



# International Journal of Research Publication and Reviews

Journal Homepage: [www.ijrpr.com](http://www.ijrpr.com) ISSN 2582-7421

## Digital Financial Platforms: Consumer Trust, Information Security, and Regulatory Compliance

*Oluwatosin Esther Ajewumi<sup>1</sup>, Susanna Ayensu Blankson<sup>2</sup>, Jalia Nabadda<sup>3</sup>, Susanna Ayensu Blankson<sup>4</sup>, Jalia Nabadda<sup>5</sup>*

<sup>1-3</sup>Olin Business School, Washington University in Saint Louis, USA

<sup>4</sup>Southern Illinois University Edwardsville, USA

<sup>5</sup>Saint Louis University, USA

### ABSTRACT

Digital financial platforms have grown rapidly, sometimes faster than users can assess their safety, and trust is a key component of platform adoption. This paper considers consumer trust as a result that needs to be explained and discusses the role of two mechanisms, namely information security and regulatory compliance, in this regard. It examines recent empirical research, the seminal work on trust, and existing U.S. law, and constructs a conceptual model that connects the two mechanisms to trust. The framework treats security and compliance as parallel paths to trust, with the coherence/stability of the regulatory regime as a precondition that can enhance or hinder the compliance path. There are five propositions to be put to the test. In the fractured and volatile United States regime, compliance buys trust only modestly, and security and compliance can diverge as much as they align.

**Keywords:** Digital Financial Platforms, Consumer Trust, Information Security, Regulatory Compliance, Fintech, Open Banking

### 1. INTRODUCTION

The financial landscape has evolved rapidly in recent years, with digital financial technologies outpacing many previous consumer innovations, such as neobanks, payment apps, and embedded-finance services. The number of neobank users worldwide has increased from approximately 146 million in 2021 to an estimated 350 million or more by 2026 (Bhalla, 2025). This expansion is on an unsteady foundation. Recent studies show that factors beyond financial or technical expertise matter for adoption, as trust often matters more than knowledge, and that trust can be built through feeling. According to Hanson & Ott (2026), consumer trust in fintech depends on trust in the underlying technology, not on financial literacy. Trust replaces informed judgement when people cannot make their own judgment. This makes trust easy to give and hard to lose, shifting the burden of justification onto two external guarantees: the security practices that safeguard users who cannot directly regulate them, and the rules that govern the conduct of firms that users cannot directly regulate.

Most fintech trust studies so far have been descriptive and focused on adoption. They consistently show that trust predicts adoption and retention, and typically treat security and regulation as among many inputs (Jafri et al., 2024; Amnas et al., 2024). Three gaps remain. Little research examines information security and regulatory compliance as distinct means of building institutional trust, or what happens when they are separated. Second, regulation is often captured in a single “perceived regulatory support” index and does not account for situations in which rules are broken down or change. Third, most evidence is limited to one country, and no evidence exists on the impact of a dynamic, sectoral regime like that of the United States on trust. This paper remedies the gaps. It proposes a conceptual model in which security and compliance are two ways to build trust; it believes that if regulatory coherence and stability are the condition on the compliance path, it is because they are also the condition on the security path; and it advances five testable propositions from the current landscape in the U.S.

### 2. RESEARCH APPROACH

This is a conceptual paper and does not collect primary data. It constructs a framework based on two pieces of evidence – data collected in a systematic narrative review. We used combinations of trust, fintech, digital finance, information security, and regulatory compliance to identify peer-reviewed sources for the academic base. We used Google Scholar and journal databases to locate peer-reviewed sources. We prioritized recent empirical studies (2018 to 2026), as well as foundational trust theory that these more recent studies build on. Wherever possible, we relied on primary legal sources such as statutes, agency rules, and official government analysis, and we used current legal commentary to characterize evolving rules. We included sources based on relevance to the security-compliance-trust connection and/or currency, given that the U.S. regulatory stance shifted in 2025 and 2026. The

framework and propositions outlined in Section 5 draw on recurring themes in these sources and are presented as a platform for further testing, not as findings.

---

### 3. CONCEPTUAL FOUNDATION AND LITERATURE REVIEW

#### 3.1 Theoretical Foundations of Trust

Trust research provides a solid foundation to investigate digital finance. The widely cited model of Mayer et al. (1995) identifies three evaluative judgements that underlie an individual's willingness to be vulnerable to another party (ability, benevolence, and integrity). McKnight et al. (2002) expanded this to the online context, distinguishing between a person's inclination to trust, their trust in the institution as a whole, and their trust in the specific provider being considered. Gefen et al. (2003) later found that trust and perceived usefulness influence online transaction intentions, directly linking trust to technology adoption. Here are two salient points from this work. Trust is multi-layered: users trust a provider, the institutions surrounding the provider, and the technology that makes the provider work. Institution-based trust matters when a new provider is not yet known firsthand. Second, trust reduces perceived risks in uncertain environments, such as when a user cannot audit a platform. The two things that provide this institution-based trust are security and regulation.

#### 3.2 Consumer Trust in Digital Finance

Recent research has indeed revealed that trust is the principal requirement for digital finance adoption and that it is harder to gain in this area than in traditional banking. Data-intensive infrastructures and automated decisions leave users more exposed but with fewer opportunities to verify that the exposure is managed appropriately (Jafri et al., 2024). Trust and security emerged as more influential in the behavioural intention to adopt than perceived usefulness or social influence, placing trust above other factors in fintech adoption in banking (Jafri et al., 2024). The worry is that trust can develop without the user being able to evaluate the service. It is partly emotional; users can extend trust they do not have the experience to withdraw. Trust built this way is easier to damage, since a breach or a visible misuse of data can remove consent that was never closely reasoned. However, trust cannot be built without continuous support from security and regulation.

#### 3.3 Information Security as a Trust Mechanism

Information security is the first support. When users cannot check a platform, security protects them in the user's absence. Empirical studies support this: data security, interface design, and customer trust directly drive intention to use fintech, with data security also functioning as a precondition for customer trust, not a supplementary feature (Stewart & Jürjens, 2018; Jafri et al., 2024). The chips are very real. In 2025, financial services data breaches cost an average of 5.56 million U.S. dollars – the second highest among all sectors – and the U.S. had the highest national average at 10.22 million dollars (IBM, 2025). If users see a visible breach, they will return to older providers.

The problem is that trust responds to perceived security rather than real security. Users cannot distinguish a true weakness from an encryption badge or certification displayed on a platform. The risk expands with third-party vendors and application programming interfaces, and a platform's security relies, to some degree, on its third-party partners. There are aspects of security signals and underlying security that differ, and users might trust in these, only to find that the trust has been misplaced, one of the areas external regulation is supposed to restrict.

#### 3.4 Regulatory Compliance as a Trust Mechanism

The second type of support is regulation and requires primarily institutional trust. Rules establish a minimum level of security and disclosure and give users a basis to trust providers they cannot assess firsthand. Strong regulatory support has been associated with increased trust and fintech adoption (Amnas et al., 2024). In this way, compliance can make invisible practices visible and believable. However, compliance fosters trust only in specific ways. The clear, enforced, and stable rule sends a strong signal, whereas the weak, fragmented, and unstable rule sends a weak signal. Studies of adoption rarely include this condition because they assume regulation is static. The next section explains why, using the current United States regime as a case in point.

---

## 4. THE UNITED STATES REGULATORY LANDSCAPE

The degree of trust in the regime affects how far users can reasonably trust digital finance: institution-based trust depends on the credibility of the platform's guarantor. But the United States divides that guarantor by design, and that division creates practical problems.

Federal protection is administered sector by sector, rather than under a single standard. No general federal data-privacy law exists. Financial data security is based on the Gramm-Leach-Bliley Act of 1999 and the Federal Trade Commission's Safeguards Rule, which requires covered financial institutions to maintain a written information-security program and, as amended in 2024, report security breaches affecting 500 or more consumers (Federal Trade Commission, n.d.). Section 5 of the FTC Act treats unfair or deceptive practices separately. This protection applies to the institution holding the data, not the user, meaning a user's protection depends on the type of institution holding the data.

States have filled in some of the void, but inconsistently. By 2026, about twenty states had comprehensive privacy laws; the California Consumer Privacy Act of 2018 was passed, and no federal law overrode these state laws at the time (Ballard Spahr, 2026). These laws have different thresholds, rights, and enforcement mechanisms, and most exclude data already subject to the Gramm-Leach-Bliley Act. Next, a fintech customer's protection depends on their state and on which regime covers their records.

The federal centre is also up for grabs. A court has paused implementation and reopened for reconsideration the open-banking rule that would grant consumers transferable rights to their financial data, established in Section 1033 of the Dodd-Frank Act in October 2024, as the Congressional Research Service reported in 2025. Meanwhile, the Consumer Financial Protection Bureau, the agency tasked with focusing on consumer protection, has been reduced and defunded until 2026 and beyond (Jackman et al., 2026). When compliance is coherent and sustainable, it can contribute to trust. Currently, the United States has a sectoral baseline at the federal level, a patchwork of state baselines of varying quality, and a dwindling enforcer of trust, so the guarantor is also in question.

## 5. CONCEPTUAL FRAMEWORK AND RESEARCH PROPOSITION

The framework combines the two mechanisms in Figure 1. The main outcome is consumer trust, which is both institution-based and technological. Two paths feed it. One way is information security – real and perceived; and the other way is regulatory compliance. The regime's coherence and stability condition the compliance path: coherent, stable rules reinforce the regime, while incoherent or unstable rules weaken it. The two mechanisms are also linked: the more real compliance is perceived to be, the more trust it creates; the less real, the more compromise will affect trust when it is discovered. Trust drives adoption and continued use.

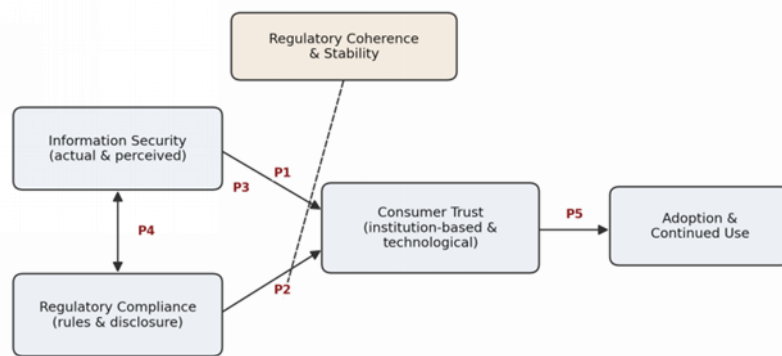


Figure 1. Security and compliance as parallel routes to consumer trust.

From this scheme, five propositions follow:

- P1. Consumers' trust in digital financial platforms is positively correlated with their perceptions of information security.
- P2. Consumer trust is positively linked to regulatory compliance, primarily through institution-based trust.
- P3. The link between compliance and trust is dampened under a fragmented or unstable regulatory regime.
- P4. Security and compliance are intertwined; therefore, the impact on trust is greater when they go together, and negative when they don't.
- P5. Adoption and continued use of digital financial platforms are positively correlated with consumer trust.

These propositions are drawn from the literature and the U.S. case and are intended to facilitate subsequent empirical work, not to report empirical results.

## 6. CONCLUSION

This paper aimed to better understand consumer trust in digital financial platforms as a result of information safety and regulatory compliance. The central theoretical insight is a conceptualization of the two as alternative paths to institution-based trust, how they interact, and the regulatory coherence and stability as a condition of the compliance path. This improves on adoption studies that treat security and regulation as separate inputs and stable rules.

This practical focus has two consequences. For providers, compliance should not be seen as a minimum security standard, but as a starting point because the difference between compliance and real security is where the trust goes. A lack of coherence and stability is not just a legal requirement; it also undermines consumer trust, since consumer confidence in adoption depends on coherence and stability.

The paper has limits. It is conceptual, meaning that it does not test its propositions. It focuses on the United States, so the regulatory reading may not be applicable to other regimes. Its evidence is current, but rules are rapidly changing and could change again. Future research is needed to validate the five

propositions using user-level data, to compare regimes with varying coherences and stabilities, and to explore consumer reactions to situations where compliance and security are clearly at odds.

### Compliance with ethical standards

#### *Disclosure of conflict of interest*

No conflict of interest to be disclosed.

### References

- 1) Amnas, M. B., Selvam, M., & Parayitam, S. (2024). FinTech and financial inclusion: Exploring the mediating role of digital financial literacy and the moderating influence of perceived regulatory support. *Journal of Risk and Financial Management*, 17(3), 108. <https://doi.org/10.3390/jrfm17030108>
- 2) Ballard Spahr. (2026, June 12). U.S. state privacy law landscape expands to 24 states: What the latest legislative wave means for businesses. Byte Back. <https://www.bytebacklaw.com/2026/06/u-s-state-privacy-law-landscape-expands-to-24-states-what-the-latest-legislative-wave-means-for-businesses/>
- 3) Bhalla, P. (2025). Neobank statistics and facts by market size, growth, revenue, user demographics, trends and insights (2025). Electro IQ. <https://electroiq.com/stats/neobank-statistics/>
- 4) Congressional Research Service. (2025). Access to consumer financial data: Open banking and the CFPB's Section 1033 rule (IF13117). <https://www.congress.gov/crs-product/IF13117>
- 5) Federal Trade Commission. (n.d.). Gramm-Leach-Bliley Act. <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>
- 6) Hanson, T. A., & Ott, C. (2026). Trust in financial technology: The role of financial literacy, digital financial literacy, technological literacy, and trust in artificial intelligence. *Journal of Risk and Financial Management*, 19(2), 97. <https://doi.org/10.3390/jrfm19020097>
- 7) IBM. (2025). Cost of a data breach report 2025. <https://www.ibm.com/reports/data-breach>
- 8) Jackman, S., Sommerfield, L., & Willis, C. (2026, February 19). GAO details CFPB reorganization, funding cuts, and litigation. Consumer Financial Services Law Monitor. <https://www.consumerfinancialserviceslawmonitor.com/2026/02/gao-details-cfpb-reorganization-funding-cuts-and-litigation/>
- 9) Jafri, J. A., Amin, S. I. M., Rahman, A. A., & Nor, S. M. (2024). A systematic literature review of the role of trust and security on fintech adoption in banking. *Heliyon*, 10(1), e22980. <https://doi.org/10.1016/j.heliyon.2023.e22980>
- 10) Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*, 26(1), 109–128. <https://doi.org/10.1108/ICS-06-2017-003>