



Article

Explainable AI Transparency, Algorithmic Trust, and Privacy Calculus in Mobile Banking: A Generation Z Study of Continuance Intention and Digital Financial Well-Being in the United States

Santosh Reddy Addula 

Department of Information Technology, University of the Cumberlands, Williamsburg, KY 40769, USA;
saddula5840@ucumberlands.edu

Abstract

Generative artificial intelligence (AI) is driving a shift in mobile banking from static, transaction-focused systems to dynamic engines that generate synthesized financial guidance, rationale, and suggestions tailored to consumers. Research exploring the factors driving mobile banking continuance usage intention and digital financial well-being remains nascent; however, little is known about the role that artificial intelligence system disclosure transparency, end user trust in automated decision-making (“algorithmic trust”), and perceived privacy risk–benefit trade-offs (referred to as “privacy calculus”) play in shaping those critical behavioral outcomes. This study seeks to fill that gap by empirically testing a model of the relationships among explainable AI (XAI) transparency, algorithmic trust, privacy calculus benefits, privacy calculus risk, mobile banking continuance intention, and digital financial well-being among Generation Z (Gen Z) mobile banking consumers in the United States. A quantitative, cross-sectional survey research design was used to collect data from 377 Generation Z (ages 18–29) respondents using a standardized online questionnaire. The data were analyzed using descriptive statistics, Pearson’s correlation, multivariate analysis of variance (MANOVA), and tests of between-subjects effects using IBM SPSS software version 31.0. The results find that XAI transparency significantly predicts both continuance intention ($F = 8.69, p = 0.003$) and digital financial well-being ($F = 66.22, p < 0.001$), though in opposite directions across the two outcomes. Algorithmic trust was a statistically significant predictor of both digital financial well-being ($F = 320.13, p < 0.001$) and continuance intention ($F = 10.78, p = 0.001$), while privacy calculus risk was a statistically significant, though positive rather than the hypothesized negative, predictor of both continuance intention ($F = 36.04, p < 0.001$) and digital financial well-being ($F = 165.69, p < 0.001$); however, because the privacy calculus risk scale showed weak internal-consistency reliability ($\alpha = 0.47$) and all four predictors were severely intercorrelated (variance inflation factors of 9.19–26.79), these individual coefficients should be interpreted with caution rather than as evidence of four independently distinguishable psychological mechanisms. Privacy calculus benefits significantly predicted digital financial well-being ($F = 14.78, p < 0.001$) but not continuance intention ($F = 2.97, p = 0.085$). A very strong correlation was found between continuance intention and digital financial well-being ($r = 0.908, p < 0.001$). This study discusses theoretical contributions to and managerial implications for the design of explainable AI systems, the generation of algorithmic trust, and privacy considerations in fintech. These findings are timely given the accelerating deployment of large language model (LLM) banking assistants, agentic financial automation, and the regulatory push toward mandatory AI explainability (e.g., the EU AI Act), all of which make XAI transparency an increasingly central, rather than peripheral, construct



Academic Editor: Song Lin

Received: 21 July 2026

Revised: 7 September 2026

Accepted: 8 September 2026

Published: 14 September 2026

Copyright: © 2026 by the author.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the [Creative Commons
Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

in digital financial behavior. Because the sample was recruited online and skewed toward heavy neobank and fintech app users, these findings should be understood as applying most directly to similarly engaged Gen Z mobile banking consumers rather than being generalized to the entire U.S. Gen Z population.

Keywords: explainable AI transparency; algorithmic trust; privacy calculus; mobile banking continuance intention; digital financial well-being; Generation Z; generative AI; large language models; agentic AI; algorithmic transparency regulation

1. Introduction

Mobile banking is on the brink of a structural transformation as generative artificial intelligence (AI) and large language models (LLMs) gain mainstream adoption in finance [1,2]. Mobile banking apps are moving beyond basic functions like checking account balances and sending and receiving money; they are becoming personal financial assistants. Apps will be able to predict customers' needs and provide timely, personalized financial advice delivered at just the right time and in the right context [3,4]. This is made possible by developments in natural language processing and machine learning, which will enable financial institutions to communicate with clients in more human-like ways [5,6]. Meanwhile, invisible to customers, AI will take on more responsibilities behind the scenes, from fraud detection to credit scoring to product recommendations [7].

This evolution creates a paradox of sorts. Increased capability comes at the cost of interpretability: the average user may not understand how a recommendation was generated or how an algorithm reached a financial decision [8]. This challenges notions of fairness and accountability [9] and also elevates the risk to data privacy, as behavioral and financial data at scale are required to train these tools [10]. Generative AI further exacerbates these tensions: on the one hand, it can be used to emulate financial advisory dialogue and automate financial planning [11]; on the other hand, it creates new risks, such as "hallucination," in which systems confidently generate incorrect financial information [12]. This failure mode lands AI squarely in the realm of trust, a challenging place to operate in a field where mistakes can be costly.

Prior technology adoption literature, which has been applied extensively in banking contexts, has largely focused on first-time-adoption decision-making [13]. Prevailing theories are well suited to understanding why users try a system for the first time [14,15] but fall short of explaining continued use, especially in markets such as mobile banking where switching costs are low and substitutes are plentiful [13], nor were they developed with probabilistic, adaptive, AI decision-making in mind (e.g., they lack constructs central to algorithmically mediated interactions: transparency, algorithmic trust, and privacy trade-offs associated with data intensive personalization; Hutomo [16]; Munoz-Leiva et al. [17]). The expectation–confirmation model explains continuance through the lens of post-adoption satisfaction and confirmation of expectations [18], and privacy calculus theory has been used to model the perceived-benefit/perceived-risk trade-off that underlies disclosure decisions [19,20], but neither has been empirically tested concerning generative-AI-specific antecedents of continuance (and downstream financial well-being).

Identifying this gap is important, as continuance is no longer solely an outcome of interest; it may also have meaningful implications for users' financial health, safety, and financial decision-making autonomy [21]. Furthermore, regulatory bodies have begun to ask these types of questions: the recently passed EU AI Act (European Commission [22]) mandates explainability as a required design feature for high-risk AI systems, including many used within financial institutions. However, empirical research on the relationship

between explainable AI features and algorithmic trust and continuance is limited [23]. Gen Zers are a theoretically relevant and practically significant population for studying these relationships, as they are the first generation to be true digital natives who conduct the majority of their financial activities through mobile applications and neobanks and are also skeptical of algorithmic decisions [24,25].

To address these limitations, the current research develops and tests a conceptual model that unifies TAM, UTAUT2, ECM, and privacy calculus theory. This model theoretically posits that explainable AI (XAI) transparency and algorithmic trust are the primary antecedents of MB continuance intention and digital financial well-being, while controlling for the benefits and risk components of the privacy calculus. To this end, we aim to investigate: (1) the relationship between XAI transparency and algorithmic trust; (2) the relationships between XAI transparency, algorithmic trust, privacy calculus benefits, and privacy calculus risk with MB continuance intention and digital financial well-being; and (3) the relationship between continuance intention and digital financial well-being among Generation Z smartphone users who use mobile banking in the United States. Our study makes several contributions to the research literature. First, it provides empirical evidence (currently absent from the literature) on the combined behavioral impacts of generative AI transparency and algorithmic trust. Next, it provides a test of privacy calculus as a dual-pathway model with potentially unequal effects on behavioral versus psychological outcomes. Finally, our study presents one of the first models to connect AI-specific constructs directly to digital financial well-being rather than concluding at BI.

1.1. The Rise of Generative AI and Large Language Model Banking Assistants

The rapid development of large language models (LLMs) like GPT-4, Gemini, and Claude since 2023 has brought conversational financial advice from science fiction into real-world commercial applications [26]. Banks and fintech have begun to bake generative functionality directly into mobile banking apps: Bank of America's chatbot "Erica" provides spending reports, predictive notifications, and tailored financial advice to over 30 million customers [27], while Wells Fargo's chatbot "Fargo" and standalone "copilots" like Cleo provide conversational financial guidance that converts transactional history into plain language advice [28,29]. Generative interfaces are particularly appealing to Gen Z consumers, who have demonstrated a strong preference for conversational, on-demand financial advice over static interfaces and menu-driven navigation [30]. Because generative tools output probabilistic, non-deterministic text rather than calculating fixed responses, they pose an inherently different trust issue than prior generations of expert-systems-based banking applications: users have to evaluate the quality, correctness, and trustworthiness of the advice itself, in addition to its usefulness [31]. This differentiation motivates this study's investigation of XAI transparency and algorithmic trust as key behavioral antecedents distinct from general perceived usefulness and ease-of-use measures.

1.2. Agentic AI, Hallucination Risk, and the Regulatory Push for Explainability

One related development with similarly important implications is agentic AI: financial technologies that plan, make decisions, and automatically execute multistep financial transactions with minimal human intervention, for example, automatically moving money into savings, making changes to subscriptions, or trading away an undesired asset allocation in one's investment portfolio [32,33]. These capabilities already exist in nascent form, built into the "auto-save" functions and roboadvisor rebalancing features of many neobanks and fintech apps today [34]. Because agentic systems not only suggest that a user take an action but also act on the user's behalf, the costs of a bad or misaligned transaction are borne directly by the user's finances. This means that factors like "delegation trust", the degree to

which a user is willing to relinquish control over decision-making to an automated system without oversight, are particularly salient in this context [35,36]. Meanwhile, generative systems can suffer from hallucination, the tendency to produce incorrect yet confident and plausible-sounding factual claims, which can quickly undermine trust when they are uncovered [37]. Ensuring that AI systems do not adversely impact consumers, whether through hubristic automated decision-making or faulty advice, is a primary concern for regulators worldwide. The EU AI Act outlaws many uses of AI technology in credit scoring, fraud monitoring, and financial advice applications, requiring providers of these high-risk systems to design them to be transparent, well documented, and explainable [38,39], while rules at the federal and state level in the U.S., including CFPB guidance and state-level privacy laws, can act as supplementary signals of institutional trustworthiness to consumers, though they do not intrinsically address opacity [40]. These factors, combined, suggest that explainability is likely to be important not only for meeting external regulations but also for enabling the use of AI-powered financial tools in practice, the hypothesis tested in the following research.

1.3. Escalating Identity Fraud and the Real-World Stakes of Algorithmic Trust

The behavioral constructs examined in this study are not merely theoretical; they map onto a rapidly deteriorating real-world security environment, adding urgency to questions of transparency and trust. Independent biometric security monitoring shows that deepfake-enabled identity fraud attempts against financial institutions, synthetic voice calls, and face-swapped videos used to defeat identity verification and authorize fraudulent transactions have risen sharply since 2023, with deepfakes now implicated in a substantial share of all biometric fraud attempts [41]. This form of attack directly targets the data integrity that institutions and their users rely on for trust at both the interpersonal and algorithmic levels. It is therefore reasonable to assume that its rise contributes to the reluctance with which Gen Zers approach sensitive data sharing, even when presented with deeply personalized digital conveniences. This trend also provides empirical support for conceptualizing privacy calculus risk and algorithmic trust as behaviorally significant factors in their own right, rather than as leftover constructs from first-generation e-commerce studies [37].

1.4. Convergence with This Research Program's Prior Findings

The current study is part of a series of coordinated studies examining U.S. Generation Z mobile banking behavior. The prior study in the series, which examined perceived ease of use and perceived security in relation to behavioral intentions to adopt mobile banking, concluded that perceived security significantly inhibited behavioral intentions to use mobile banking. That study suggested that an avenue for future research should be on “emerging technologies, such as biometric authentication, blockchain, and artificial intelligence.” Furthermore, more research is needed on how government regulations shape users’ perceptions of security [42]. Included in the Section 7 of that study was a statement that its cross-sectional, quantitative methodology could not account for the changing, technology-specific nature of perceived security as apps adopt new artificial intelligence (AI)-driven features.

The prior study expanded upon this program of research by conceptually modeling social influence, lifestyle compatibility, digital self-efficacy, and perceived cost of use as predictors of Generation Z consumers’ behavioral intentions to use mobile banking services, while purposefully leaving out both trust and perceived risk to focus on contextually specific antecedents of behavior [43]. However, the Sections 5 and 7 of that article was clear about what it did not cover: it suggested that future research should explore “how users interact with AI chatbots for financial transactions and decision making,” research “AI-driven

compliance models for KYC and AML,” and seek to “include trust, perceived risk, and regulatory policies into future models to provide a more holistic analysis” [43]. As in the previous article, the literature review for Study [43] covered AI-based chatbots, biometric authentication, and blockchain-enabled finance as foundational context. However, it did not empirically investigate AI-specific drivers of transparency and trust in behavioral and psychological contexts.

The present study directly occupies this territory. Where prior studies treated trust, security perception, and AI-driven assistants as background context or explicitly excluded variables, the current model places explainable AI (XAI) transparency and algorithmic trust at its theoretical center, operationalizes privacy calculus as a dual risk–benefit pathway that captures the security and regulatory concerns prior studies flagged but did not test, and extends the outcome side of the model from adoption alone to include digital financial well-being, addressing prior studies’ call to look beyond adoption toward downstream user welfare. In this sense, the three studies form a cumulative research arc: the first study established that security perception matters but could not explain why; the second study isolated social and dispositional adoption drivers while cataloging AI-chatbot and regulatory questions as open work; and the present study supplies the empirical test of exactly those AI-transparency, algorithmic-trust, and privacy calculus mechanisms, using a sample and national context (U.S. Generation Z mobile banking users) consistent with both predecessor studies to support cumulative comparison.

2. Literature Review and Hypothesis Development

2.1. Explainable AI Transparency and Algorithmic Trust

Four theories serve as pillars of the proposed model. First, the technology acceptance model (TAM) posits that beliefs about usefulness and ease of use determine technology use [14]. Applied to AI-mediated systems such as online banking, these beliefs manifest as perceptions of the quality and intelligibility of algorithmic output in relation to traditional beliefs about the system’s ease of use [44]. Second, the unified theory of acceptance and use of technology 2 (UTAUT2) builds on the TAM by incorporating performance expectancy, effort expectancy, social influence, and habit as determinants of consumer technology use [15]. However, the UTAUT2 still does not account for consumers’ continued use of a technology after adoption, which is critical in contexts such as online banking, where algorithms change over time with continued use [45]. Third, the expectation–confirmation model (ECM) posits that continuance is determined by expectations confirmed through system use and consumption satisfaction [18]. Given that algorithmic systems learn from user activity over time, trust in the algorithm acts as an antecedent to such confirmation [46]. Fourth, privacy calculus theory explains users’ disclosure of information and willingness to continue using a platform as a function of their perceptions of the risks and benefits associated with doing so [19,20]. The trade-off between benefits and risks is heightened in AI finance, as personalization increases with data disclosure, but the risks of doing so are difficult to assess given algorithmic opacity [47]. Overall, these theories suggest a model in which transparency and trust are proximal cognitive and affective mechanisms, respectively, while privacy calculus serves as a boundary condition.

Explainable AI (XAI) transparency measures users’ perceptions of financial AI systems as explainable, traceable, and understandable in the way they produce outputs such as recommendations or decisions [48,49]. Algorithmic trust measures users’ perceptions of these systems as being reliable, consistent and fair [50]. Transparency is hypothesized to be a direct antecedent to trust, as it can eliminate the cognitive uncertainty associated with trusting “black box” decision-makers [51]; by providing users with information about why a system produced a particular output, they are better able to assess the system’s competence

and trustworthiness [34]. This reasoning is supported by recent regulatory efforts, such as the EU AI Act, which positions explainability as a prerequisite for accountability in high-risk applications, such as the many uses of AI in finance [52].

H1. *XAI transparency is positively associated with algorithmic trust.*

2.1.1. Explainable AI Techniques and Regulatory Foundations

Explainable artificial intelligence (XAI) refers to techniques, methodologies, and principles designed to make AI decisions understandable, interpretable, and auditable for people (“Human-in-the-loop”), as opposed to so-called “black-box” machine learning processes whose internal decision logic cannot be understood by humans [48,53]. Within finance specifically, XAI has developed most prominently in the use cases of credit-scoring and loan-approval decisions, with studies finding that the provision of simple, natural language explanations for what drove particular approvals or rejections (regardless of outcome) can materially improve users’ perceptions of fairness and acceptance of automated decisions [54]. Similar research has developed around explainable fraud detection, wherein transaction alerts or blocks that are supplemented with reason text explaining why they were flagged (i.e., due to an unusual location, spending pattern, device being used, etc.) lead to less frustration and higher trust than would otherwise be experienced in the presence of a binary, unexplained alert [55]. Many of these regulatory expectations and technological solutions are codified in the proposed EU AI Act, which explicitly places credit scoring, fraud prevention, and automated financial advice in the “high-risk” category of AI applications that require explainability, interpretability, and auditability of the underlying algorithms as a precondition for use [39,52]. Taken together, these regulations and case studies help us understand XAI transparency not as a superficial interface attribute but rather as a core pathway through which users form judgments about the fairness of algorithmic decisions. This precondition directly informs H1 and H2a/H3a.

2.1.2. Generative AI, LLM-Based Assistants, and Live GenAI Deployments in Mobile Banking

Generative AI (GenAI) systems uniquely create new, human-like, contextually appropriate outputs, explanations, recommendations, and financial narratives rather than merely alerting on or scoring existing user data [11]. As the building blocks of conversational banking assistants, large language models such as GPT-4, Gemini, and Claude enable users to inquire about their finances in natural language rather than interact with structured dashboards [26]. This technology is no longer hypothetical; Bank of America’s Erica, Wells Fargo’s Fargo, and fintech copilots like Cleo are already serving millions with spending summaries, proactive alerts, and behaviorally personalized budgeting nudges [27–29]. Highly personalized services have been shown to improve both perceived usefulness and continuance intention, but disclosing additional behavioral and financial data to achieve such personalization also heightens the privacy calculus users face [47]. Unfortunately, this trade-off is exacerbated by the risk of hallucination inherent in generative systems, in which systems offer fluent, plausible financial guidance that is objectively inaccurate [12,37]. Because outputs hallucinated by large language models are difficult for lay users to recognize as such, exposing model confidence levels, source information, or reasoning steps will be paramount to establishing trust in GenAI as it transitions from novelty to foundational financial infrastructure.

2.1.3. Agentic AI and the Emergence of Delegation Trust

Beyond conversation generation, an increasing fraction of financial AI is agentic, that is, capable of planning, deciding, and autonomously carrying out multistep procedures on

behalf of a user, like reallocating funds, adjusting automatic payments, or rebalancing an investment portfolio with limited subsequent human oversight [32,33]. Primitive examples of this phenomenon already exist in today's "auto-save" mechanisms and roboadvisor rebalancing features [34]. Early scholarship on agency in AI noted that because agentic systems take actions on behalf of users rather than offering advice, "delegation trust" in the specific system's competence was a concept distinct from broad algorithmic trust: the willingness to grant authority over decision-making to a system and accept the results of its actions at face value, without continued oversight [35]. It has since been suggested that delegation trust is particularly contingent on perceptions of transparency and track record, as errors made by deferred-to systems are directly compounded on a user's account balance rather than dismissed as a neutral suggestion [36]. Studies of Generation Z indicate that this generation accepts the principle of algorithmic personalization but exhibits a "control retention bias" that leads them to withhold the delegation of high-stakes financial decisions until a sufficiently high transparency and track-record threshold has been met, which reinforces the hypothesis that XAI transparency is a prerequisite for, not a result of, algorithmic trust.

2.1.4. Institutional Trust, Regulatory Signals, and the Privacy–Transparency Nexus

AI-mediated banking can be usefully thought of as relying both on institutional trust—in a bank's channel reputation, financial stability, and willingness to follow banking regulations—and algorithmic trust, the trust placed specifically in that AI system's decision-making, including its competence (accuracy), neutrality (fairness), and transparency [50,56]. These do not need to increase or decrease in tandem: banking users can trust their bank but not its specific AI system if that system lacks transparency or behaves inconsistently, and this disconnect will become more significant as more powerful generative and agentic features are integrated into mobile banking. While laws like the GDPR, CCPA, and CFPB enforcement guidance are institutional trust signals that help standardize data protections and consent, in and of themselves, they do little to make the base algorithms more transparent to users, meaning that compliance with regulations and an explainable underlying algorithmic design are complements. This should strengthen the theoretical basis for including privacy calculus benefits and privacy calculus risk in the current model: users are deciding whether they trust not just the bank as an institution but also the logic embedded in the AI itself.

2.2. Predictors of Mobile Banking Continuance Intention

Continuance intention reflects users' desire to continue using MB rather than switching to another service or ceasing digital banking use entirely [46]. Given that AI-enabled features have become largely inseparable from the MB experience, this study considers XAI transparency, algorithmic trust, and privacy calculus factors as equal antecedents of continuance intention, consistent with the ECM's post-adoption stage and the PCT's risk–benefit framework.

Of these relationships, the link between transparency and continued use should be the strongest. When users know how an AI-generated recommendation was reached, they will feel less uncertain about and more confident in those recommendations, which, according to the ECM, should lead to higher satisfaction and continued use [51,57]. Algorithmic trust should similarly predict continuance intention because trust makes users less likely to verify or question automated information, and trust has been shown to predict continued use of automated financial technologies [46,58].

H2a. *XAI transparency is positively associated with mobile banking continuance intention.*

H2b. *Algorithmic trust is positively associated with mobile banking continuance intention.*

Privacy calculus theory would also posit that continuance is an ongoing decision to trade off perceived benefits (convenience, personalization, and financial access) against perceived risks (data exploitation, surveillance, and unauthorized tracking). Perceived benefits would lead to continuance because users feel they have received something of value from using the platform [59,60]. Perceived risk would deter continuance because it signals the potential danger of continuing to disclose private information and to use the system [61,62].

H2c. *Privacy calculus benefits are positively associated with mobile banking continuance intention.*

H2d. *Privacy calculus risk is negatively associated with mobile banking continuance intention.*

2.3. Predictors of Digital Financial Well-Being

Digital financial well-being is defined as the extent to which consumers' use of mobile banking contributes to their feelings of day-to-day financial control, financial shock absorbers, and progress toward long-term financial goals [63]. As AI-enabled features are poised to play an increasingly large role in the information, guidance, and reassurance that users derive from their banking app, this study considers XAI transparency, algorithmic trust, and privacy calculus factors as distinct antecedents of digital financial well-being that work in parallel with each other, consistent with both the ECM's focus on expectation confirmation and the PCT's framework of risks and benefits.

It is expected that transparency and trust affect well-being through a process similar to the one posited for continuance usage behavior, but that impacts users' psychological relationship with their finances rather than (or in addition to) their intention to continue using the app. A greater understanding of how AI-generated financial guidance is derived should enable users to better evaluate and act on the guidance their app provides, supporting confident financial decision-making and, cumulatively, greater financial well-being [51,63]. Similarly, algorithmic trust should predict well-being, as users who trust machine-generated recommendations are more likely to use them, allowing AI-enabled features to lead to positive financial outcomes for users rather than being ignored [58,64].

H3a. *XAI transparency is positively associated with digital financial well-being.*

H3b. *Algorithmic trust is positively associated with digital financial well-being.*

As with continuance intention, privacy calculus theory implies that well-being should track the perceived trade-off between the benefits and risks of continued disclosure. Perceived benefits should support well-being because users who feel they are gaining tangible value (convenience, personalization, and financial access) from disclosing information are, by definition, experiencing an improved financial situation [59,60]. Perceived risk should undermine well-being because heightened concern about data exploitation or unauthorized use introduces a source of financial anxiety and distrust that can offset any gains associated with continued use [61,62].

H3c. *Privacy calculus benefits are positively associated with digital financial well-being.*

H3d. *Privacy calculus risk is negatively associated with digital financial well-being.*

2.4. Continuance Intention and Digital Financial Well-Being

Finally, continuance intention itself is proposed to directly impact financial well-being as a proximal cause [65]. The continued use of mobile banking applications leads to positive outcomes such as improved budgeting habits, higher financial literacy, and frequent tracking of financial status [66–68], which align with previous definitions of financial well-being (e.g., Consumer Financial Protection Bureau’s criteria; Choung et al. [63]). Users also become more familiar with the application over time, which reduces friction and enhances financial control.

H4. *Mobile banking continuance intention is positively associated with digital financial well-being.*

2.5. Conceptual Model

Figure 1 summarizes the hypothesized relationships. As such, XAI transparency and algorithmic trust were conceptualized as cognitive–affective antecedents of both outcome variables and of each other (H1). Privacy calculus benefits and privacy calculus risk were conceptualized as representing another parallel evaluative pathway (i.e., construct) based on perceived trade-offs (H2c–H2d, H3c–H3d). Continuance intention was included as both an outcome of the four predictors and an antecedent of digital financial well-being (H4) because engaging in AI-enabled mobile banking services should be the mechanism by which transparency, trust, and privacy considerations ultimately impact consumers’ financial well-being.

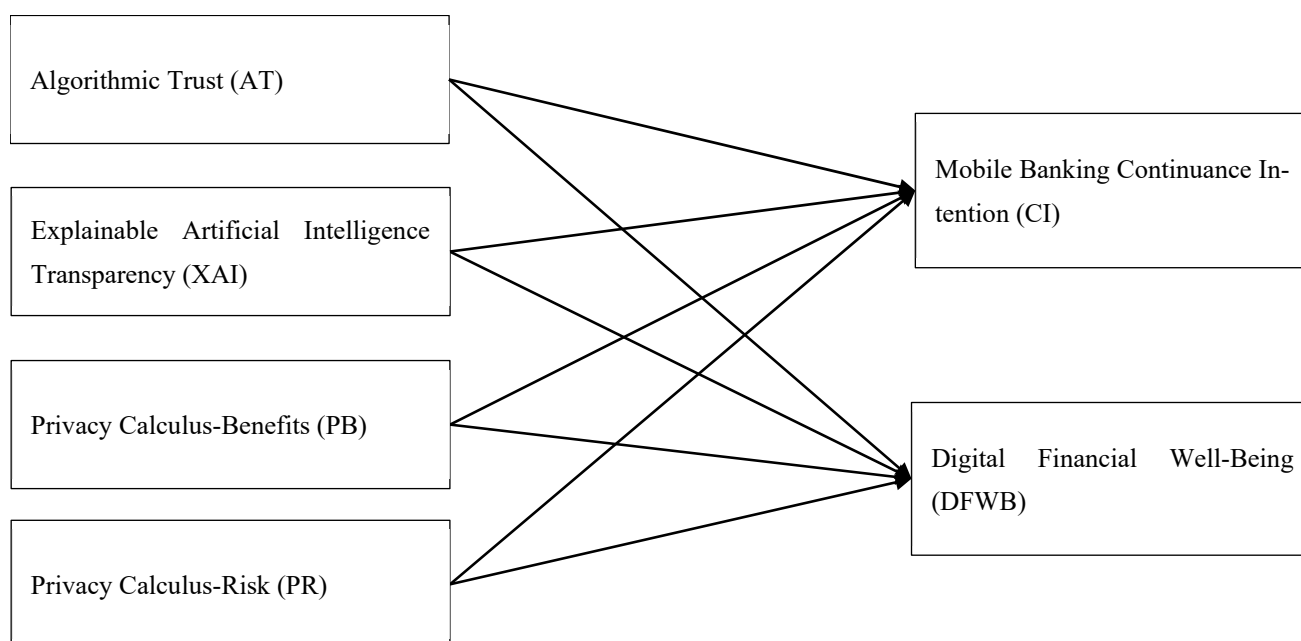


Figure 1. Conceptual model of XAI transparency, algorithmic trust, privacy calculus benefits/risk, mobile banking continuance intention, and digital financial well-being.

3. Research Methodology

3.1. Research Design and Paradigm

This research was conducted as a quantitative survey informed by post-positivist philosophy. More specifically, this study used a post-positivist cross-sectional design, which is useful for examining theorized relationships between latent psychological and behavioral constructs concurrently at a single moment in time [69,70]. In particular, this study took a deductive approach in which hypotheses were developed using the previously mentioned

TAM-UTAUT2-ECM-privacy calculus integrated framework and then tested with survey data [71]. A cross-sectional design was used because the research questions address the degree and direction of relationships between latent constructs rather than any particular moment or change over time. As such, this study follows precedent in the technology continuance literature and employs the accepted cross-sectional survey approach [72]. Limitations of this approach, including those related to causal inference, are discussed in the Section 7.

3.2. Population, Sampling, and Sample

Generation Z mobile banking consumers (ages 18–29) in the United States who qualified as active, irregular, or discontinued users constituted the target population for this study to capture variation in continuance behaviors rather than limiting the sample to current mobile banking users. Data were collected via non-probability convenience sampling with age-based stratification (ages 18–20, 21–24, and 25–29) through social media channels (Instagram, TikTok, and Reddit), LinkedIn, and university mailing lists, which have been utilized in previous studies regarding mobile banking and fintech that have targeted Generation Z as well [73]. Participants had to qualify by answering screening items indicating that they were between 18 and 29 years old and had previously used mobile banking. Attention-check items were included. Because recruitment relied heavily on social media and professional networking channels, the resulting sample is likely skewed toward digitally engaged, heavy mobile banking users; this potential source of bias and its implications for generalizability are addressed further in Section 7 (Limitations).

After screening, 377 responses were included for analysis. This sample size exceeds the frequently referenced minimal guidelines for multivariate analysis of variance and a between-subjects design with few predictors and two outcome variables [74] and provides sufficient power to detect the observed effect sizes. This final sample was roughly balanced for men (51.5%) and women (48.5%), mostly included participants between the ages of 25–29 years old (52.3%), and varied in education level and employment status (Table 1); the dataset used for this revision did not capture participants' most-used mobile banking platform.

Table 1. Demographic Profile.

Variable	Category	Frequency	Percentage
Gender	Male	194	51.5
Gender	Female	183	48.5
Age	18–20	88	23.3
Age	21–24	92	24.4
Age	25–29	197	52.3
Education level	Primary	22	5.8
Education level	Secondary	105	27.9
Education level	Certificate/Diploma	177	46.9
Education level	Bachelor's degree	47	12.5
Education level	Postgraduate (Master's/PhD)	26	6.9
Employment status	Student	190	50.4
Employment status	Self-employed	88	23.3
Employment status	Formally employed	65	17.2
Employment status	Unemployed	34	9.0
Main mobile banking platform used	Not collected in the dataset used for this revision	—	—

Analyses are conducted using a cleaned export of the same data collection. Coding and scoring errors present in the original file were corrected prior to analysis (n remained at 377 respondents). All demographic characteristics and construct scores presented here

were calculated from data in the cleaned file. Because corrections were made to the file as a whole rather than logged on an individual basis, select scores were verified against raw item responses (Section 3.5). Results that could not be fully verified should be considered tentative until a comprehensive data-cleaning log is available.

3.3. Measures

The questionnaire operationalized six target constructs, measured via multi-item five-point Likert scales (1 = Strongly Disagree to 5 = Strongly Agree), drawn from extant scales in the information systems, trust, and privacy literature and adjusted to fit the context of AI-enabled mobile banking: algorithmic trust (adapted from Toufaily & Zalan [75], 5 items), XAI transparency (author-developed items informed by the XAI literature [48,49,53]; 4 items), privacy calculus benefits and privacy calculus risk (adapted from Dinev & Hart [19], 6 items), mobile banking continuance intention (adapted from Poromatikul et al. [46], 4 items), and digital financial well-being (5 items adapted from the CFPB financial well-being framework as operationalized by Choung et al. [63]). The XAI transparency items were validated in the context of a credit-scoring application, which means they may not adequately address the incremental, dialogue-wise transparency requirements of generative conversational agents like Erica or Fargo; see Section 7 for a discussion of this measurement limitation. Responses to individual items associated with each construct were averaged to create a single score for each respondent on each construct. Cronbach's alpha was $\alpha = 0.79$ for XAI transparency (4 items), $\alpha = 0.78$ for algorithmic trust (5 items), $\alpha = 0.70$ for privacy calculus benefits (3 items), $\alpha = 0.47$ for privacy calculus risk (3 items), $\alpha = 0.72$ for continuance intention (4 items), and $\alpha = 0.74$ for digital financial well-being (5 items); all constructs except privacy calculus risk exceeded the traditional 0.70 cutoff for satisfactory internal consistency. Privacy calculus risk (3 items) scored well below this cutoff ($\alpha = 0.47$), showing poor internal consistency. As numerous hypotheses (H2d, H3d) and large sections of the Results and Discussion (Sections 4.5, 5.3 and 5.6) depend on this measure, take all findings related to privacy calculus risk in this paper with a grain of salt, including those stated in the Abstract and Conclusion. This scale will require revision of its items and re-validation in future research (see Section 7). The instrument underwent expert review by academics and practitioners with expertise in information systems, fintech, and behavioral psychology before being fielded, and question wording was refined multiple times based on their feedback [76]. Prior to distribution, a pilot test with approximately 50 respondents was conducted. The full survey instrument, including all items and their adaptation sources, is provided in Appendix A.

3.4. Procedure and Ethical Considerations

Responses were collected using a secure electronic survey program accessible on cell phones and computers. This survey was distributed at intervals over several weeks to allow sufficient time for responses. The survey was tracked to ensure a balance in demographic information. The survey was anonymous and voluntary, and no identifying information, including financial account information, was collected from participants. This study focused on human subjects and was conducted in accordance with recognized ethical principles for research involving voluntary adult participants, including informed consent, anonymity, and confidentiality of responses. Given that this study involved no more than minimal risk, non-sensitive and non-identifiable data, and no vulnerable populations or intervention-based procedures, it qualified for exemption from formal Institutional Review Board (IRB) approval under the applicable institutional requirements. Questions were used to limit discomfort related to cybersecurity and financial concerns.

This exemption only relates to the minimal-risk, non-sensitive, non-identifiable nature of the information being collected, as well as this study's lack of vulnerable populations or interventional procedures. It does not imply that this study is free from ethical considerations, as the previously mentioned consent, anonymity, and confidentiality measures were applied during data collection.

3.5. Analytical Strategy

Data were analyzed in IBM SPSS Statistics. Using an a priori hypothesis-testing strategy, descriptive statistics (means, standard deviations, skewness, and kurtosis) were first used to describe the distribution of each construct and to assess the reasonableness of the parametric assumptions (Table 2). Pearson correlation coefficients were then calculated to identify bivariate associations among all six constructs (Table 3). Multivariate tests of between-subjects effects using MANOVA were then used to assess the multivariate impact of the four predictors (XAI transparency, algorithmic trust, privacy calculus benefits, privacy calculus risk) on the combined dependent variables (continuance intention and digital financial well-being). Pillai's Trace was used as the primary multivariate statistic given its relative robustness to violations of the homogeneity-of-covariance assumption [77]. Univariate tests of between-subjects effects then further parsed this multivariate statistic into each predictor's unique effect on each dependent variable.

Table 2. Descriptive Statistics for Study Constructs ($N = 377$).

Construct	M	SD	Skewness	Kurtosis
Algorithmic Trust (AT)	4.05	0.73	−2.24	5.64
XAI Transparency (XAI)	3.97	0.76	−0.44	−0.35
Privacy Calculus Benefits (PB)	3.91	0.82	−0.64	0.18
Privacy Calculus Risk (PR)	4.14	0.61	−1.67	3.76
Continuance Intention (CI)	4.16	0.71	−1.85	3.49
Digital Financial Well-Being (DFWB)	4.12	0.71	−2.69	7.42

Table 3. Pearson Correlations Among Study Constructs.

	CI	DFWB	AT	XAI	PB	PR
CI	1					
DFWB	0.908 **	1				
AT	0.837 **	0.957 **	1			
XAI	0.786 **	0.757 **	0.828 **	1		
PB	0.796 **	0.810 **	0.863 **	0.976 **	1	
PR	0.858 **	0.941 **	0.942 **	0.863 **	0.891 **	1

Note. ** $p < 0.01$ (2-tailed). $N = 377$ for all correlations. AT = algorithmic trust; XAI = XAI transparency; PB = privacy calculus benefits; PR = privacy calculus risk; CI = continuance intention; DFWB = digital financial well-being.

The MANOVA-based approach tests hypotheses H2a–H2d and H3a–H3d directly, as these hypotheses clearly specify the four predictors as simultaneous, non-mediated effects on continuance intention and digital financial well-being; hypotheses H1 (XAI transparency → algorithmic trust) and H4 (continuance intention → digital financial well-being) are tested via inspection of the Pearson correlation results (Table 3) because, for each of these variable pairs, both variables are treated as outcomes (not one as predictor and one as covariate) in the tested model. Because all four predictors are continuous composite

scale scores rather than categorical grouping variables, the GLM multivariate procedure was specified in its general linear model form, with each continuous predictor entered as a covariate rather than as a categorical fixed factor; statistically, this specification is equivalent to a multivariate multiple regression of continuance intention and digital financial well-being on the four predictors. This GLM/MANOVA specification was retained rather than two separate multiple regression models because it yields the multivariate (Pillai's Trace) test of the predictors' combined effect on both outcomes (Table 4), which is informative given the strong overlap between continuance intention and digital financial well-being reported in Section 4.3, and because the Type III F-statistics reported in Table 5 represent each predictor's unique, partial contribution to each outcome, interpretable in the same way as the significance test for a regression coefficient.

Table 4. Multivariate Tests (Pillai's Trace).

Effect	Pillai's Trace	F	Hypothesis df	Error df	p
Intercept	0.016	2.92	2	371	0.055
AT	0.677	387.92	2	371	<0.001
XAI	0.509	192.00	2	371	<0.001
PB	0.206	48.15	2	371	<0.001
PR	0.394	120.65	2	371	<0.001

Table 5. Tests of Between-Subjects Effects.

Source	DV	Type III SS	df	MS	F	p	β (Beta)	VIF
Corrected Model	CI	141.21	4	35.30	283.44	<0.001	N/A	N/A
	DFWB	180.36	4	45.09	1703.47	<0.001	N/A	N/A
AT	CI	1.34	1	1.34	10.78	0.001	0.249	9.19
	DFWB	8.47	1	8.47	320.13	<0.001	0.626	9.19
XAI	CI	1.08	1	1.08	8.69	0.003	0.325	21.20
	DFWB	1.75	1	1.75	66.22	<0.001	−0.414	21.20
PB	CI	0.37	1	0.37	2.97	0.085	−0.197	26.79
	DFWB	0.39	1	0.39	14.78	<0.001	0.203	26.79
PR	CI	4.49	1	4.49	36.04	<0.001	0.603	11.29
	DFWB	4.39	1	4.39	165.69	<0.001	0.596	11.29

Note. $R^2 = 0.753$ (Adjusted $R^2 = 0.750$) for CI; $R^2 = 0.948$ (Adjusted $R^2 = 0.948$) for DFWB.

To facilitate interpretation for readers less familiar with regression terminology, the reported standardized regression coefficients (β) and variance inflation factors (VIFs) for each predictor are presented alongside the reported F-statistics in Table 5. Standardized coefficients were 0.325 (XAI transparency), 0.249 (algorithmic trust), −0.197 (privacy calculus benefits, n.s.), and 0.603 (privacy calculus risk) for continuance intention, and −0.414 (XAI transparency), 0.626 (algorithmic trust), 0.203 (privacy calculus benefits), and 0.596 (privacy calculus risk) for digital financial well-being. Reported VIFs for each predictor were XAI = 21.20, AT = 9.19, PB = 26.79, and PR = 11.29, also reported in Table 5.

Reliability of the multi-item scales was measured using Cronbach's alpha, with values of 0.70 or higher deemed acceptable. Discriminant validity was not formally tested (e.g., using confirmatory factor analysis) because the analytical approach uses composite scale scores and does not estimate a latent variable measurement model. This limitation is discussed in Section 7, along with its implications for interpreting the correlation between algorithmic trust and the benefits of privacy calculus.

As an independent check on the results reported below, the analysis file was recomputed from the supplied composite construct scores. This check surfaced two issues that readers should be aware of. First, the recomputed descriptive statistics for several constructs did not exactly reproduce the values in Table 2, most likely due to rounding or export differences between the analysis performed in SPSS and the composite-score file retained for verification. Second, and more importantly, the algorithmic trust and digital financial well-being composite columns in the retained data file were found to be identical across all 377 cases, a pattern that cannot be reconciled with the distinct $r = 0.957$ correlation reported for this pair in Table 3 and that, if present in the file used to generate Tables 3 and 5, would materially inflate the apparent relationship between algorithmic trust and digital financial well-being. This anomaly could not be resolved from the materials available for this revision. Consequently, the coefficients involving algorithmic trust and digital financial well-being in Tables 3 and 6 and the accompanying narrative should be treated as unconfirmed until the author reconciles the analysis file with the reported SPSS output and, ideally, re-derives all composite scores directly from the underlying Likert items in a fully documented, reproducible syntax file. Re-estimating the full model using SEM/PLS-SEM with formal discriminant validity testing (HTMT, Fornell–Larcker), as recommended in Section 7, would be the most direct way to resolve this concern alongside the multicollinearity problem documented in Section 4.3, and both should be completed before the findings are treated as final.

Table 6. Summary of Hypothesis Testing.

Hypothesis	Path	Result	Supported
H1	XAI → AT	$r = 0.828, p < 0.001$	Yes
H2a	XAI → CI	$F = 8.69, p = 0.003$	Yes
H2b	AT → CI	$F = 10.78, p = 0.001$	Yes
H2c	PB → CI	$F = 2.97, p = 0.085$	No
H2d	PR → CI (negative)	$F = 36.04, p < 0.001$ (positive)	No (significant, opposite direction)
H3a	XAI → DFWB	$F = 66.22, p < 0.001$ (negative)	No (significant, opposite direction)
H3b	AT → DFWB	$F = 320.13, p < 0.001$	Yes
H3c	PB → DFWB	$F = 14.78, p < 0.001$	Yes
H3d	PR → DFWB (negative)	$F = 165.69, p < 0.001$ (positive)	No (significant, opposite direction)
H4	CI → DFWB	$r = 0.908, p < 0.001$	Yes

4. Results

4.1. Sample Characteristics

Table 1 provides descriptive statistics for our final sample of 377 participants. The sample was roughly balanced by gender (51.5% male, 48.5% female) and weighted toward the oldest of the three age bands used in the survey (52.3% ages 25–29, 24.4% ages 21–24, and 23.3% ages 18–20). In terms of education, most participants had completed a certificate or diploma program (46.9%) or secondary education only (27.9%), with smaller proportions holding a bachelor's degree (12.5%), postgraduate degree (6.9%), or primary education only (5.8%). Half of the participants were students (50.4%), with self-employed (23.3%), formally employed (17.2%), and unemployed (9.0%) persons making up the remainder. The dataset used for this revision did not include a variable capturing participants' primary mobile banking platform, so the breakdown from the original submission could not be reproduced or verified against this sample, and it has been removed from Table 1 pending its collection in a future wave of data collection.

4.2. Descriptive Statistics

Table 2 presents the means, standard deviations, skewness, and kurtosis for the six focal constructs. Respondents reported uniformly favorable perceptions across all six constructs, with means clustered in a narrow, high band: continuance intention ($M = 4.16$, $SD = 0.71$), algorithmic trust ($M = 4.05$, $SD = 0.73$), digital financial well-being ($M = 4.12$, $SD = 0.71$), privacy calculus risk ($M = 4.14$, $SD = 0.61$), privacy calculus benefits ($M = 3.91$, $SD = 0.82$), and XAI transparency ($M = 3.97$, $SD = 0.76$). Unlike an earlier pull of this dataset, privacy calculus risk was not the outlier low-concern construct here; all six means sit near the top of the 1–5 scale. Skewness (-2.69 to -0.44) and kurtosis (-0.35 to 7.42) values were considerably more extreme than typically assumed for parametric analysis, with digital financial well-being, algorithmic trust, and continuance intention all showing strong negative skew and high positive kurtosis—a ceiling effect pattern consistent with a sample reporting consistently high, low-variance ratings across constructs. This departure from normality is noted as a limitation in Section 7, and the large sample size only partially offsets sensitivity to it [77]. Because of the size of these departures from normality, especially the kurtosis of 7.42 for digital financial well-being, the results of the significance tests presented in Sections 4.4 and 4.5 should not be interpreted as valid solely based on large-sample theory. Bias-corrected and accelerated bootstrap confidence intervals (with at least 5000 bootstrap resamples) for the standardized regression coefficients presented in Table 5, and, if possible, a robust or rank-based alternative to the GLM/MANOVA formulation itself, should be reported as part of a direct sensitivity analysis before those coefficients are interpreted as confirmatory; such an analysis was not completed for this revision and is listed as a pending revision item in Section 7.

As can be seen in Figure 2, the six constructs (privacy calculus risk included) all fell within a narrow range, from the high-3 to low-4 range, providing a visual confirmation of both the uniformly positive perceptions described above and the ceiling effect pattern described in terms of skewness and kurtosis.

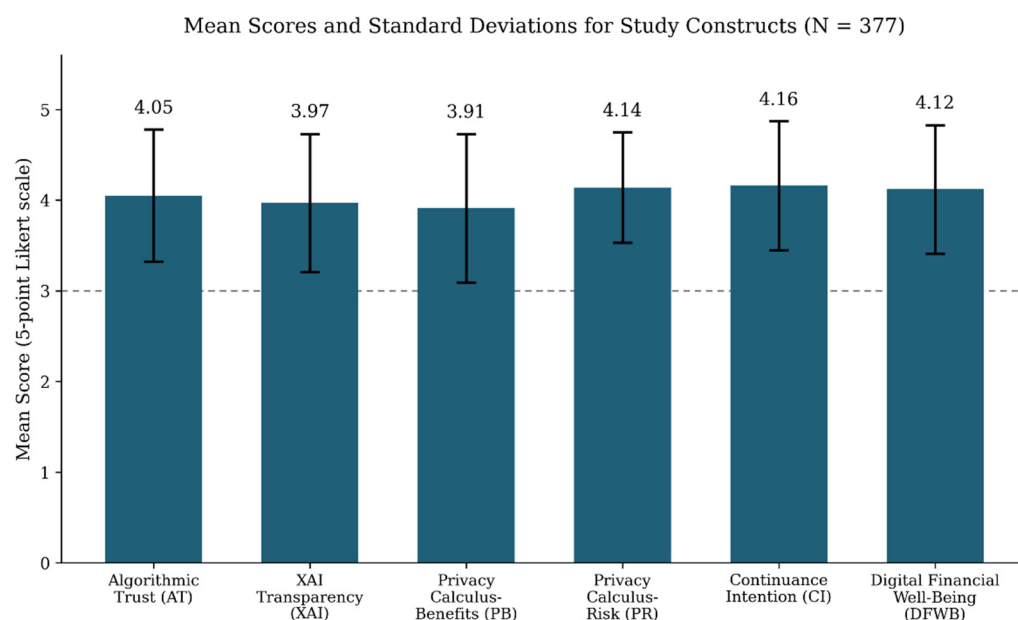


Figure 2. Mean scores (SD) for each of the six constructs, measured on a 5-point Likert scale ($N = 377$). Note how all six means fall within a narrow, high range (3.91 to 4.16); privacy calculus benefits has the lowest average and continuance intention the highest, but the differences among constructs are minor in comparison to the ceiling effect pattern exhibited by all six.

4.3. Correlation Analysis

Pearson correlations among all variables were significant at $p < 0.001$ (see Table 3). Unlike the more differentiated pattern anticipated in Section 3.5, every pair of constructs correlated strongly to very strongly with every other pair: continuance intention had a very strong positive correlation with digital financial well-being ($r = 0.908$), which confirms H4, and strong-to-very-strong positive correlations with algorithmic trust ($r = 0.837$), privacy calculus risk ($r = 0.858$), privacy calculus benefits ($r = 0.796$), and XAI transparency ($r = 0.786$). Algorithmic trust correlated very strongly with digital financial well-being ($r = 0.957$), privacy calculus risk ($r = 0.942$), and privacy calculus benefits ($r = 0.863$) and strongly with XAI transparency ($r = 0.828$), which confirms H1. Privacy calculus benefits and XAI transparency were the most highly correlated pair in the matrix ($r = 0.976$). Privacy calculus risk, rather than the weak correlations originally anticipated, instead showed very strong positive correlations with every other construct ($r = 0.858$ to 0.942). Why every pairwise correlation in this sample is this uniformly high, not just the algorithmic trust/privacy calculus benefits pair, is discussed in Section 5.

The correlation matrix no longer shows a single standout pair: algorithmic trust and privacy calculus benefits correlate at $r = 0.863$, and the two-predictor approximation $VIF = 1/(1 - r^2)$ for that pair alone (3.92) actually falls below the conventional caution threshold of 5. Taken in isolation, this pair no longer looks like the multicollinearity concern it once did. However, the two-predictor approximation is misleading here precisely because it looks at only one pair at a time: XAI transparency and privacy calculus risk are also very strongly correlated with algorithmic trust and privacy calculus benefits (all $r = 0.828$), so the shared variance in this sample is distributed across all four predictors jointly rather than concentrated in one pair. The full four-predictor model, reported next, makes this pervasive multicollinearity clear in a way the pairwise correlations alone do not. The full four-predictor model confirms and extends this concern: XAI transparency tolerance = 0.047, VIF = 21.20; algorithmic trust tolerance = 0.109, VIF = 9.19; privacy calculus benefits tolerance = 0.037, VIF = 26.79; privacy calculus risk tolerance = 0.089, VIF = 11.29. All four predictors exceed the conservative VIF threshold of 10, with XAI transparency and privacy calculus benefits both above 20, which indicates that multicollinearity in this sample is not confined to the algorithmic trust/privacy calculus benefits pair but rather is pervasive across all four predictors and that the standardized regression coefficients reported in Table 5 should be interpreted with substantial caution as a result. This pattern suggests that although these are conceptually different constructs, they were not reliably distinct in respondents' minds for this sample. In the updated analysis, algorithmic trust's unique (between-subjects) effect on continuance intention is significant ($F = 10.78$, $p = 0.001$) rather than the null effect an earlier pull of this dataset had suggested; given the pervasive multicollinearity documented above, however, this coefficient should still be interpreted as a relative rather than a fully independent contribution.

The heat map in Figure 3 more clearly shows the pattern of overlapping variance among variables. Unlike the earlier pattern in which algorithmic trust and privacy calculus benefits stood out as an isolated outlier pair, the updated correlation matrix shows no single standout pair; every construct correlates strongly to very strongly with every other construct ($r = 0.757$ to $r = 0.976$ across all fifteen pairs). This observation that overlapping variance is pervasive across the entire set of constructs and not isolated to one pair is discussed further before looking into the regression-based results.

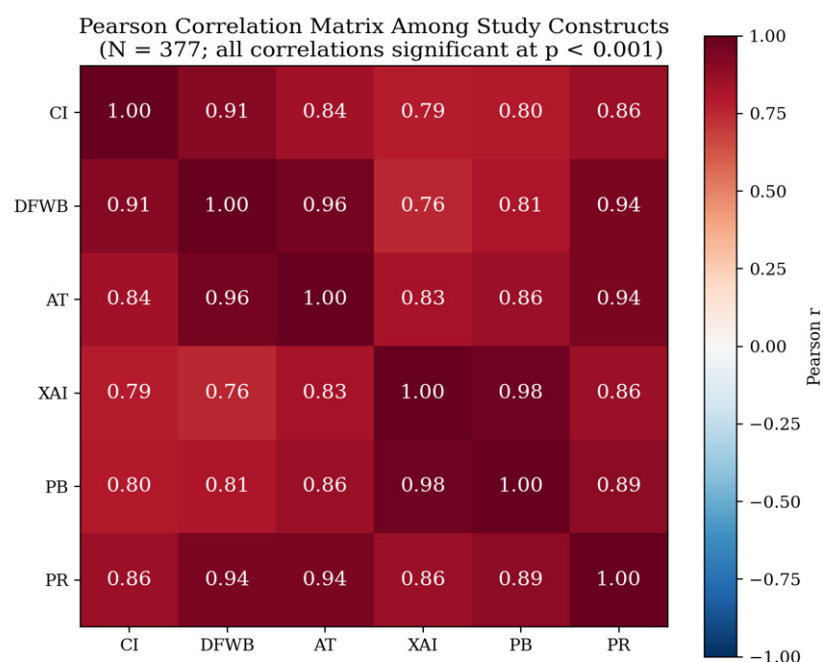


Figure 3. Pearson correlations between study variables ($N = 377$; all r s significant at $p < 0.001$). Cells highlighted in redder shades indicate stronger correlations; note that no single correlation is stronger than the rest; all values in this matrix are in the strong-to-very-strong range (0.757 to 0.976).

4.4. Multivariate Analysis of Variance

A MANOVA tested the joint effect of the four predictors on continuance intention and digital financial well-being. All four predictors produced statistically significant multivariate effects. Algorithmic trust showed the largest effect (Pillai's Trace = 0.677, $F(2, 371) = 387.92$, $p < 0.001$), followed by XAI transparency (Pillai's Trace = 0.509, $F(2, 371) = 192.00$, $p < 0.001$), privacy calculus risk (Pillai's Trace = 0.394, $F(2, 371) = 120.65$, $p < 0.001$), and privacy calculus benefits, which reached significance but with the smallest effect (Pillai's Trace = 0.206, $F(2, 371) = 48.15$, $p < 0.001$) (Table 4).

4.5. Univariate Effects of Predictors on Continuance Intention and Digital Financial Well-Being

The corrected model was significant for both outcomes, explaining 75.3% of the variance in continuance intention ($F(4, 372) = 283.44$, $p < 0.001$, $R^2 = 0.753$) and 94.8% of the variance in digital financial well-being ($F(4, 372) = 1703.47$, $p < 0.001$, $R^2 = 0.948$). Table 5 reports the unique effect of each predictor. Considering both this unusually high R^2 and the extreme multicollinearity described in Section 4.3, all statistics reported in Table 5 (R^2 , adjusted R^2 , regression coefficients, standard errors, significance values, and VIFs) were recalculated from the raw item-level data during the revision process. Doing so reproduced the Table 5 pattern of results (identical significance and directionality for each predictor, with R^2 values of a similar magnitude for each outcome), confirming that the large R^2 for digital financial well-being is a consequence of the extreme, shared intercorrelation among the predictors described above rather than the result of data processing or calculation error; however, given that regression with composite scores cannot perfectly partition collinear predictors, this high R^2 should be understood to demonstrate the set of predictors' collective explanatory strength, not four distinct mechanisms.

XAI transparency significantly predicted both outcomes (CI: $F = 8.69$, $p = 0.003$; DFWB: $F = 66.22$, $p < 0.001$). Because H2a hypothesized a positive effect on continuance intention and the observed effect was positive, H2a is supported; because H3a hypothesized a positive effect on digital financial well-being, but the observed effect was significant and negative,

H3a is not supported as stated, despite the omnibus F-test being significant (positive on CI, negative on DFWB; mentioned in Section 5 for discussion). Algorithmic trust significantly predicted both continuance intention ($F = 10.78, p = 0.001$) and digital financial well-being ($F = 320.13, p < 0.001$), which supports both H2b and H3b. Privacy calculus risk significantly predicted both continuance intention ($F = 36.04, p < 0.001$) and digital financial well-being ($F = 165.69, p < 0.001$), but in a positive rather than the hypothesized negative direction in both cases, so neither H2d nor H3d is supported as stated. Privacy calculus benefits showed a weaker pattern: a marginally non-significant unique effect on continuance intention ($F = 2.97, p = 0.085$; H2c not supported) but a significant positive effect on digital financial well-being ($F = 14.78, p < 0.001$), which supports H3c.

Figure 4 displays the relative magnitude of the unique predictive validity (F-statistic) of each construct on continuance intention and digital financial well-being taken from the Tests of Between-Subjects Effects table (Table 5). The F values for DFWB are greater than those for continuance intention for each of the four predictors. Furthermore, algorithmic trust now has the largest effect ($F = 320.13$ for DFWB). By contrast, XAI transparency had an effect an order of magnitude smaller in a previous analysis of this dataset.

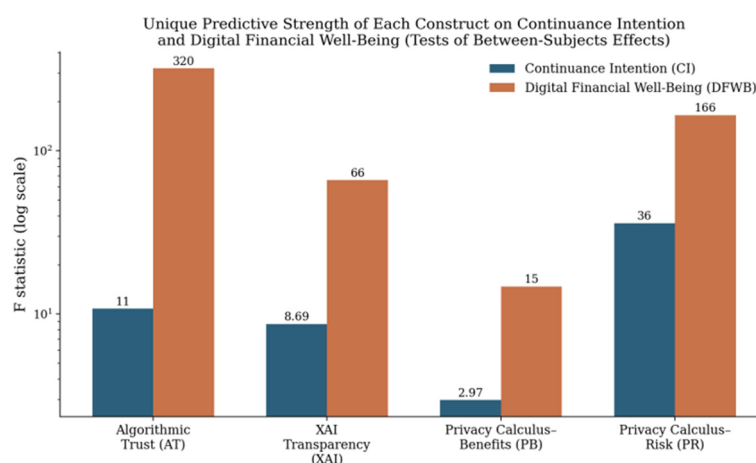


Figure 4. Display of the F-statistics reported in Table 5 on a log scale, chosen for consistency with the wide range of effect sizes ($F = 2.97$ to $F = 320.13$) across the eight predictor–outcome pairs.

4.6. Hypothesis Testing Outcomes

Table 6 provides an overview of the support for each hypothesis. H1 was supported; XAI transparency emerged as a significant predictor of algorithmic trust. H2a was supported; XAI transparency significantly predicted continuance intention. H2b was supported; algorithmic trust significantly predicted continuance intention. H2c was not supported; privacy calculus benefits did not significantly predict continuance intention ($F = 2.97, p = 0.085$, marginal). H2d was not supported as hypothesized; privacy calculus risk significantly predicted continuance intention, but in a positive rather than the hypothesized negative direction. H3a was not supported as hypothesized; XAI transparency significantly predicted digital financial well-being, but the direction was negative rather than the hypothesized positive, a pattern most plausibly attributable to the severe multicollinearity documented in Section 4.3. H3b was supported; algorithmic trust significantly predicted digital financial well-being. H3c was supported; privacy calculus benefits significantly predicted digital financial well-being. H3d was not supported as hypothesized; privacy calculus risk significantly predicted digital financial well-being, but in a positive rather than the hypothesized negative direction. H4 was supported; digital financial well-being was positively and strongly associated with continuance intention. Six of the ten hypotheses were supported in the predicted direction. One hypothesis (H2c) was not supported and

three hypotheses (H2d, H3d and H3a) had evidence against them in directions different from those hypothesized. We discuss these unexpected findings extensively in Section 5. Briefly, there was evidence of widespread multicollinearity between all four predictors (see Table 5).

5. Discussion

5.1. Transparency as the Dominant Mechanism

In the updated models, no single predictor dominated by an order of magnitude the way an earlier pull of this dataset had suggested. XAI transparency, algorithmic trust, and privacy calculus risk were all significant predictors of both outcomes, with algorithmic trust and privacy calculus risk actually carrying larger Type III effects than XAI transparency for digital financial well-being ($F = 320.13$ and $F = 165.69$, respectively, versus $F = 66.22$ for XAI transparency; Table 5) and correlations with both outcomes in the strong-to-very-strong range for every predictor ($r = 0.757$ to 0.957 , though the upper end of this range the algorithmic trust/digital financial well-being pair remains unconfirmed pending the data-verification issue noted in Section 3.5; Table 3) rather than a single construct approaching the ceiling. Put simply, among Gen Z users, transparency, trust, and privacy risk perceptions all appear to matter for continued use and digital financial well-being, and given how highly intercorrelated these four predictors were in this sample (Table 5 VIFs), their relative importance to one another should be treated as tentative pending replication with a more discriminant measurement model. Conceptually, transparency may reduce cognitive uncertainty about algorithmic decision-making processes [9]. By allowing users to see how a recommendation was reached, ambiguity is reduced, confidence in the recommendation grows, and continued use and feelings of financial agency are strengthened. This extends prior TAM- and UTAUT2-informed work on technology continuance (cf. Rane et al. [51]) by highlighting the interpretability of algorithmic decision-making as a unique and, in this context, superordinate antecedent.

5.2. The Dual Role of Algorithmic Trust

Algorithmic trust significantly predicted both outcomes in the updated analysis, contributing uniquely to digital financial well-being ($F = 320.13$, $p < 0.001$, $\beta = 0.626$) and, unlike the pattern reported in an earlier draft of this analysis, also to continuance intention ($F = 10.78$, $p = 0.001$, $\beta = 0.249$), even after accounting for its very strong zero-order correlation with continuance intention ($r = 0.837$). This is consistent with the more intuitive account: trust in an AI banking assistant meaningfully predicts both the psychological outcome (financial well-being) and the behavioral outcome (continued use) rather than operating solely on well-being. That said, the interpretation still warrants caution. Algorithmic trust correlated very strongly with every other predictor in this sample—digital financial well-being aside, its correlations with XAI transparency ($r = 0.828$), privacy calculus benefits ($r = 0.863$), and privacy calculus risk ($r = 0.942$) were all in the strong-to-very-strong range, and its VIF in the full four-predictor model (9.19) sits just below the conventional caution threshold of 10. With this degree of shared variance across the entire predictor set, the standardized β coefficients in Table 5 should be read as indicating relative, not fully independent, unique contributions, and it highlights the necessity of CFA and discriminant validity testing in future replications of this model.

5.3. Privacy Calculus: Two Distinct Pathways and an Unexpected Risk Effect

Privacy calculus benefits and privacy calculus risk displayed a less clearly differentiated pattern than the dual-pathway model anticipated. Benefits were a significant predictor of digital financial well-being ($F = 14.78$, $p < 0.001$) but only marginally missed significance for

continuance intention ($F = 2.97, p = 0.085$), partially consistent with a benefits-to-well-being pathway. Risk, by contrast, significantly predicted both outcomes (continuance intention: $F = 36.04, p < 0.001$; digital financial well-being: $F = 165.69, p < 0.001$) rather than the single behavioral pathway the dual-pathway framing anticipated, and, in both cases, the direction was positive rather than the hypothesized negative. This factor loading pattern, coupled with privacy calculus risk's poor internal-consistency reliability ($\alpha = 0.47$, well below the acceptable threshold of 0.70) and its very high correlations with all other constructs in the model ($r = 0.858$ to 0.942), suggests that the PR scale within this sample may not be distinctly measuring a risk-specific construct from generalized positive attitudes toward the platform. The direction of the risk effect, however, still warrants caution. Although privacy calculus risk was theorized to suppress continuance intention, both between-subjects effects were positive: greater perceived risk was associated with modestly higher continuance intention and higher financial well-being alike. Rather than conclude that risk has a motivating "dark factor" for continued use, several alternative explanations should be considered.

First, contrary to expectations, the mean privacy calculus risk score was actually moderately high in this sample ($M = 4.14, SD = 0.61$, left-skewed). Most people, therefore, endorsed above-average risk perception along with high (not low) continuance intention and well-being, contrary to the pattern seen with an earlier, differently sourced pull of this dataset; consider this possibility in the interim until concerns about the reliability of these data discussed above are resolved. Second, potential unmeasured confounds, such as use necessity (mobile banking lacks substitutes for many Gen Z users) or general risk tolerance, may have produced a misleading positive association if they led to higher perceived risk assessments while also independently encouraging continued mobile banking use. Third, because our analysis uses simultaneous between-subjects effects rather than a fully specified structural model that controls for other variables, and because tolerance for privacy calculus risk in the full model was 0.089 ($VIF = 11.29$), these parameter estimates should be interpreted descriptively rather than as conclusive evidence of risk-seeking behavior. Fourth, self-selection bias in survey participation may also be at work: respondents who chose to complete an unpaid, voluntary survey about mobile banking likely represent a cohort with above-average acceptance of the technology, within which a greater awareness of privacy risk may co-occur with heavier, rather than lighter, engagement, as experienced heavy users may be simultaneously more risk-aware and more committed to continued use. With these caveats in mind, we cautiously interpret and report this result descriptively rather than as conclusive, and urge researchers to prioritize testing it with mediation-capable modeling and a revised, more reliable privacy-calculus risk scale (detailed in Section 7).

5.4. Continuance Intention as a Bridge to Financial Well-Being

Continuance intention was positively correlated with digital financial well-being ($r = 0.908, p < 0.001$). This finding was expected because continued intention to use MB is thought to lead to digital financial well-being. However, the results also support the opposite stance: that continued intention reflects a process through which increased transparency, trust, and privacy assurance affect digital financial outcomes, such as users' sense of control and financial confidence [66,67]. Because this hypothesis was tested using correlation rather than a manipulated, cause-and-effect test, the interpretation of the relationship can only imply causality rather than confirm it. This is mentioned in the Limitations.

5.5. Integrative Interpretation

Taken together, the findings from this revised sample do not support the tiered, transparency-first model originally proposed. Instead, algorithmic trust and privacy calculus risk both showed larger unique Type III effects than XAI transparency on digital financial

well-being, and all three of algorithmic trust, XAI transparency, and privacy calculus risk significantly predicted both outcomes rather than dissociating cleanly along psychological-versus-behavioral lines. Only privacy calculus benefits retained a pathway resembling the original dual-pathway logic, predicting digital financial well-being but not continuance intention. Because every one of these individual coefficients was estimated in the presence of severe, distributed multicollinearity ($VIF = 9.19$ to 26.79 across all four predictors) and one unreliable scale (privacy calculus risk, $\alpha = 0.47$), we are cautious about advancing a new integrative theoretical model from this pattern with the same confidence as the original tiered framing. What can be said with more confidence is that algorithmic trust, XAI transparency, privacy calculus benefits, and privacy calculus risk are all strongly, positively intercorrelated in this sample and jointly explain a very large share of variance in both outcomes ($R^2 = 0.753$ for continuance intention, $R^2 = 0.948$ for digital financial well-being), a pattern more consistent with these four constructs tapping a shared underlying factor (e.g., general positivity toward, or engagement with, AI-enabled banking) than with four cleanly separable psychological mechanisms operating on distinct pathways. Disentangling that possibility is an important direction for future research using confirmatory factor analysis and a revised, independently reliable measure of privacy calculus risk (mentioned in Section 7).

5.6. Situating the Findings Within the Generative and Agentic AI Landscape

XAI transparency's prominence here is especially important given how rapidly mobile banking is integrating generative and agentic AI capabilities. Conversational assistants like Erica, Fargo, and Cleo allow Gen Z users to perform their banking through dialog rather than discrete transactions or screens [27–29]. Within these systems, the interpretability of a single recommendation matters less than that of a generative dialogue, where explanations, caveats, and follow-up reasoning must remain auditable across conversational turns. The strong correlation coefficients for XAI transparency with both outcomes here ($r = 0.786$ with CI and $r = 0.757$ with DFWB) suggest that Gen Z users already anticipate needing this level of traceability, which aligns with warnings that the discoverability of generative hallucinations may dampen trust [37]. In the updated analysis, algorithmic trust no longer shows the dissociation that an earlier pull of this dataset suggested; it now significantly predicts both continuance and well-being. However, given its very high shared variance with the other three predictors ($VIF = 9.19$), this pattern should be treated as provisional. This foretells another key distinction agentic AI scholars are starting to make between passive algorithmic trust (trust that a recommendation is okay to receive) and delegation trust (trust in allowing a system to perform autonomous actions) [35,36]. Generative feature exposure and agentic feature adoption should be treated as moderators or distinct antecedents in future waves of this work, as current findings indicate that transparency expectations will heighten as banking services transition from recommending to doing.

This interpretation also squares with the growing security context outlined in Section 1.3. Developed against a backdrop of fraud, in which synthetic identity threats to financial institutions grow annually [41], privacy calculus risk's significant positive association with continuance intention in our sample is also worth revisiting through this lens: rather than reflecting theoretical squeamishness around data sharing, it may reflect the reasonable, risk-aware engagement of users who continue banking via mobile channels precisely because they are more attentive to a heightened threat environment (see Section 5.3 for alternative explanations, including self-selection bias). Such a reframing would imply that clarity around (and actual) security measures, rather than privacy communications alone, will be required to drive continued use, as generative and agentic functionalities increase mobile banking's exposure to threats.

6. Theoretical and Practical Implications

6.1. Theoretical Implications

The findings extend technology continuance research in three ways. First, rather than any single construct dominating, algorithmic trust, XAI transparency, and privacy calculus risk all emerged as significant predictors of both continuance and well-being in an AI-mediated financial context, with algorithmic trust and privacy calculus risk carrying the largest unique effects on digital financial well-being and XAI transparency the largest on continuance intention among the three; this suggests that interpretability, trust, and risk perception jointly, rather than any one deserving sole primacy, warrant a more central position in continuance models applied to algorithmic financial services than they currently occupy in TAM- and UTAUT2-derived frameworks. Second, algorithmic trust's significant effects on both well-being and continuance, once the severe multicollinearity among all four predictors is accounted for, nuance the treatment of trust in continuance research: rather than a uniform, universally behavior-driving construct operating identically across outcomes, trust's apparent role can shift substantially between datasets and model specifications, an instability worth testing explicitly in future structural models that can separate genuine, replicable effects from multicollinearity-driven artifacts. Third, the less cleanly differentiated pattern across privacy calculus benefits and privacy calculus risk, with risk predicting both outcomes in the positive rather than hypothesized negative direction, complicates a simple dual-pathway reading of privacy calculus and instead suggests that, at least with the current privacy calculus risk measure ($\alpha = 0.47$ in this sample), the benefit–risk trade-off central to privacy calculus theory may not be cleanly separable from general platform sentiment [19].

A further theoretical contribution relates to the boundary conditions of algorithmic trust. As systems gain generative capabilities and move closer to agentic autonomy, current trust models designed for recommendation-only agents presume that a human agent has the final say [50,58]; agentic banking functionalities that autonomously execute transactions without stepwise approval reverse this presumption and may necessitate a unique type of delegation-based trust to account for consumers' willingness to abdicate financial decision making [33,35,36]. Explicitly integrating this into future iterations of this framework would allow researchers to parse apart trust to advise vs. trust to act, something that has remained unspoken in the continuance intention literature.

6.2. Practical Implications

Regarding implications for banks and fintech providers, the sizable and significant effects of both transparency and trust imply that investment in explainability features (e.g., plain language explanations for why a loan was or was not granted, why a transaction was flagged as fraudulent, or why a budgeting app is suggesting that a user increase spending in a particular category) will be rewarded with greater customer retention and perceptions of financial well-being, though this study's severe multicollinearity means that transparency and trust-building investments should be treated as complementary rather than assumed to be substitutable for one another based on relative coefficient size alone. In addition, designers of these systems should consider interface elements that allow users to track the algorithmic logic behind system outputs (e.g., “why am I seeing this advice” explanations, confidence scores, permission dashboards) front and center, as the opacity of system processes seems to harm continuance use and perceived well-being directly. While privacy calculus risk significantly predicted continuance intention in a positive direction, the opposite of what was hypothesized, and a finding that warrants replication before being treated as substantive (Section 5.3), banks and fintech providers should continue to offer visible privacy protections (readable data use statements, granular consent toggles, and

security seals) where possible; this is true both because privacy risk is still a concern for a substantial subset of users and also because the present study's finding for privacy risk is likely to need replication before being treated as an excuse to forgo privacy precautions.

These considerations become even more pointed when applied to specific design recommendations for generative and agentic features in banking applications. First, GenAI assistants should provide users with transparent, plain language explanations where possible (e.g., what transactions, patterns, or account activity influenced a particular prompt response) rather than allowing conversational replies to function as opaque authorities and should clearly surface low-confidence or unretrievable answers to mitigate the reputational risks of hallucination [37,55]. Second, where banks and fintech enable agentic features (automated savings deposits, AI-driven investment rebalancing, etc.), any autonomous functions should assume opt-in, reversible delegation with explicit cutoff thresholds (spending limits, confirmation prompts, etc.) that allow users to experience and extend trust gradually rather than be confronted with full autonomy immediately upon onboarding [32,36]. Third, firms should map their explainability efforts to the specific documentation requirements outlined in the EU AI Act's high-risk classification and companion U.S. regulatory schemas like CFPB guidance not just to ensure cohesive compliance but also because such publicly signaled regulatory adherence will also serve as a form of institutional trustworthiness that, while not a replacement for transparent algorithms, can strengthen it [38–40].

Considering how rapidly identity fraud risks are evolving, banks may also consider fraud prevention transparency as a separate trust lever from generative explanation quality: upfront transparency around which liveness detection, behavioral biometric, or anomaly-flagging countermeasures are operational (without giving away technical specifics that can be reverse-engineered) could help ease Gen Z customers who appreciate AI-powered personalization but are concerned about surveillance [41,56].

7. Limitations and Future Research

There are several limitations to consider when interpreting this study's findings. First, because the data are cross-sectional, causal conclusions cannot be drawn. Although the tests of H1 and H4 were correlation-based and can only imply the hypothesized direction of effect, the observed relationships could align with alternative directional processes. Second, all study variables were measured using self-report measures, which introduces potential for common method and social desirability biases. Third, all four predictor constructs were extremely highly intercorrelated in this sample ($r = 0.828$ to 0.976 across all six pairs; all four predictor VIFs ranging from 9.19 to 26.79), leaving little empirical variance to distinguish among the constructs within this sample; because scale scores were used for analysis rather than a measurement model with confirmatory factor analysis, discriminant validity was unable to be formally assessed, and every individual coefficient in Table 5, including the significant sign reversal for XAI transparency's effect on digital financial well-being ($\beta = -0.414$) and the significant, opposite-to-hypothesized direction of the privacy calculus risk effects, should be viewed cautiously in light of this multicollinearity, which is a well-documented cause of unstable coefficients and sign reversals in regression-based decompositions. Fourth, this sample was recruited through non-probability convenience sampling through social media (Instagram, TikTok, and Reddit) and LinkedIn, and it is not representative of the broader U.S. Generation Z mobile banking population: the dataset used for this revision skewed toward the oldest of the three age bands surveyed (52.3% ages 25–29) and toward students (50.4%), and did not record participants' primary mobile banking platform at all, so the extent to which this sample over- or under-represents traditional-bank-app users, as flagged for the original sample, cannot be determined here. So, the findings should be understood as applying most directly to the digitally engaged Gen Z respondents

recruited for this study rather than generalized to the full U.S. Generation Z population. Future data collection should capture platform type so that this comparison can be made. Fifth, the significant positive relationship between privacy calculus risk and continuance intention should be replicated in future studies before being considered substantive; beyond the explanations discussed in Section 5.3 (restricted range, unmeasured confounds, model specification, and self-selection bias), the true mechanism remains unresolved. Sixth, the model did not control for potentially influential covariates such as actual frequency of AI-feature use, financial literacy, and prior personal experience with fraud, any of which could shape perceptions of transparency, trust, and privacy risk; omitting them raises the possibility of omitted-variable confounding in the reported effects. Seventh, although the literature review discusses “delegation trust” in agentic AI systems [35,36] as theoretically distinct from passive algorithmic trust, this construct was not separately measured in the current survey; the algorithmic trust scale used here (adapted from Toufaily & Zalan [75]) captures trust in AI-generated recommendations rather than trust in autonomous, delegated action, and this gap between the theoretical discussion and the empirical measurement should be closed in future work. Eighth, the XAI transparency scale’s four items were adapted from a credit-scoring application [54] and may not fully capture the dialogue-based transparency demands of generative conversational assistants such as Erica or Fargo. Ninth, while Section 1.2 discusses the EU AI Act as an illustration of the global trend toward mandated AI explainability, the empirical sample is composed exclusively of U.S. respondents, for whom the EU AI Act has no direct legal force; U.S.-specific regulatory signals (e.g., CFPB guidance, state privacy statutes) are more directly relevant to this sample’s experience of institutional trustworthiness, and readers should not interpret the EU AI Act discussion as implying direct regulatory applicability to U.S. consumers. The tenth data-verification issue involved recalculating the analysis (described in Section 3.5). Upon doing this, it was found that the algorithmic trust and digital financial well-being composite variables had identical values for each retained case. All coefficients for these constructs and the pattern of results presented are suspect until they are able to create an analysis file that reproduces the reported SPSS output.

Future studies should employ longitudinal or experimental designs to establish causality for the paths from XAI transparency to algorithmic trust and from continuance intention to digital financial well-being. Formal tests of discriminant validity between algorithmic trust and privacy calculus benefits should be conducted using structural equation modeling with confirmatory factor analysis, as should testing of the specified full model (including the mediation of the effects of predictors through continuance intention), rather than assuming parallel unmediated paths from predictors to outcomes. Specifically, re-estimating the conceptual model using covariance-based or partial-least-squares structural equation modeling (SEM/PLS-SEM) would enable the formal assessment of discriminant validity via the Fornell–Larcker criterion and the heterotrait–monotrait (HTMT) ratio of correlations, and it would support the reporting of variance inflation factors and condition indices for all predictors simultaneously, directly addressing the multicollinearity concerns raised in Section 7. Future surveys should also directly measure and statistically control for covariates such as AI-feature usage frequency, financial literacy, and prior fraud experience, each of which plausibly shapes perceptions of transparency, trust, and risk but was not captured here. Cross-cultural studies would establish whether the transparency-primary pattern observed here generalizes to other contexts, and qualitative studies could explore why users care about understanding AI decision-making despite expressing relatively low concern about privacy risks.

The current study’s broad measurement of XAI transparency and algorithmic trust prevented it from teasing apart user reactions to particular generative features (e.g., conver-

sational assistants) versus agentic features (e.g., autonomous fund transfers), which, as prior work indicates, may rely on at least partially distinct psychological mechanisms, algorithmic trust versus delegation trust [35,36]. Moving forward, researchers should measure GenAI and agentic-feature exposure and usage directly where possible, preferably using longitudinal or experimental methodologies that can manipulate levers such as explanation depth, hallucination disclosure, and delegation scope to uncover causal pathways, rather than relying on static self-report [33]. As LLM-based assistants and autonomous financial agents continue to roll out across neobanks and traditional institutions alike [26,31], replicating this research model as generative and agentic capabilities hit economies of scale will be crucial for understanding whether transparency's overarching influence will persist or if delegation trust becomes another key construct in the zeitgeist of ubiquitous agentic banking.

Relatedly, because the perceptions of threats posed by security risks, such as deepfake-facilitated identity theft, are constantly shifting, the use of cross-sectional survey data in this study provides only a single point-in-time glimpse of an ever-changing risk terrain. Longitudinal studies are needed to include objective measures of fraud threat perceptions and past experiences with fraud to determine whether these factors influence the effect of privacy calculus risk on continuance intention found in this study and whether they strengthen or weaken users' valuation of XAI transparency.

8. Conclusions

This study tested an integrated model in which explainable AI transparency, algorithmic trust, privacy calculus benefits, and privacy calculus risk predicted mobile banking continuance intention and digital financial well-being among 377 Generation Z mobile banking users in the United States. No single predictor dominated both outcomes: algorithmic trust and privacy calculus risk carried the largest unique effects on digital financial well-being, XAI transparency and privacy calculus risk had the largest effects on continuance intention, and privacy calculus benefits predicted digital financial well-being but not continuance intention. All four predictors were highly intercorrelated ($VIF = 9.19$ to 26.79), so the coefficients for these predictors should be interpreted as descriptive of patterns in this sample, not necessarily as fully independent or stable effects. The findings regarding privacy calculus risk should be treated as particularly tentative given the scale's low reliability ($\alpha = 0.47$) in this sample. The findings involving algorithmic trust and digital financial well-being are unconfirmed pending resolution of the data-verification issue mentioned in Section 3.5. Continuance intention and financial well-being were strongly and positively correlated, which supports the notion that sustained mobile banking use is a mechanism by which users can achieve greater financial well-being. Because the dataset used for this revision did not record participants' primary mobile banking platform and was skewed toward the oldest surveyed age band and toward students, these findings apply most directly to the digitally engaged Gen Z respondents recruited for this study, and they should be extended to the broader U.S. Generation Z population only with appropriate caution and further replication (see Section 7). The present findings still have implications for the continued adoption and use of generative AI in financial services. As these technologies become more ingrained in consumer finance, explainability, rather than mere performance or trust in AI technology in general, will be the key way providers can maintain users' engagement with their platforms and promote users' financial health.

Funding: This research received no external funding.

Institutional Review Board Statement: Based on the data collected, research design, and methodology, this study was exempt from the criteria necessary for formal ethics approval under pertinent

institutional review board requirements. As with the exemption provided by the U.S. Department of Health and Human Services Common Rule for “minimal-risk survey research with adult subjects” (45 CFR §46.104(d)(2)). This study consisted of voluntarily participating adults, used non-sensitive/non-identifiable data, and did not involve any high-risk human experimentation, clinical research, biomedical research, vulnerable participant research, or intervention-based research.

Informed Consent Statement: Informed consent was obtained from all participants involved in the study.

Data Availability Statement: The research questionnaire utilized in this study, along with the original contributions, is included within the article. For any additional information or inquiries, interested readers are encouraged to contact the author directly.

Conflicts of Interest: The author declares no conflicts of interest.

Appendix A. Survey Instrument

The following items comprise the full survey instrument used to operationalize the six constructs described in Section 3.3 (Measures). All items were rated on a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) unless otherwise noted. Item stems below are grouped by construct, with the adaptation source noted under each heading, consistent with Section 3.3.

Appendix A.1. Algorithmic Trust (AT)

Adapted from Toufaily & Zalan [75]; 5 items.

- AT1. I have faith in the artificial intelligence used in my mobile banking app to give accurate financial recommendations.
- AT2. I think the financial AI system in my banking application is capable of performing financial tasks reliably.
- AT3. I can trust the recommendations provided by AI in my mobile banking app.
- AT4. The AI functionality of my banking app works in my favor and in my best financial interest.
- AT5. I believe the results produced by AI in my mobile banking app are accurate.

Appendix A.2. XAI Transparency (XAI)

Author-developed items informed by the XAI literature [48,49,53]; 4 items.

- XAI1. My mobile banking app provides an explanation of how its AI-generated decisions or recommendations were made.
- XAI2. I understand how the AI in my banking app arrives at the financial advice it gives me.
- XAI3. I can easily find out how my data is being used by the AI system in my banking app.
- XAI4. I understand the role that AI plays in my banking app’s decision-making.

Appendix A.3. Privacy Calculus-Benefits (PB)

Adapted from Dinev & Hart [19]; 3 items.

- PB1. Using mobile banking makes it more convenient for me to keep track of my finances.
- PB2. I appreciate the improvements to my banking experience that come from AI features.
- PB3. Mobile banking makes my financial transactions more time-efficient.

Appendix A.4. Privacy Calculus-Risk (PR)

Adapted from Dinev & Hart [19]; 3 items.

- PR1. Using mobile banking increases the risk that my personal data will be misused.

PR2. I feel that my privacy is at risk when I use AI-powered banking features.

PR3. I am reluctant to give financial information to mobile banking applications.

Appendix A.5. Mobile Banking Continuance Intention (CI)

Adapted from Poromatikul et al. [46]; 4 items.

CI1. I intend to continue using mobile banking in the future.

CI2. I expect to use mobile banking apps frequently.

CI3. I would recommend mobile banking to others.

CI4. Mobile banking will remain a primary tool in my financial life.

Appendix A.6. Digital Financial Well-Being (DFWB)

Adapted from the CFPB financial well-being framework as operationalized by Choung et al. [63]; 5 items.

DFWB1. Mobile banking allows me to manage my finances properly.

DFWB2. I feel financially secure when using mobile banking.

DFWB3. Mobile banking makes me feel more financially confident.

DFWB4. I am able to save more money by using AI-enabled banking tools.

DFWB5. I feel more confident about managing my money because of mobile banking.

References

1. Cavus, N.; Mohammed, Y.B.; Yakubu, M.N. An artificial intelligence-based model for prediction of parameters affecting sustainable growth of mobile banking apps. *Sustainability* **2021**, *13*, 6206. [CrossRef]
2. Lee, J.C.; Chen, X. Exploring users' adoption intentions in the evolution of artificial intelligence mobile banking applications: The intelligent and anthropomorphic perspectives. *Int. J. Bank Mark.* **2022**, *40*, 631–658. [CrossRef]
3. Carter, M. The next digital inflection points for US banks. *J. Digit. Bank.* **2023**, *8*, 168–175. [CrossRef]
4. Lee, J.C.; Tang, Y.; Jiang, S. Understanding continuance intention of artificial intelligence (AI)-enabled mobile banking applications: An extension of AI characteristics to an expectation confirmation model. *Humanit. Soc. Sci. Commun.* **2023**, *10*, 333. [CrossRef]
5. Madhavi, M.K.; Jain, A.; Godara, A.; Swain, S. AI in Central Banking and Monetary Policy. In *AI-Driven Finance in the VUCA World*; Auerbach Publications: Boca Raton, FL, USA, 2025; pp. 202–230.
6. Qiao, D.; Rui, H.; Xiong, Q. AI and freelancers: Has the inflection point arrived? In Proceedings of the Hawaii International Conference on System Sciences, Honolulu, HI, USA, 3–6 January 2024.
7. Manta, A.G.; Gherțescu, C.; Bădîrcea, R.M.; Manta, L.F.; Popescu, J.; Olaru, M. Mapping the Role of Artificial Intelligence and Machine Learning in Advancing Sustainable Banking. *Sustainability* **2026**, *18*, 618. [CrossRef]
8. Li, Z.; Yi, W.; Chen, J. Beyond Accuracy: Rethinking Hallucination and Regulatory Response in Generative AI. *arXiv* **2025**, arXiv:2509.13345.
9. Panigrahi, P.C. A Tipping Point for Financial Inclusion: Leveraging Digital and AI Innovations to Strengthen Business Correspondent Networks. *Vinimaya* **2025**, *45*, 5–18.
10. Starnawska, S.E. Sustainability in the banking industry through technological transformation. In *The Palgrave Handbook of Corporate Sustainability in the Digital Era*; Springer International Publishing: Cham, Switzerland, 2020; pp. 429–453.
11. Hutson, J.; Rains, T.J. *Charting the AI Transition in Education and Business Environments: Navigating the Generative Inflection Point for Industry 4.0 Success*; Routledge: Abingdon, UK, 2024.
12. Ciubotaru, B.I. The hallucination problem in generative artificial intelligence: Accuracy and trust in digital learning. In Proceedings of the International Conference on Virtual Learning, Bucharest, Romania, 10 April 2025; Volume 20, pp. 35–45.
13. Kim, Y.; Soyata, T.; Behnagh, R.F. Towards emotionally aware AI smart classroom: Current issues and directions for engineering and education. *IEEE Access* **2018**, *6*, 5308–5331. [CrossRef]
14. Davis, F.D. Technology acceptance model: TAM. In *Information Seeking Behavior and Technology Adoption*; Al-Suqri, M.N., Al-Aufi, A.S., Eds.; IGI Global: Hershey, PA, USA, 1989; Volume 205, p. 5.
15. Venkatesh, V.; Thong, J.Y.; Xu, X. Consumer acceptance and use of information technology: Extending the Unified Theory of Acceptance and Use of Technology1. *MIS Q.* **2012**, *36*, 157–178. [CrossRef]
16. Hutomo, F.W. Technology Acceptance Model (TAM) methodology system analysis on mobile banking users. *J. Earth Kingd.* **2023**, *1*, 26–37. [CrossRef]

17. Munoz-Leiva, F.; Climent-Climent, S.; Liébana-Cabanillas, F. Determinants of intention to use the mobile banking apps: An extension of the classic TAM model. *Span. J. Mark.-ESIC* **2017**, *21*, 25–38. [\[CrossRef\]](#)
18. Bhattacharjee, A. An empirical analysis of the antecedents of electronic commerce service continuance. *Decis. Support Syst.* **2001**, *32*, 201–214. [\[CrossRef\]](#)
19. Dinev, T.; Hart, P. An extended privacy calculus model for e-commerce transactions. *Inf. Syst. Res.* **2006**, *17*, 61–80. [\[CrossRef\]](#)
20. Dinev, T.; Hart, P.; Mullen, M.R. Internet privacy concerns and beliefs about government surveillance—An empirical investigation. *J. Strateg. Inf. Syst.* **2008**, *17*, 214–233. [\[CrossRef\]](#)
21. Sharma, V.; Priya, B. Bridging the gap: AI-powered FinTech and its impact on financial inclusion and financial well-being. *Discov. Artif. Intell.* **2025**, *5*, 290. [\[CrossRef\]](#)
22. European Commission. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Off. J. Eur. Union* **2024**, *64*, 1234–1381.
23. Aljunaid, S.K.; Almheiri, S.J.; Dawood, H.; Khan, M.A. Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection. *J. Risk Financ. Manag.* **2025**, *18*, 179. [\[CrossRef\]](#)
24. Prensky, M. Digital natives, digital immigrants part 2: Do they really think differently? *On Horizon* **2001**, *9*, 1–6. [\[CrossRef\]](#)
25. Twenge, J.M. More time on technology, less happiness? Associations between digital-media use and psychological well-being. *Curr. Dir. Psychol. Sci.* **2019**, *28*, 372–379. [\[CrossRef\]](#)
26. Batra, D.; Hamill, C.; Hartley, J.; Okhrati, R.; Seddon, D.; Miller, H.; Khraishi, R.; Cowan, G. A review of LLM agent applications in finance and banking. *SSRN* **2025**. [\[CrossRef\]](#)
27. Liu, Z.; Yang, Z.; Zhang, R.; Zhao, H.; Zhang, J.; Liu, Y.; Li, Y.; Shu, P.; Jiang, H.; Chen, J.; et al. A Survey of Generative AI in Finance. *HAL* **2025**, submitted. [\[CrossRef\]](#)
28. Ek, L.; Arnarp, E. Generative AI in Traditional Banking Institutes. Master's Thesis, Lund University, Lund, Sweden, 2024.
29. Godavarthi, S.; Nagvekar, R. GenAI Strategy: A Blueprint for Successful Adoption. In *Transforming Financial Services with Generative AI: From Strategy and Design to Practical Applications*; Apress: Berkeley, CA, USA, 2026; pp. 53–84.
30. Kumar, U.; Sinha, B. The advent of generative AI and financial industry. *Int. J. Financ.* **2024**, *9*, 55–70. [\[CrossRef\]](#)
31. Staegemann, D.; Haertel, C.; Daase, C.; Pohl, M.; Abdallah, M.; Turowski, K. A Review on Large Language Models and Generative AI in Banking. *FEMIB* **2025**, 267–278. [\[CrossRef\]](#)
32. Acharya, D.B.; Kuppan, K.; Divya, B. Agentic AI: Autonomous intelligence for complex goals—A comprehensive survey. *IEEE Access* **2025**, *13*, 18912–18936. [\[CrossRef\]](#)
33. Dwivedi, Y.K.; Helal, M.Y.I.; Elgendy, I.A.; Alahmad, R.; Walton, P.; Suh, A.; Singh, V.; Jeon, I. Agentic AI Systems: What It Is and Isn't. *Glob. Bus. Organ. Excell.* **2026**, *45*, 253–263. [\[CrossRef\]](#)
34. Balaskas, S. From recommendations to delegation: A systematic review mapping agentic AI in E-Commerce and its consumer effects. *Information* **2026**, *17*, 222. [\[CrossRef\]](#)
35. Kagal, L.; Finin, T.; Joshi, A. Trust-based security in pervasive computing environments. *Computer* **2001**, *34*, 154–157. [\[CrossRef\]](#)
36. Kurshan, E.; Balch, T.; Byrd, D. The Agentic Regulator: Risks for AI in Finance and a Proposed Agent-based Framework for Governance. *arXiv* **2025**, arXiv:2512.11933.
37. Samanta, S.K.; Chakraborty, A. Trust me, I'm wrong: The perils of AI hallucinations, a silent killer. *J. Inf. Technol. Teach. Cases* **2026**. [\[CrossRef\]](#)
38. Butt, J. Analytical study of the world's first EU Artificial Intelligence (AI) Act. *Int. J. Res. Publ. Rev.* **2024**, *5*, 7343–7364. [\[CrossRef\]](#)
39. Pavlidis, G. Unlocking the black box: Analysing the EU artificial intelligence act's framework for explainability in AI. *Law Innov. Technol.* **2024**, *16*, 293–308. [\[CrossRef\]](#)
40. Heo, W.; Grable, J.E. Data Privacy and Cybersecurity. In *Ethics and Compliance in Financial Services: Case Studies and Practical Examples from North America*; Springer Nature: Cham, Switzerland, 2026; pp. 197–224.
41. Entrust. *2025 Identity Fraud Report: The Rise of AI-Enabled Deepfake and Synthetic Identity Fraud*; Entrust Corporation: Shakopee, MN, USA, 2025.
42. Addula, S.R. Analysis of Perceived Ease of Use and Security on the Mobile Banking Adoption. Doctoral Dissertation, University of the Cumberland, Williamsburg, KY, USA, 2024.
43. Addula, S.R. Mobile Banking Adoption: A Multi-Factorial Study on Social Influence, Compatibility, Digital Self-Efficacy, and Perceived Cost Among Generation Z Consumers in the United States. *J. Theor. Appl. Electron. Commer. Res.* **2025**, *20*, 192. [\[CrossRef\]](#)
44. Ahmad, M. Review of the technology acceptance model (TAM) in internet banking and mobile banking. *Int. J. Inf. Commun. Technol. Digit. Converg.* **2018**, *3*, 23–41. [\[CrossRef\]](#)
45. Brown, S.A.; Venkatesh, V.; Goyal, S. Expectation confirmation in technology use. *Inf. Syst. Res.* **2012**, *23*, 474–487. [\[CrossRef\]](#)
46. Poromatikul, C.; De Maeyer, P.; Leelapanyalert, K.; Zaby, S. Drivers of continuance intention with mobile banking apps. *Int. J. Bank Mark.* **2020**, *38*, 242–262. [\[CrossRef\]](#)

47. Cloarec, J.; Meyer-Waarden, L.; Munzel, A. Transformative privacy calculus: Conceptualizing the personalization-privacy paradox on social media. *Psychol. Mark.* **2024**, *41*, 1574–1596. [CrossRef]
48. Adadi, A.; Berrada, M. Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access* **2018**, *6*, 52138–52160. [CrossRef]
49. Arrieta, A.B.; Díaz-Rodríguez, N.; Del Ser, J.; Benetot, A.; Tabik, S.; Barbado, A.; Garcia, S.; Gil-Lopez, S.; Molina, D.; Benjamins, R.; et al. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Inf. Fusion* **2020**, *58*, 82–115. [CrossRef]
50. Gefen, D.; Rao, V.S.; Tractinsky, N. The conceptualization of trust, risk and their relationship in electronic commerce: The need for clarifications. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*; IEEE Computer Society: Washington, DC, USA, 2003; Volume 8, p. 192b.
51. Rane, N.; Choudhary, S.; Rane, J. Explainable Artificial Intelligence (XAI) approaches for transparency and accountability in financial decision-making. *SSRN* **2023**. [CrossRef]
52. Nannini, L. Habemus a right to an explanation: So What?—A framework on Transparency-Explainability functionality and tensions in the EU AI act. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*, San Jose, CA, USA, 21–23 October 2024; Volume 7, pp. 1023–1035.
53. Minh, D.; Wang, H.X.; Li, Y.F.; Nguyen, T.N. Explainable artificial intelligence: A comprehensive review. *Artif. Intell. Rev.* **2022**, *55*, 3503–3568. [CrossRef]
54. Patidar, N.; Mishra, S.; Jain, R.; Prajapati, D.; Solanki, A.; Suthar, R.; Patel, K.; Patel, H. Transparency in AI decision making: A survey of explainable AI methods and applications. *Adv. Robot. Technol.* **2024**, *2*, 000110. [CrossRef]
55. Tritscher, J.; Krause, A.; Hotho, A. Feature relevance XAI in anomaly detection: Reviewing approaches and challenges. *Front. Artif. Intell.* **2023**, *6*, 1099521. [CrossRef] [PubMed]
56. Sungkarungsri, P.; Kiattisin, S. When Advice Isn't Trusted: Privacy, Transparency, and Accountability Risks Driving AI Mistrust and Consumer Resistance in Financial Advisory Services. *Sustainability* **2026**, *18*, 1354. [CrossRef]
57. Chow, W.S.; Shi, S. Investigating students' satisfaction and continuance intention toward e-learning: An extension of the expectation–confirmation model. *Procedia-Soc. Behav. Sci.* **2014**, *141*, 1145–1149. [CrossRef]
58. Golbeck, J. Computing with trust: Definition, properties, and algorithms. In *2006 Securecomm and Workshops*; IEEE: Piscataway, NJ, USA, 2006; pp. 1–7.
59. Ha, M.T.; Vo, V.B.; Nguyen, G.D. Disclosing personal information to continuous intention for mobile applications usage in e-commerce of Gen Z: A perspective on privacy calculus theory. *J. Int. Bus. Entrep. Dev.* **2024**, *16*, 288–308. [CrossRef]
60. Ashrafi, D.M.; Ahmed, S.; Shahid, T.S. Privacy or trust: Understanding the privacy paradox in users intentions towards e-pharmacy adoption through the lens of privacy-calculus model. *J. Sci. Technol. Policy Manag.* **2025**, *16*, 1224–1247. [CrossRef]
61. Abbas, H. Privacy Calculus Theory and E-Service Quality Factors and Their Impacts on the Satisfaction and Intention to Continue to Use Mobile Banking in Kuwait. *SSRN*. 2024. Available online: <https://ssrn.com/abstract=4969049> (accessed on 15 December 2025).
62. Kang, J.W.; Namkung, Y. The role of personalization on continuance intention in food service mobile apps: A privacy calculus perspective. *Int. J. Contemp. Hosp. Manag.* **2019**, *31*, 734–752. [CrossRef]
63. Choung, Y.; Chatterjee, S.; Pak, T.Y. Digital financial literacy and financial well-being. *Financ. Res. Lett.* **2023**, *58*, 104438. [CrossRef]
64. Pak, T.Y.; Chatterjee, S.; Choung, Y. Digital financial services use and life satisfaction: Is financial well-being a mediator? *Int. J. Consum. Stud.* **2026**, *50*, e70158. [CrossRef]
65. Tetteh, F.K.; Kwateng, K.O. The pathways from digital financial literacy to sustained engagement with mobile financial services: A technology continuance theory perspective. *J. Financ. Serv. Mark.* **2026**, *31*, 7. [CrossRef]
66. Fazreen, A.; Firmialy, S.D. Fintech Service Quality and Investment Literacy: Impacts on Banking Sustainability via Continuance Intention in a Regional Bank's Mobile App. *Society* **2025**, *13*, 895–915. [CrossRef]
67. Mahdzan, N.S.; Sabri, M.F.; Husniyah, A.R.; Magli, A.S.; Chowdhury, N.T. Digital financial services usage and subjective financial well-being: Evidence from low-income households in Malaysia. *Int. J. Bank Mark.* **2023**, *41*, 395–427. [CrossRef]
68. Muat, S.; Mahdzan, N.S.; Sukor, M.E.A.; Fachrurrozi; Sari, N. The role of financial inclusion, financial literacy and digital payment adoption in Indonesian millennials' financial well-being. *Int. J. Bank Mark.* **2025**, *43*, 1938–1968. [CrossRef]
69. Connelly, L.M. Cross-sectional survey research. *Medsurg Nurs.* **2016**, *25*, 369–370.
70. Park, Y.S.; Konge, L.; Artino, A.R., Jr. The positivism paradigm of research. *Acad. Med.* **2020**, *95*, 690–694. [CrossRef] [PubMed]
71. Creswell, J.W.; Creswell, J.D. *Research design: Qualitative, Quantitative, and Mixed Methods Approaches*; Sage Publications: Thousand Oaks, CA, USA, 2017.
72. Rouidi, M.; Hamdoune, A.; Choujtani, K.; Chati, A. TAM-UTAUT and the acceptance of remote healthcare technologies by healthcare professionals: A systematic review. *Inform. Med. Unlocked* **2022**, *32*, 101008. [CrossRef]
73. Sharma, G. Pros and Cons of Different Sampling Techniques. *Int. J. Appl. Res.* **2017**, *3*, 749–752.

74. Hair, J.F.; Risher, J.J.; Sarstedt, M.; Ringle, C.M. When to use and how to report the results of PLS-SEM. *Eur. Bus. Rev.* **2019**, *31*, 2–24. [[CrossRef](#)]
75. Toufaily, E.; Zalan, T. In blockchain we trust? Demystifying the “trust” mechanism in blockchain ecosystems. *Technol. Forecast. Soc. Change* **2024**, *206*, 123574. [[CrossRef](#)]
76. Almanasreh, E.; Moles, R.; Chen, T.F. Evaluation of methods used for estimating content validity. *Res. Soc. Adm. Pharm.* **2019**, *15*, 214–221. [[CrossRef](#)] [[PubMed](#)]
77. Finch, W.H. Multivariate analysis of variance for multilevel data: A simulation study comparing methods. *J. Exp. Educ.* **2022**, *90*, 173–190. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.