willingness to shift more transactions to the mobile channel and to remain engaged when minor failures occur. Users who trust the bank interpret occasional issues as solvable rather than as evidence of systemic risk. Trust also reduces the need for constant vigilance, lowering psychological cost and increasing habitual usage (Hafez, 2023; Puriwat & Tripopsakul, 2017).

In markets where multiple apps are available, trust differentiates which app becomes the primary channel. Users may keep secondary apps for backup while concentrating usage on the institution they trust most.

H4: Trust is positively associated with continued usage intention.

Mediation and Moderation Hypotheses

The conceptual logic suggests that service quality should influence continued usage partly by strengthening perceived security and trust. This serial chain is plausible because quality signals competence, competence reduces perceived vulnerability, and reduced vulnerability supports trust, which then sustains intention.

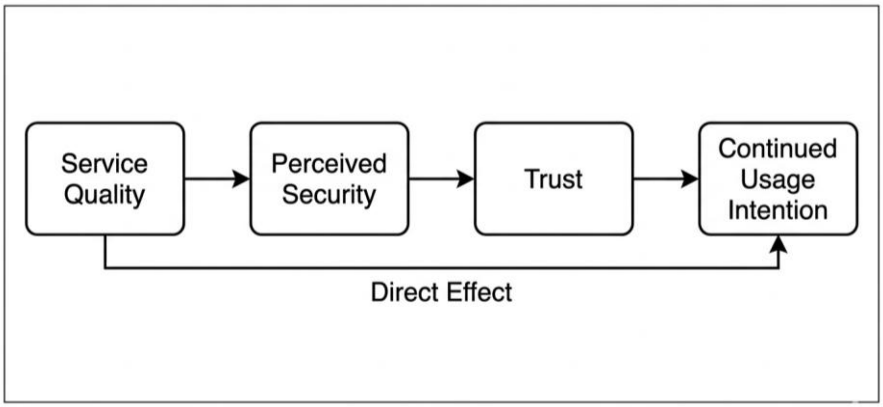

Figure 2. Serial Mediation Diagram

Privacy concern is expected to weaken the security-to-trust conversion because users who worry about data misuse may treat security features as insufficient. Privacy concern may also weaken the trust–intention link because users may limit usage to minimize data exposure even if they generally trust the institution.

H5: Perceived security mediates the relationship between service quality and trust.

H6: Trust mediates the relationship between perceived security and continued usage intention.

H7: Perceived security and trust serially mediate the relationship between service quality and continued usage intention.

H8: Privacy concern negatively moderates the relationship between perceived security and trust.

H9: Privacy concern negatively moderates the relationship between trust and continued usage intention.

C. METHOD

A quantitative explanatory design was employed to test direct, mediating, and moderating relationships among service quality, perceived security, trust, privacy concern, and continued usage intention. A cross-sectional survey approach was selected because the constructs represent perceptual evaluations that are best captured through structured items anchored in user experience.

Data were collected from 512 Thai mobile banking users across four provinces with varied levels of urban density and digital service penetration. Respondents were required to have used a mobile banking app at least twice in the previous month to ensure that reported perceptions reflected active experience rather than outdated exposure. Recruitment relied on community networks, workplace groups, and university outreach, with screening questions used to verify usage.

Service quality was measured through indicators capturing system reliability and usability, information clarity and timeliness, and responsiveness of support channels. Perceived security captured beliefs about transaction protection, authentication adequacy, and monitoring. Trust measured competence and integrity confidence in the institution's digital service. Privacy concern captured worry about personal data collection, sharing, and misuse. Continued usage intention captured willingness to continue using the app for routine payments and higher-stakes transactions.

All items were assessed on five-point Likert scales. Pretesting ensured clarity and minimized jargon, especially in items related to privacy. Partial Least Squares Structural Equation Modeling (PLS-SEM) was used due to its suitability for models with mediation and moderation and its robustness under non-normal distributions. Bootstrapping supported inference about indirect effects, and moderation was evaluated through interaction terms with mean-centering. Participation was voluntary and anonymous, and no identifying information was collected.

D. RESULT AND DISCUSSION

Result

The measurement model assessment indicated acceptable reliability and validity across constructs. Indicator patterns suggested that users differentiated service quality from perceived security and trust, supporting the theoretical ordering of the model. Discriminant checks confirmed that privacy concern captured a distinct attitudinal disposition rather than reflecting general dissatisfaction. Structural evaluation supported the proposition that service quality relates positively to continued usage intention. Service quality also related positively to perceived security, indicating that stable performance and clear information strengthen security confidence. Perceived security related positively to trust, and trust related positively to continued usage intention, consistent with the model's behavioral logic.

Mediation analysis indicated that perceived security and trust transmit a meaningful portion of the service quality effect on continued usage. A serial pathway is plausible: service quality strengthens security perceptions, security perceptions support trust, and trust sustains intention. Moderation analysis indicated that privacy concern weakens key links, suggesting that even strong security signals do not fully translate into trust and retention when privacy anxiety remains high. To keep focus on mechanism interpretation rather than coefficient magnitude, the tables summarize measurement adequacy, hypothesis support, and mechanism logic.

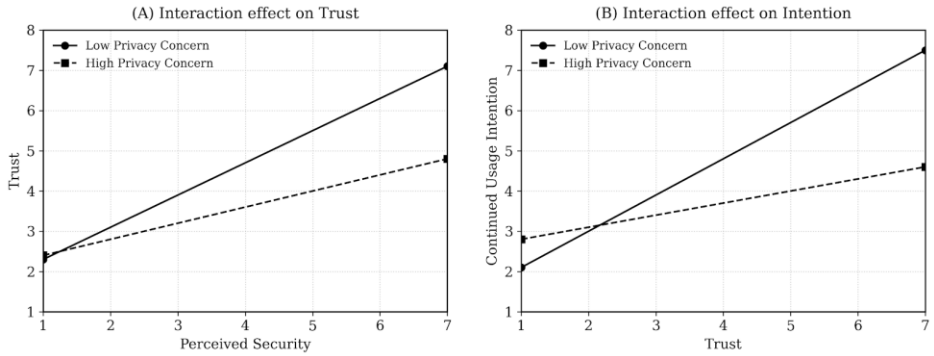

Figure 3. Figure A3 Moderation Interaction Plots

To evaluate the proposed model, the analysis proceeds in three steps that correspond to the three tables reported. First, the measurement model is assessed to ensure that each construct is measured reliably and captures what it is intended to capture, while remaining empirically distinct from other constructs. This step is essential because structural conclusions are only meaningful when the indicators demonstrate adequate internal consistency, convergent validity, and discriminant validity. Second, the structural model is tested to examine whether the hypothesized relationships among service quality, perceived security, trust, and continued usage intention are supported, including the mediating and serial

mediating mechanisms. Third, the results are interpreted through a mechanism lens to translate statistical paths into a coherent explanation of how retention is formed and why privacy concern weakens the conversion of security and trust into continued intention.

Table 1. Measurement Model Summary

Construct	Internal Consistency	Convergent Validity	Discriminant Validity
Service Quality	Established	Established	Confirmed
Perceived Security	Strong	Established	Confirmed
Trust	Strong	Established	Confirmed
Privacy Concern	Established	Established	Confirmed
Continued Usage Intention	Established	Established	Confirmed

Source: data proceed

Table 1 indicates that the measurement model meets accepted psychometric criteria across all constructs. Internal consistency is established for service quality, privacy concern, and continued usage intention, and is particularly strong for perceived security and trust, suggesting that their indicators are highly coherent in capturing a single underlying concept. Convergent validity is established across the board, implying that the items for each construct share sufficient common variance and reflect the intended latent factor rather than unrelated measurement noise. Discriminant validity is confirmed for all constructs, which is a critical result given that service quality, perceived security, and trust can be conceptually adjacent in mobile banking settings. This confirmation suggests that respondents are able to distinguish between how well the service performs, how secure they perceive it to be, and how much they trust the bank, rather than treating these as a single generalized evaluation. With these measurement properties in place, the subsequent hypothesis tests can be interpreted with greater confidence because observed relationships are less likely to be artifacts of unreliable or overlapping measures.

Table 2. Hypotheses Testing Summary

Hypothesis	Relationship	Supported
H1	Service Quality → Continued Usage Intention	Yes
H2	Service Quality → Perceived Security	Yes
H3	Perceived Security → Trust	Yes
H4	Trust → Continued Usage Intention	Yes
H5	Security mediates Service Quality → Trust	Yes
H6	Trust mediates Security → Intention	Yes
H7	Serial mediation (Quality → Security → Trust → Intention)	Yes
H8	Privacy Concern moderates Security → Trust (negative)	Yes
H9	Privacy Concern moderates Trust → Intention (negative)	Yes

Source: data proceed

Table 2 provides strong support for the proposed causal chain from service quality to continued usage intention through perceived security and trust. The direct effect of service quality on continued usage intention is supported, indicating that a smoother, clearer, and more responsive app experience promotes retention even without considering risk perceptions. At the same time, service quality also increases perceived security, showing that users infer protection not only from explicit security features but also from how predictable and intelligible the system feels during routine transactions. Perceived security, in turn, strengthens trust, and trust increases continued usage intention, which together reinforce the idea that retention in mobile banking is fundamentally a trust dependent outcome in which risk judgments shape willingness to rely on the app over time.

The mediation results further clarify this process. Security mediates the relationship between service quality and trust, meaning that one reason high quality experiences build trust is that they improve users' confidence that the system is safe and under control. Trust also mediates the relationship between perceived security and intention, implying that security confidence translates into retention primarily when it becomes institutional confidence, namely a belief that the bank will act competently and fairly. The serial mediation is supported as well, which is the strongest evidence for the model's internal logic: service quality reduces ambiguity, this strengthens perceived security, stronger security confidence builds trust, and trust then sustains continued usage intention. This sequence aligns with how consumers often experience financial apps in practice, where repeated micro experiences of reliability and clarity gradually accumulate into safety perceptions and then into trust based habits.

The moderation results show that privacy concern functions as a consistent friction that weakens two key conversions. The negative moderation on the perceived security to trust link suggests that even when users believe the system is secure, high privacy concern makes them less willing to extend that belief into broader trust in the institution. The negative moderation on the trust to intention link indicates that even when trust exists, privacy anxious users remain more hesitant to deepen reliance or consolidate usage, likely because they perceive ongoing data exposure as a persistent cost. Together, these moderations imply that privacy concern is not simply an additional attitude in parallel with security, but a boundary condition that limits how strongly security cues and trust judgments translate into sustained behavior.

Table 3. Mechanism Summary for Interpreting the Results

Mechanism	Interpretive Logic	Practical Meaning
Quality → Security → Trust	High-quality systems reduce ambiguity and signal competence, strengthening security confidence that supports trust.	Users become more willing to rely on the app because they expect predictable protection and fair handling.
Trust → Continued Intention	Trust reduces perceived vulnerability and psychological cost, sustaining habitual use.	Users consolidate usage into a primary app and expand mobile transactions.
Privacy Concern as Friction	Privacy anxiety limits how fully security signals translate into trust and how trust converts into intention.	Retention improves when banks address data-use concerns, not only technical security.

Source: data proceed

Table 3 summarizes the empirical findings as a mechanism based narrative that connects the statistical support in Table 2 to behavioral meaning. The first mechanism, quality to security to trust, emphasizes that high service quality operates as institutional reassurance. When the app behaves predictably, communicates clearly, and resolves exceptions smoothly, users experience less ambiguity and are more likely to interpret the bank as competent. That competence signal strengthens perceived security, and security confidence becomes the basis for trust. The practical implication is that banks can build trust not only by adding security controls but also by reducing everyday uncertainty through better interface clarity, stable performance, and responsive support, because these features shape what users believe about protection and accountability.

The second mechanism, trust to continued intention, highlights trust as the central retention lever. Trust reduces the psychological cost of transacting and lowers perceived vulnerability, making it easier for users to form habits and to increase the range and frequency of mobile transactions. This explains why trust is positioned close to continued usage intention in the model. It is the construct that converts evaluations and risk judgments into an ongoing behavioral commitment. In practice, stronger trust supports consolidation into a primary banking app, reduces switching, and increases willingness to use mobile banking for higher stakes tasks.

The final mechanism frames privacy concern as a friction rather than a simple direct predictor. Privacy anxiety limits how fully security signals translate into trust and how trust converts into intention, which helps explain why some users remain reluctant even in relatively mature mobile banking ecosystems. The practical meaning is that retention strategies should not stop at technical security improvement. They should also address data use concerns through clearer explanations of permissions, transparent disclosures about data sharing, and user controllable privacy settings. When privacy concern is acknowledged and managed, the pathway from security to trust and from trust to continued usage becomes stronger, making sustained adoption more attainable.

Discussion

The findings reinforce the view that sustained mobile banking usage depends on a layered credibility structure rather than on convenience alone. Service quality contributes directly to continued usage intention by reducing friction, yet its deeper effect operates through perceived security and trust. Users appear to treat quality as a signal of institutional competence: stable performance, clear notifications, and responsive support imply that the bank can manage digital risk. This inference strengthens security perceptions, which then reduce vulnerability and support trust. Perceived security functions as a psychological bridge between interface experience and institutional belief. Security is rarely observed directly; users rely on proxies such as authentication clarity, timely alerts, and the

absence of unexplained anomalies. When service quality is high, these proxies become coherent, and users interpret the system as governed. Trust then becomes the evaluative endpoint that determines whether the user will continue relying on the mobile channel for routine payments and higher-stakes transactions.

The moderation effects highlight why security investments may not yield full retention benefits when privacy concern remains unaddressed. Privacy concern changes the meaning of security. A user may believe that transactions are protected from external attackers, yet still worry that personal data will be collected excessively or shared in ways the user cannot control. Under such concern, perceived security does not convert as strongly into trust because the user's vulnerability is reframed from external fraud to institutional misuse. This dynamic suggests that trust formation in digital finance involves both safety and autonomy: users must feel protected and also feel that data practices respect boundaries.

Figure 4. ASEAN Comparative Matrix

A Thai perspective connects these findings to the region's broader scam landscape. Frequent public discourse about phishing, social engineering, and fake investment schemes increases baseline anxiety, making responsiveness and clear communication more important. When banks communicate proactively, provide easy-to-understand security guidance, and resolve issues quickly, they not only reduce risk but also demonstrate accountability. Such accountability supports trust and reduces the chance that users retreat to cash or limit digital activity.

An ASEAN comparative lens suggests that the quality–security–trust architecture is likely to hold across markets, though the relative strength of privacy concern may vary. In countries where data protection regulation is perceived as strong and enforcement visible, privacy concern may exert less friction, allowing security signals to translate more smoothly into trust. Where regulation is fragmented or publicized breaches are common, privacy concern may intensify, requiring banks to provide clearer data-use transparency and user controls. Cambodia and Vietnam, for example, exhibit rapid digital finance growth alongside diverse regulatory maturity; users may rely more heavily on institutional reputation and incident-response visibility. Indonesia's scale and heterogeneity can generate varying levels of privacy anxiety, making localized consumer education and consistent disclosure practices critical.

Managerial implications are practical. Banks seeking retention should treat service quality as trust infrastructure. Technical stability, clear information, and responsive support reduce ambiguity that users interpret as risk. Privacy concern can be addressed through explicit data-use disclosures, permission minimization, and user-facing controls that make privacy boundaries visible. Security messaging should avoid alarmism that normalizes fear; instead it should cultivate informed confidence by explaining protections and providing straightforward steps when incidents occur.

Policy implications extend to consumer protection. Regulators and industry bodies can support retention and inclusion by encouraging standard disclosure formats for fees and data use, promoting incident-reporting norms, and strengthening coordination against scams. Consumer literacy programs that integrate privacy awareness with secure behavior can reduce anxiety without shifting responsibility entirely onto users. Limitations suggest future research directions. Cross-sectional designs limit temporal inference; longitudinal tracking could reveal how incidents or policy changes shift privacy concern and trust over time. Multi-group comparisons across age cohorts and digital experience levels could clarify who is most affected by privacy friction. Linking survey perceptions to objective service outage and incident data could strengthen causal interpretation.

A complementary interpretation views service quality as a form of institutional reassurance. Financial applications compress the distance between user action and potentially irreversible outcomes. When the interface communicates clearly through consistent labels, timely confirmations, and intelligible error messages, users experience lower cognitive uncertainty, which reduces privacy driven rumination and supports stable habits. This reassurance function is particularly important for older users or those with limited digital confidence, who may interpret interface ambiguity as evidence of hidden risk.

Privacy concern also interacts with cultural expectations about data boundaries. Users may tolerate certain data collection when the perceived benefits are obvious, yet they may resist data reuse for targeted marketing or third party integration. Banks that offer granular controls and explain why specific permissions are necessary can transform privacy concern from a generalized anxiety into a manageable evaluation. Such transformation can strengthen the conversion of security into trust.

Incident response readiness can be treated as a service quality subdimension in future research. Users rarely observe cybersecurity investments directly, but they do observe how banks communicate after incidents, how quickly accounts can be secured, and how disputes are resolved. Transparent incident narratives and timely support can protect trust even when incidents occur, suggesting that resilience communication is part of retention strategy.

A measurement agenda could decompose perceived security into confidentiality, integrity, and availability beliefs. Users may feel that authentication protects confidentiality yet still worry about system availability during peak periods. Similarly, transparency could be modeled as a moderator that reduces privacy concern by clarifying data practices. These refinements can deepen understanding of how banks can reduce avoidance behavior without downplaying legitimate privacy risks. From an ASEAN policy standpoint, interoperability initiatives may influence trust formation indirectly. When users can transfer funds seamlessly across banks and wallets, they may interpret the ecosystem as more mature and governed. Maturity signals can reduce anxiety, although they may also expand data sharing pathways that heighten privacy concern. Balancing interoperability with data minimization thus becomes a strategic regulatory question.

E. CONCLUSION

This study shows that mobile banking service quality supports continued usage intention among Thai consumers through perceived security and trust, while privacy concern weakens key conversion mechanisms. The findings indicate that retention depends on more than functional convenience: users continue using mobile banking when the digital experience signals competence, when security feels credible, and when data practices do not trigger persistent anxiety. For banks and policymakers, the results suggest that improving retention requires integrated governance. Stability and responsiveness build security confidence, transparent communication builds trust, and privacy-sensitive design reduces friction that otherwise limits the payoff of security investments. As ASEAN markets expand digital finance, combining technical safeguards with data-use transparency and consumer education can strengthen sustained engagement and reduce avoidance behavior.

REFERENCES

Almaiah, M. A., Al-Otaibi, S., Shishakly, R., Hassan, L., Lutfi, A., Alrawad, M., Qatawneh, M., & Alghanam, O. A. (2023). Investigating the role of perceived risk, perceived security and perceived trust on smart m-banking application using SEM. *Sustainability*, *15*(13), 9908.

Biswas, B., Nur Ullah, M., Rahman, M. M., & Al Masud, A. (2024). Service quality, satisfaction, and intention to use Pourasava Digital Center in Bangladesh: The moderating effect of citizen participation. *PloS One*, *19*(6), e0304178.

Çallı, L. (2023). Exploring mobile banking adoption and service quality features through user-generated content: the application of a topic modeling approach to Google Play Store reviews. *International Journal of Bank Marketing*, *41*(2), 428–454.

Chiu, J. L., Bool, N. C., & Chiu, C. L. (2017). Challenges and factors influencing initial trust and behavioral intention to use mobile banking services in the Philippines. *Asia Pacific Journal of Innovation and Entrepreneurship*, *11*(2), 246–278.

Chuchuen, C., & Chanvarasuth, P. (2022). The role of trust in mobile payment adoption: A case study of Thailand. *ABAC Journal*, *42*(4), 64.

Ha, M. T., Tran, K. T., Sakka, G., & Ahmed, Z. U. (2024). Understanding perceived risk factors toward mobile payment usage by employing extended technology continuance theory: a Vietnamese consumers' perspective. *Journal of Asia Business Studies*, *18*(1), 158–182.

Hafez, M. (2023). Examining the effect of consumption values on mobile banking adoption in Bangladesh: the moderating role of perceived security. *Kybernetes*, *52*(12), 6232–6250.

Hanif, Y., & Lallie, H. S. (2021). Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM-with perceived cyber security, risk, and trust. *Technology in Society*, *67*, 101693.

Inan, D. I., Hidayanto, A. N., Juita, R., Soemawilaga, F. F., Melinda, F., Puspacinantya, P., & Amalia, Y. (2023). Service quality and self-determination theory towards continuance usage intention of mobile banking. *Journal of Science and Technology Policy Management*, *14*(2), 303–328.

IVANOVA, A., & NOH, G. (2022). The impact of service quality and loyalty on adoption and use of mobile banking services: Empirical evidence from Central Asian context. *The Journal of Asian Finance, Economics and Business*, *9*(5), 75–86.

Kim, L., Wichianrat, K., & Yeo, S. F. (2024). An integrative framework enhancing perceived e-banking service value: A moderating impact of e-banking experience. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(3), 100336.

Kumar, P., Chauhan, S., Gupta, P., & Jaiswal, M. P. (2023). A meta-analysis of trust in mobile banking: the moderating role of cultural dimensions. *International Journal of Bank Marketing*, *41*(6), 1207–1238.

Mahakunajirakul, S. (2022). Mobile banking adoption in Thailand: the moderating role of hedonic and utilitarian consumer types. *The Journal of Behavioral Science*, *17*(1), 85–99.

Namahoot, K. S., & Laohavichien, T. (2018). Assessing the intentions to use internet banking: The role of perceived risk and trust as mediating factors. *International Journal of Bank Marketing*, *36*(2), 256–276.

Naruetharadhol, P., Ketkaew, C., Hongkanchanapong, N., Thaniswannasri, P., Uengkusolmongkol, T., Prasomthong, S., & Gebsombut, N. (2021). Factors affecting sustainable intention to use mobile banking services. *Sage Open*, *11*(3), 21582440211029924.

Nguyen, Y. T. H., Tapanainen, T., & Nguyen, H. T. T. (2022). Reputation and its consequences in Fintech services: the case of mobile banking. *International Journal of Bank Marketing*, *40*(7), 1364–1397.

Palamidovska-Sterjadovska, N., Rasul, T., Lim, W. M., Ciunova-Shuleska, A., Ladeira, W. J., De Oliveira Santini, F., & Bogoevska-Gavrilova, I. (2025). Service quality in mobile banking. *International Journal of Bank Marketing*, *43*(6), 1195–1230.

Pokhrel, L., & KC, A. (2024). Mobile banking service quality and continuance intention: mediating role of satisfaction: a two-stage structural equation modeling-artificial neural network approach. *International Journal of Bank Marketing*, *42*(3), 389–413.

Puriwat, W., & Tripopsakul, S. (2017). The impact of e-service quality on customer satisfaction and loyalty in mobile banking usage: Case study of Thailand. *Polish Journal of Management Studies*, *15*(2), 183–193.

Qatawneh, A. M., & Makhlouf, M. H. (2025). Influence of smart mobile banking services on senior banks' clients intention to use: moderating role of digital accounting. *Global Knowledge, Memory and Communication*, *74*(3–4), 1028–1044.

Rabaa'i, A. A., & ALMaati, S. A. (2021). Exploring the determinants of users' continuance intention to use mobile banking services in Kuwait: extending the expectation-confirmation model. *Asia Pacific Journal of Information Systems*, *31*(2), 141–184.

Rajaobelina, L., Prom Tep, S., Arcand, M., & Ricard, L. (2021). The relationship of brand attachment and mobile banking service quality with positive word-of-mouth. *Journal of Product & Brand Management*, *30*(8), 1162–1175.

Rakangthong, N. K., Kim, L., Ru-Zhue, J., Nupueng, S., & Issayeva, G. (2025). From service attributes to e-banking value development influencing e-banking user feedback: a moderating effect of technological competency: NK Rakangthong et al. *Journal of Financial Services Marketing*, *30*(2), 14.

Silanoi, W., Naruetharadhol, P., & Ponsree, K. (2023). The confidence of and concern about using mobile banking among generation Z: A case of the post COVID-19 situation in Thailand. *Social Sciences*, *12*(4), 198.

Sreejesh, S., & Anusree, M. R. (2016). Effect of information content and form on customers' attitude and transaction intention in mobile banking: Moderating role of perceived privacy concern. *International Journal of Bank Marketing*, *34*(7), 1092–1113.

Van, H. N., Pham, L., Williamson, S., Chan, C.-Y., Thang, T. D., & Nam, V. X. (2021). Explaining intention to use mobile banking: Integrating perceived risk and trust into the technology acceptance model. *International Journal of Applied Decision Sciences*, *14*(1), 55–80.

Van, H. N., Pham, L., Williamson, S., Huong, V. T., Hoa, P. X., & Trang, P. L. H. (2020). Impact of perceived risk on mobile banking usage intentions: trust as a mediator and a moderator. *International Journal of Business and Emerging Markets*, *12*(1), 94–118.

Wichittakul, C., & Prasongsukarn, K. (2018). Factors affecting the level of trust in mobile banking: A case study of customer perception toward commercial mobile banking adoption in Bangkok, Thailand. *2018 5th International Conference on Business and Industrial Research (ICBIR)*, 429–434.

Zalloum, L., Alghadeer, H., & Nusairat, N. (2019). The effect of using mobile banking services applications on electronic word of mouth: The mediating role of perceived trust. *International Business Research*, *12*(9), 62–80.