Digital Payment Scams and the Consumer Trust Crisis: A Critical Review of Vulnerability, Blame, and Behavioral Backlash in Mobile Banking

Raksha Sharma

Abstract

The rapid expansion of mobile banking and digital payment systems has transformed consumer–financial service relationships while increasing exposure to phishing, impersonation, social engineering and account compromise. Existing research primarily examines these incidents through cybersecurity, perceived risk, technology adoption and fraud-prevention perspectives. This critical integrative review argues that these approaches insufficiently explain how scam exposure transforms technologically mediated service relationships into crises of consumer trust. Synthesising literature on digital payments, FinTech trust, consumer vulnerability, threat avoidance, innovation resistance, service failure and recovery, attribution, trust betrayal and consumer backlash, the paper develops the Consumer Trust Backlash Cycle. The framework comprises digital dependence, scam exposure, vulnerability appraisal, responsibility attribution, trust recalibration, emotional evaluation, behavioural response and institutional recovery or resistance amplification. It distinguishes technology-based from institutional trust and explains responses ranging from heightened vigilance and selective avoidance to reduced usage, provider switching, negative word-of-mouth and broader marketplace resistance. The paper reframes digital payment scams as consumer relationship problems and theorises post-adoption resistance and negative trust spillover across interconnected financial technologies.

Keywords: Digital Payment Scams, Consumer Trust, Mobile Banking; Fintech, Consumer Vulnerability, Behavioral Backlash, Innovation Resistance, Trust Violation, Institutional Trust, Consumer Resistance

Corresponding author (s):
ITM School of Business and Leadership, ITM University, Gwalior, Madhya Pradesh, India- 475001
Email: raksha.som@itmuniversity.ac.in

1. Introduction

Digital payment technologies have moved from optional service innovations to embedded infrastructures of everyday consumption. Mobile banking applications, digital wallets, instant transfers, QR-code payments, and biometric authentication have reduced the temporal and physical boundaries traditionally associated with financial exchange. The diffusion of digital finance has therefore been interpreted primarily as a success story of technological adoption, financial innovation, and consumer empowerment. Yet this success narrative contains an important paradox. The greater the extent to which consumers depend upon digital financial systems, the greater the potential consequences when those systems become associated with vulnerability. Digital transactions remove many forms of friction, but they also reduce the visibility of financial exchange. Consumers frequently cannot observe the technological processes through which transactions are authenticated, monitored, routed, or protected. They must therefore depend upon institutions and technologies whose underlying mechanisms they may neither understand nor control. Trust consequently remains fundamental to digital finance. As Hofmann (2020) argues, monetary systems depend fundamentally upon public confidence, even though the forms through which money is created, represented, and exchanged continue to evolve. The digitization of money does not eliminate the requirement for trust; rather, it redistributes trust across technological systems, financial institutions, platforms, regulatory arrangements, and increasingly complex infrastructures.

The contemporary FinTech literature similarly recognizes that trust cannot be treated as a simple attribute of a single organization. Devlin et al. (2025) identify institutional, interpersonal, and technology-related dimensions of trust as central to understanding contemporary FinTech relationships. The foundational trust literature reinforces this multidimensionality: Mayer et al. (1995) establish ability, benevolence, and integrity as the core dimensions of trustworthiness, while Rousseau et al. (1998) demonstrates that trust is defined across disciplines as a psychological state involving the willingness to accept vulnerability based upon positive expectations of another's behaviors.

However, a significant theoretical problem remains. Much of the digital banking literature examines trust as an antecedent of adoption, satisfaction, continuance intention, or usage (Gefen et al., 2003; Pavlou, 2003; Saibaba, 2024). This adoption-oriented perspective is valuable but incomplete. It does not adequately explain what occurs when consumers have already accepted technology and subsequently encounter fraud, impersonation, phishing, or sophisticated social engineering. Consumers may not simply reconsider whether technology is useful. Instead, they may reconsider whether they are safe within the relationship created by that technology. A consumer can perceive mobile banking as useful while simultaneously becoming distrustful of it, continuing to use a digital payment application because of convenience, network effects, or lack of practical alternatives while reducing the psychological trust placed in the system. Thus, continued use should not automatically be interpreted as continued trust.

The central argument of this paper is that digital payment scams should be understood as consumer vulnerability events capable of producing a progressive trust crisis and behavioral backlash. The longer-term consequence may be a reduced willingness to remain vulnerable within the digital financial ecosystem. This paper develops a critical integrative review addressing four questions: How has existing research conceptualized consumer trust and risk in digital financial services? Why is the prevailing framing of digital payment scams as cybersecurity incidents theoretically insufficient from a marketing perspective? How do vulnerability and responsibility attribution transform scam experiences into trust erosion and behavioral responses? Under what conditions can private consumer distrust evolve into broader behavioral backlash and resistance to digital financial innovation? The paper contributes to the literature in three principal ways: it reframes digital payment scams as relationship-disrupting marketplace events rather than exclusively technological security failures; it distinguishes perceived risk from trust violation, arguing that the latter provides a more powerful explanation of post-scam behavioral responses; and it develops the Consumer Trust Backlash Cycle, which conceptualizes consumer responses as a dynamic progression from scam exposure to vulnerability appraisal, blame attribution, trust recalibration, emotional evaluation, behavioral withdrawal, and either trust restoration or resistance amplification.

2. Review Approach: A Critical Integrative Perspective

This study adopts a critical integrative review approach, appropriate where the objective is to synthesize fragmented knowledge, interrogate dominant assumptions, identify conceptual blind spots, and develop new theoretical connections across adjacent research domains. The review integrates five interconnected streams: research on digital payments and mobile banking (Gefen et al., 2003; Pavlou, 2003; Saibaba, 2024); trust in financial services and FinTech (Bhattacherjee, 2002; Devlin et al., 2025; Sirdeshmukh et al., 2002); technology threats, innovation resistance, and technological mistrust (Liang & Xue, 2009; Ram, 1989; Ram & Sheth, 1989; Thompson & Rust, 2023); service failure and recovery, attribution theory, trust betrayal, and consumer backlash (Folkes, 1984; Grégoire & Fisher, 2008; Grégoire et al., 2009; Keaveney, 1995; Khamitov et al., 2020; Tax et al., 1998; Tomlinson & Mryer, 2009; Weiner, 1986); and emerging work on digital mistrust and consumer backlash (Ozturkcan & Bozdağ, 2025). The purpose of integrating these streams is not to suggest that digital payment scams are identical to AI bias, unethical banking behavior, or food-delivery boycotts. Rather, these literatures illuminate complementary mechanisms that remain insufficiently integrated within digital financial services research: vulnerability, responsibility, trust violation, emotional evaluation, and resistance.

3. The Digital Payment Paradox: Convenience, Dependence, and Vulnerability

3.1. From adoption to dependence

Digital payment research has generally emphasized the benefits associated with technological adoption, including reduced geographical and temporal constraints, speed, convenience, and increased consumer autonomy. These benefits help explain why perceived usefulness, ease of use, service quality, and trust are consistently associated with adoption and continuance (Gefen et al., 2003; Pavlou, 2003). However, the adoption narrative can obscure an important transformation. Once technology becomes embedded within everyday financial life, consumers may move from voluntary adoption to practical dependence. Employers, merchants, platforms, service providers, and peer networks increasingly assume the availability of digital payments, and physical alternatives may become less convenient or socially efficient. This development creates an important theoretical distinction: adoption concerns whether consumers begin using technology, whereas dependence concerns whether consumers can easily disengage from it. The distinction matters because a dependent consumer may continue using a service despite declining trust, and continued usage may therefore conceal an underlying deterioration in the consumer–technology relationship. Saibaba's (2024) study of mobile banking continuance intention in India identifies perceived risk, perceived trust, service quality, and satisfaction as important post-adoption

determinants, yet the dominant outcome remains continuance intention. Literature therefore remains better equipped to explain why consumers continue than why they may remain digitally active while psychologically withdrawing trust. This creates what may be termed the acceptance–dependence fallacy: the assumption that observable continued use necessarily reflects continued psychological acceptance.

3.2. Convenience can coexist with insecurity

Digital finance creates a second paradox. Systems are increasingly designed to reduce friction, yet reduced friction can create new forms of consumer exposure. A transaction completed within seconds leaves less opportunity for reflection. Communication channels that allow institutions to contact consumers instantly can also be imitated by fraudsters. Seamless authentication reduces effort but may obscure the processes through which security is maintained. The problem is exacerbated by information asymmetry: financial institutions possess technical knowledge, transaction histories, fraud analytics, and security expertise that individual consumers generally do not possess. This dependence makes trust central. McKnight et al. (2011) distinguish trust in technology from trust in people and organizations, demonstrating that confidence in a specific technology represents a meaningful construct with implications for technology-related beliefs and behavior. In digital finance, this distinction is particularly important because consumers simultaneously rely on an application, a financial institution, authentication infrastructure, and a wider governance system. A consumer may thus ask two different questions after a scam: Can I trust this technology? and Can I trust the institutions responsible for protecting me through this technology? Existing adoption research often does not sufficiently separate these questions.

4. Beyond Cybersecurity: Reframing Digital Payment Scams as Consumer Vulnerability Events

4.1. The limitations of cybersecurity framing

The dominant approach to digital fraud is largely technical, focusing on identifying threats, strengthening authentication, improving fraud detection, and encouraging consumers to recognize suspicious behavior. These measures are essential. However, from a consumer behavior perspective, the cybersecurity framing is incomplete because it focuses primarily on how fraud occurs rather than on what fraud means to consumers after it occurs. A digital payment scam can represent several things simultaneously: a criminal event, a financial loss, a failure of consumer control, a perceived institutional failure, and a violation of expected protection. The consumer's interpretation determines the relationship consequence. Technology threat avoidance theory provides an important starting point. Liang and Xue (2009) argue that threat avoidance differs qualitatively from technology acceptance: individuals respond to malicious technological threats through threat appraisal and coping appraisal, evaluating susceptibility, severity, the effectiveness of safeguarding measures, safeguarding costs, and self-efficacy. However, digital payment scams extend this logic because the threat may exploit the trust relationships surrounding technology. A scammer may impersonate a bank, reproduce institutional communication, or manipulate legitimate transaction processes. The consumer therefore encounters an unusual situation: the symbols that normally reduce uncertainty can become instruments of deception.

4.2. Scam exposure and vulnerability

Consumer vulnerability should not be treated as synonymous with consumer incompetence. Baker et al. (2005) defines consumer vulnerability as a state in which consumers experience limited control over marketplace interactions due to personal, social, or structural factors. Vulnerability is relational and situational rather than a permanent demographic characteristic. A highly educated and technologically experienced consumer can remain vulnerable to sophisticated social engineering because the fraudster may possess superior information regarding deception techniques or institutional impersonation. The financial consequences are particularly significant because consumers may perceive limited capacity to reverse digital transactions once authorization has occurred, generating a sense of reduced control. This realization is consequential because trust requires willingness to accept vulnerability (Mayer et al., 1995; Rousseau et al., 1998). When consumers perceive that vulnerability has become excessive, they may attempt to reduce dependence on the system. Kanyurhi et al. (2024) further show that unresponsive banking practices can undermine consumer trust, emphasizing that consumers who experience negative relational treatment may conclude that they cannot depend upon banks for assistance when difficulties arise. This insight is highly relevant to scam experiences: the consumer may initially fear the fraudster but subsequently fear the consequences of being left unsupported by the institution.

4.3. The consumer protection paradox

Digital finance has created what this review terms the consumer protection paradox. Financial institutions increasingly automate transactions, authentication, risk assessment, fraud monitoring, communication, and service interactions. At the same time, consumers are increasingly expected to act as the final line of defense against deception. They are instructed to identify phishing, verify communication, protect credentials, recognize impersonation, and detect social engineering. Consumer education is

therefore necessary, but it can also unintentionally shift responsibility from institutions to individuals. This raises an important marketing and ethical question: How much responsibility can reasonably be transferred to consumers in increasingly sophisticated digital environments? If consumers perceive that institutional communication, fraud prevention, or recovery mechanisms are inadequate, they may interpret the burden placed upon them as unfair. This interpretation moves the consumer response beyond perceived risk and toward responsibility attribution.

5. From Perceived Risk to Trust Violation

5.1. Risk is not equivalent to trust violation

A major conceptual weakness in digital banking research is the tendency to treat perceived risk as the principal negative counterpart of trust (Pavlou, 2003). Risk and trust are related but not identical. Perceived risk concerns the possibility of negative outcomes. Vulnerability concerns the consumer's exposure and perceived inability to fully control those outcomes. Trust concerns the willingness to accept vulnerability based on positive expectations regarding another actor, institution, or system (Mayer et al., 1995; Rousseau et al., 1998). Trust violation occurs when those expectations are perceived to have been breached. This distinction is crucial because consumers can accept risk without believing that trust has been violated. A successful fraud attempt does not automatically produce institutional distrust. However, if the consumer believes that the institution failed to provide adequate protection, communicated poorly, or treated the victim unfairly after the event, the experience may be interpreted as a violation of the trust relationship. The consumer's question therefore changes from 'Is this technology risky?' to 'Why was I not protected?' The second question is relational and institutional.

5.2. Trust in technology and trust in institutions

The distinction between technology-based trust and institutional trust is particularly important in digital finance. Technology-based trust involves beliefs regarding system reliability, security, technical competence, predictability, and functional integrity (McKnight et al., 2011). Institutional trust involves beliefs regarding organizational competence, benevolence, responsiveness, accountability, fairness, and structural protection (Devlin et al., 2025; Mayer et al., 1995; Morgan & Hunt, 1994; Sirdeshmukh et al., 2002). A scam can damage either dimension independently. A consumer may conclude that the technology is vulnerable, or alternatively that the technology may be imperfect, but the institution should have helped. The second response can be more damaging because it involves perceived failure of the organization responsible for maintaining the consumer relationship.

5.3. The movement toward perceived betrayal

The strongest form of trust disruption may occur when consumers experience betrayal-like interpretations. Perceived betrayal is more emotionally significant than generalized dissatisfaction because it involves the belief that a trusted relationship failed at a moment when the consumer was vulnerable. Grégoire and Fisher (2008) demonstrate that perceived betrayal is a key motivational force leading customers to restore fairness available, including retaliation. Their findings reveal that the 'love becomes hate' effect is particularly pronounced among customers with strong prior relationships when they attribute the failure to the firm's controllability. Financial services are especially susceptible to such responses because consumers entrust institutions with economically sensitive resources. Kanyurhi et al. (2024) further find that disrespect can undermine trust because consumers interpret such behavior as evidence that the institution does not value their dignity or interests. This insight suggests that the consumer's post-scam experience may be as important as the scam itself: a technically sophisticated fraud incident followed by rapid institutional support may remain an external criminal event, whereas the same incident followed by delayed communication, blame shifting, or procedural opacity may become an institutional violation.

6. Who Failed the Consumer? Responsibility Attribution and Institutional Blame

6.1. Attribution as a marketplace process

The question of responsibility represents one of the most underdeveloped dimensions of digital payment scam research. Objectively, responsibility may involve several actors: the fraudster, the consumer, the bank, the payment provider, technology intermediaries, and regulators. However, consumer behavior is shaped primarily by perceived responsibility. Attribution theory provides the essential framework. Weiner (1986) proposes that individuals interpret negative events along three causal dimensions—locus, stability, and controllability—and that these interpretations generate distinct emotional and behavioral consequences. Folkes (1984) demonstrates that the attributed reason for a product failure influence whether consumers desire refunds, perceive that an apology is owed, or want to hurt the firm's business. Applied to digital payment scams, a consumer who attributes the event entirely to a sophisticated criminal may maintain trust in the bank. A consumer who believes that the institution failed to detect suspicious behavior may become distrustful. A consumer who believes that the institution subsequently blamed the victim may experience anger or betrayal.

Institutional response is therefore a central stage in the construction of responsibility. The same fraud event can produce different consumer meanings depending on how the institution responds. One response may frame the institution as a protector—'You were targeted by a sophisticated fraudster, and we are actively helping you recover'—while another may frame the institution as a distant counterparty—'You authorized the transaction; therefore, responsibility is yours.' This distinction is highly relevant to relationship marketing because trust depends not only upon technical performance but also upon perceived concern and responsiveness (Morgan & Hunt, 1994; Sirdeshmukh et al., 2002). Tomlinson and Mryer (2009) demonstrate that trust is more difficult to restore when the cause of a transgression is attributed to internal, controllable factors within the transgressor.

6.2. When prevention fails, recovery becomes the service

No security system can eliminate all fraud. Consequently, consumer trust depends not only on prevention but also on recovery. This represents a major conceptual limitation in existing digital payment research, where fraud prevention is often treated as the central institutional objective. Yet from the consumer's perspective, the critical moment may occur after prevention has failed. At this point, consumers evaluate how quickly the institution responds, whether they can contact a human representative, whether the process is understandable, whether responsibility is explained fairly, and whether the institution appears concerned. The service recovery literature provides robust theoretical grounding. Tax et al. (1998) demonstrate that customers evaluate complaint incidents in terms of distributive, procedural, and interactional justice, and that these evaluations directly influence trust and commitment. Smith et al. (1999) show that customers prefer recovery resources that match the type and magnitude of the failure. Magnini et al. (2010) further argue that perceived fairness during service recovery involves counterfactual thinking—consumers assess whether the service provider could and should have done something more—and that when providers do not appear to exhibit appropriate effort, consumers attribute this to not caring, leading to anger. Dawar and Pillutla (2000) provide additional evidence that ambiguous or stonewalling responses can erode postcrisis brand equity. Thus, the post-scam response should be treated as a relationship recovery process, not simply an administrative procedure.

7. From Distrust to Behavioral Backlash

7.1. Why discontinuance is too narrow

Consumer responses to trust erosion are unlikely to be binary. A consumer does not necessarily either trust or reject mobile banking. Instead, behavioral responses may occur across a continuum. Traditional technology research frequently operationalizes negative outcomes through reduced adoption intention, discontinuance intention, or switching intention (Keaveney, 1995). These outcomes are useful but insufficient. Consumers can modify their behavior without abandoning the technology completely. This review therefore conceptualizes behavioral backlash as a multidimensional set of protective, resistant, and expressive responses that emerge when consumers perceive digital financial systems as exposing them to unacceptable vulnerability.

7.2. The continuum of behavioral responses

At the initial level, consumers may engage in protective behavior, including verifying communications more frequently, reducing transaction values, avoiding clicking links, and using additional authentication. These behaviors should not automatically be interpreted as rejection; they may represent rational coping consistent with technology threat avoidance theory (Liang & Xue, 2009). When threat perception persists, consumers may reduce their dependence on technology through consumption withdrawal, including reduced transaction frequency, avoidance of high-value digital payments, selective use of banking features, and increased reliance on physical channels. This behavior is particularly important because conventional adoption metrics may fail to detect it. A consumer may remain an active mobile banking user while substantially reducing the role of digital payments in everyday financial life.

As trust erosion deepens, relationship withdrawal may follow. Consumers may move accounts, use alternative payment providers, reduce financial product holdings, and recommend competing institutions. Keaveney (1995) identifies core service failure, failed service recovery, and pricing issues among the primary drivers of customer switching in service industries. These outcomes transform a technology-security issue into a customer-relationship issue. At the expressive level, consumers may externalize their dissatisfaction through complaints, negative word-of-mouth, social media criticism, and public storytelling of scam experiences. Hennig-Thurau et al. (2004) identify concern for other consumers, venting of negative feelings, and the desire for social interaction as primary motivations for electronic word-of-mouth. At this stage, the consumer is no longer simply protecting himself or herself but is participating in the social construction of marketplace trust, which is particularly important because trust is socially transmissible.

At the most extensive level, consumers may engage in collective marketplace resistance. Grégoire et al. (2009) demonstrate that when customer love turns

into lasting hate, the effects of relationship strength and time produce both revenge and avoidance behaviors. Laeeque and Samdani (2026) provide a relevant mechanism from consumer ethics research, demonstrating how perceived ethical violations in platform contexts can produce ethical judgments, moral outrage, and boycott-related behavioral resistance. The relevant question for digital financial services is therefore: under what conditions does individual caution become collective resistance? Consumers may tolerate unavoidable risk but react more strongly when they believe institutions have failed ethically or relationally.

8. Innovation Resistance and the Generalization of Distrust

Innovation resistance theory provides an additional lens for understanding post-scam behavior. Ram and Sheth (1989) identify functional barriers—including usage, value, and risk—and psychological barriers, such as tradition and image, as important sources of consumer resistance. Ram (1989) further demonstrates that perceived risk and cognitive resistance can generate opposition to innovations. However, the traditional innovation resistance perspective primarily addresses barriers to acceptance. Digital payment scams require an extension toward post-adoption resistance: a consumer may initially perceive an innovation as valuable and later reinterpret it as threatening after a harmful experience. Thus, resistance need not precede adoption. The consumer trajectory may instead follow the path of acceptance, dependence, vulnerability, mistrust, and resistance. Thompson and Rust (2023) provide a complementary perspective, demonstrating that digital innovation is shaped by social, cultural, and institutional factors and that resistance can emerge when technological change threatens existing relationships or information structures. Consumers may resist a technologically superior payment system if it becomes associated with loss of control, increased vulnerability, institutional uncertainty, or perceived unfairness.

A particularly important but underexplored consequence is negative trust spillover. A consumer harmed by a mobile banking scam may not limit distrust to the original application. Instead, the experience may generalize to digital wallets, biometric authentication, AI-enabled banking, open banking, cryptocurrency, and automated investment platforms. The consumer may form a broader cognitive category that digital financial technology is unsafe. The brand spillover literature supports this mechanism: Roehm and Tybout (2006) demonstrate that brand scandals can spill over to competing brands and the broader product category, while Ahluwalia et al. (2000) show that consumer commitment moderates the processing of negative publicity. Dawar and Pillutla (2000) further establish that product-harm crises can erode brand equity depending on consumer expectations and firm response. The systematic review by Khamitov et al. (2020) integrates brand transgression, service failure, and product-harm crisis research, demonstrating that these three streams share common underlying mechanisms. Ozturkcan and Bozdağ's (2025) analysis of the AI mistrust cycle provides an additional parallel, arguing that technological enthusiasm can deteriorate into public skepticism and backlash when implementation failures and ethical concerns undermine expectations. The implication for digital finance is that trust failure may travel across technologies.

9. The Consumer Trust Backlash Cycle

The preceding review suggests that the relationship between scams and consumer resistance is neither linear nor inevitable. The same scam may produce caution, trust erosion, anger, switching, or collective resistance depending on how consumers interpret the event and how institutions respond. The following framework synthesizes the reviewed literature into eight interconnected stages.

Stage 1: Digital dependence. Consumers become increasingly reliant on mobile banking and digital payments because of convenience, network participation, institutional expectations, and reduced transaction friction. At this stage, usage may be high, but usage should not be assumed to represent unconditional trust.

Stage 2: Scam exposure. Consumers experience direct victimization, attempted fraud, impersonation, unauthorized activity, repeated scam communication, or indirect exposure through peers or media. Direct financial loss is one possible outcome but not the only psychologically significant one. Even attempted fraud can activate threat appraisal processes (Liang & Xue, 2009).

Stage 3: Vulnerability appraisal. Consumers reassess their ability to recognize threats, their capacity to control exposure, the severity of potential losses, and the reliability of available safeguards. This stage corresponds with the threat and coping processes described by Liang and Xue (2009) and with the vulnerability framework of Baker et al. (2005), who emphasize that vulnerability is multidimensional, context-specific, and not necessarily enduring.

Stage 4: Responsibility attribution. Consumers determine who they believe failed. Potential attribution targets include fraudsters, the consumer, the technology, the financial institution, payment intermediaries, and regulators. This stage is critical because the attribution of institutional responsibility transforms an external security incident into a relationship problem. Weiner's (1986) attribution

theory and Folkes's (1984) consumer attribution research demonstrate that the perceived locus, controllability, and stability of the cause determine subsequent emotional and behavioral responses.

Stage 5: Trust recalibration. Consumers reassess both technology-based trust and institutional trust. The distinction is essential because trust in technology and trust in the institution responsible for the relationship may deteriorate independently (Devlin et al., 2025; McKnight et al., 2011). A consumer may maintain confidence in the technical infrastructure while losing confidence in the institution's benevolence and responsiveness, or vice versa.

Stage 6: Emotional evaluation. Depending on perceived severity and responsibility, consumers may experience anxiety, fear, frustration, anger, betrayal, or moral outrage. Weiner (1986) demonstrates that distinct causal attributions produce distinct emotions: attributions to external, uncontrollable factors generate anxiety, whereas attributions to controllable institutional failures generate anger. Grégoire and Fisher (2008) further show that perceived betrayal is a particularly potent emotional state that motivates retaliatory behavior. Emotional intensity determines whether distrust remains private or becomes expressive.

Stage 7: Behavioral response. Responses can range from vigilance to selective avoidance, reduced usage, switching, negative word-of-mouth, and collective resistance. This progression should not be treated as inevitable. Consumers may remain at earlier stages depending upon the effectiveness of institutional recovery. Keaveney (1995) demonstrates that service failure and poor recovery are among the most powerful drivers of customer switching, while Hennig-Thurau et al. (2004) show that venting negative emotions is a primary motivation for electronic word-of-mouth.

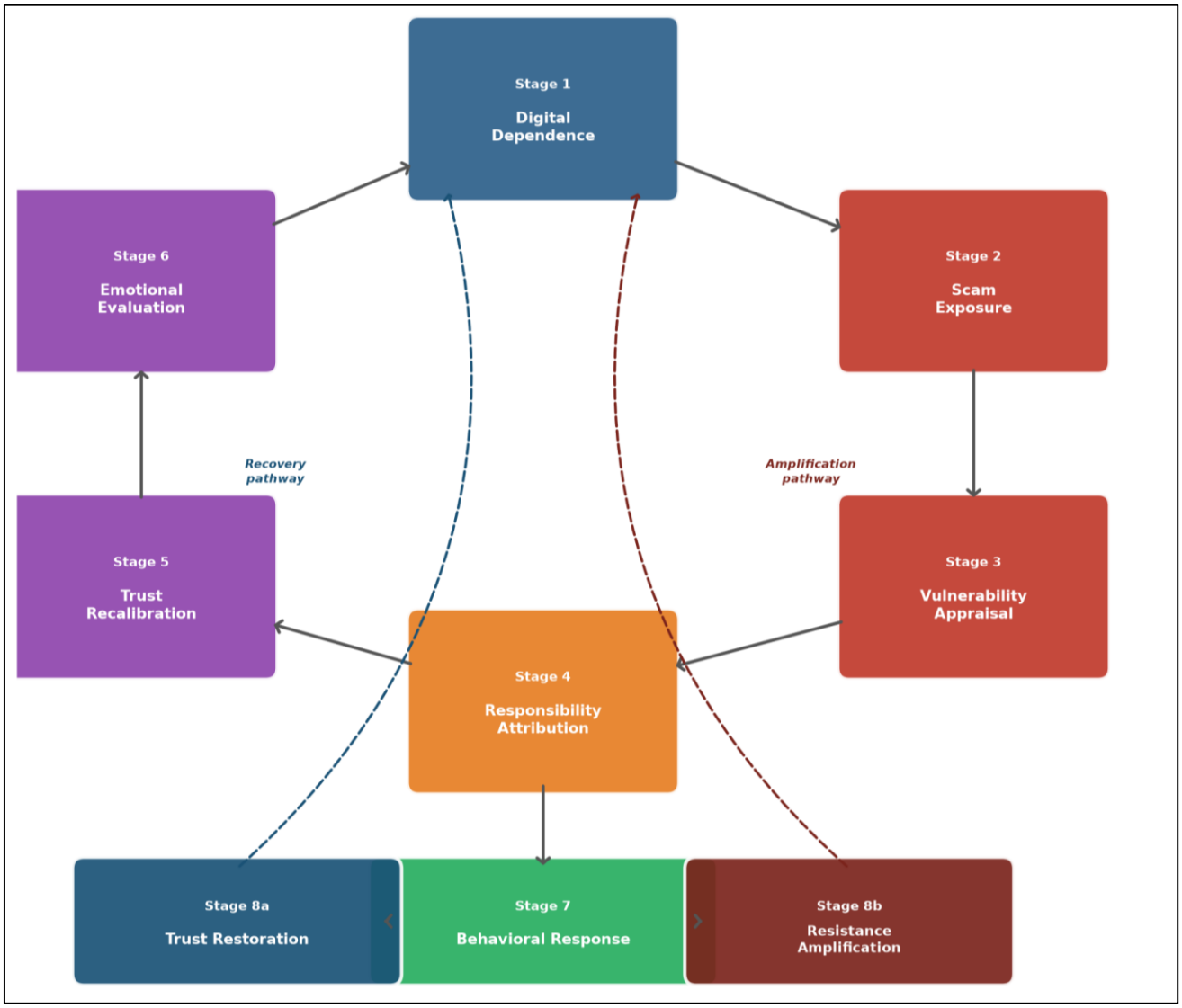

Figure 1. The Consumer Trust Backlash Cycle

Stage 8: Institutional response. Institutional response can produce two different outcomes. Trust restoration is more likely when institutions demonstrate transparency, responsiveness, empathy, fair procedures, clear communication, accessible human support, and credible fraud prevention improvements

(Smith et al., 1999; Tax et al., 1998). Resistance amplification is more likely when consumers experience opacity, delayed responses, shifting, automated detachment, perceived disrespect, or inconsistent communication (Grégoire & Fisher, 2008; Kanyurhi et al., 2024). This final stage makes the framework cyclical rather than linear. Institutional conduct after fraud determines whether vulnerability is gradually reduced or incorporated into a continuing cycle of mistrust. Figure 1 illustrates the cyclical framework, and Table 1 summarizes its stages and theoretical anchors.

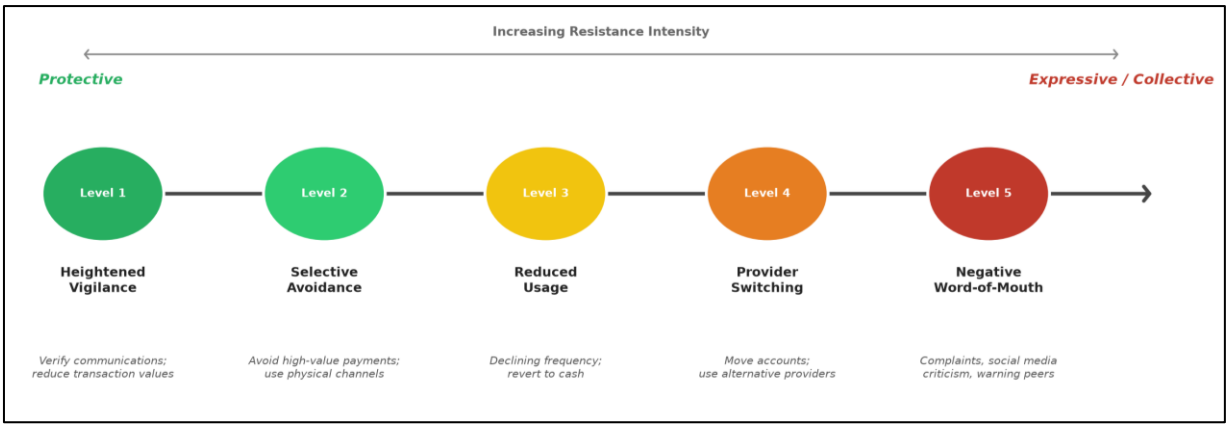

Figure 2. Continuum of Consumer Behavioral Responses to Digital Payment Scams

Table 1. The Consumer Trust Backlash Cycle

Stage	Core Process	Key Theoretical Anchor
1. Digital dependence	Reliance on digital finance; usage ≠ trust	Adoption–dependence fallacy
2. Scam exposure	Direct/indirect fraud encounter	Technology threat avoidance (Liang & Xue, 2009)
3. Vulnerability appraisal	Reassessment of control and exposure	Consumer vulnerability (Baker et al., 2005)
4. Responsibility attribution	Assignment of perceived blame	Attribution theory (Weiner, 1986; Folkes, 1984)
5. Trust recalibration	Independent erosion of technology vs. institutional trust	Trust in technology (McKnight et al., 2011)
6. Emotional evaluation	Anxiety, anger, betrayal, moral outrage	Attribution–emotion link (Weiner, 1986)
7. Behavioral response	Vigilance → avoidance → switching → NWOM → resistance	Switching (Keaveney, 1995); NWOM (Hennig-Thurau et al., 2004)
8. Institutional response	Trust restoration or resistance amplification	Service recovery justice (Tax et al., 1998)

10. Critical Research Agenda

The literature reviewed in this paper reveals several unresolved theoretical tensions that warrant future empirical investigation. First, the dominant assumption that continued usage represents continued acceptance should be directly tested. Future research should investigate consumers who remain active users of mobile banking but report declining institutional trust, perceived safety, and willingness to conduct high-value transactions, distinguishing behavioral persistence from psychological commitment through longitudinal designs.

Second, future studies should examine when scam exposure produces perceived risk and when it produces perceived betrayal. Possible boundary conditions include the severity of financial loss, the degree of institutional impersonation, consumer attribution of preventability, institutional response quality, and prior relationship strength. Tomlinson and Mryer (2009) demonstrate that the dimensions along which a trust violation is attributed—particularly whether it is perceived as intentional and controllable—significantly influence the difficulty of trust repair. Theoretical models that combine all negative perceptions under the umbrella of perceived risk may obscure important differences in emotional intensity and behavioral persistence.

Third, future research should investigate the consumer protection paradox: how much responsibility consumers believe they should bear, how institutional communication influences self-blame, when fraud awareness education becomes perceived responsibility shifting, and whether consumers evaluate technologically sophisticated

institutions more harshly after scams. Fourth, not all distrust becomes visible. Future research should distinguish between private avoidance, complaint behavior, negative word-of-mouth, social media advocacy, and collective resistance. Laeeque and Samdani's (2026) findings regarding ethical judgments, moral outrage, and consumer resistance suggest that future digital-finance research should examine the emotional and moral mechanisms through which harmful marketplace experiences become collective behavioral responses.

Fifth, negative trust spillover requires empirical investigation. Researchers should examine whether a negative experience with one digital financial technology changes consumers' evaluations of other financial technologies, using longitudinal designs because generalized resistance may emerge gradually. The brand spillover literature (Ahluwalia et al., 2000; Roehm & Tybout, 2006) and the systematic review of Khamitov et al. (2020) provide a methodological foundation for such investigation. Finally, literature should move beyond asking whether fraud prevention systems are effective. It should also examine which institutional responses restore trust, whether human interaction outperforms automated recovery, whether compensation restores technology trust or only institutional trust, whether transparency reduces perceived betrayal, and how procedural fairness influences post-scam loyalty.

11. Managerial and Policy Implications

The review has several implications for financial institutions and FinTech providers. First, fraud prevention should be treated as a customer relationship strategy rather than exclusively a cybersecurity function. Fraud affects not only financial assets but also consumer perceptions of the institution's competence and benevolence—dimensions that Mayer et al. (1995) identify as foundational to trustworthiness. Second, institutions should design visible security, as mechanisms that remain invisible may technically protect consumers but fail to generate confidence. Third, the post-scam period should be treated as a critical relationship moment: when prevention fails, the recovery process becomes the primary evidence through which consumers evaluate institutional trustworthiness. The service recovery literature (Smith et al., 1999; Tax et al., 1998) demonstrates that perceived justice in recovery directly influences trust, commitment, and loyalty. Fourth, consumer education should enhance consumer agencies without implying that consumers alone are responsible for preventing technologically sophisticated fraud. Finally, financial institutions should monitor behavioral indicators of emerging distrust, including reduced transaction frequency, declining transaction values, avoidance of features, and switching behavior following fraud alerts. Such indicators may reveal a trust crisis before it becomes visible through customer attrition. Ozturkcan and Bozdağ (2025) emphasize transparency, ethical governance, and human agency as mechanisms for interrupting cycles of technological mistrust. The broader principle applies technological legitimacy cannot be sustained through technical performance alone when consumers perceive the system as opaque or unresponsive.

12. Conclusion

Digital payment technologies have transformed financial consumption by reducing friction, increasing accessibility, and embedding financial transactions within everyday digital life. Yet the same transformation has produced a new consumer paradox: the technologies that increase convenience may simultaneously increase dependence upon infrastructures that consumers cannot fully understand, observe, or control. This review argues that digital payment scams should therefore not be understood solely as cybersecurity failures. They are also consumer vulnerability events and potential relationship-disrupting marketplace events. The central contribution of this paper is the argument that the movement from scam exposure to consumer resistance depends upon several interpretive stages. Consumers first evaluate vulnerability, then assign responsibility, recalibrate trust, experience emotional responses, and finally modify their behavior. These modifications may range from rational vigilance to selective avoidance, relationship withdrawal, negative word-of-mouth, collective resistance, and generalized technological mistrust.

The proposed Consumer Trust Backlash Cycle consequently challenges a central assumption of digital adoption research: that continued use necessarily represents continued acceptance. In increasingly digitized financial environments, consumers may remain functionally dependent while psychologically distrustful. Such hidden distrust may represent an important early warning signal for financial institutions. The long-term sustainability of digital finance will therefore depend not only upon reducing fraud but also upon maintaining consumers' willingness to remain vulnerable within digital financial relationships. When prevention fails, institutions must demonstrate competence, responsiveness, transparency, fairness, and concern. Otherwise, an isolated criminal event may become a broader crisis of consumer trust.

References

Ahluwalia, R., Burnkrant, R. E., & Unnava, H. R. (2000). Consumer response to negative publicity: The moderating role of commitment. Journal of

Marketing Research, 37(2), 203–214. https://doi.org/10.1509/jmkr.37.2.203.18734

Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building understanding of the domain of consumer vulnerability. Journal of Macromarketing, 25(2), 128–139. https://doi.org/10.1177/0276146705280622

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. Journal of Management Information Systems, 19(1), 211–241. https://doi.org/10.1080/07421222.2002.11045715

Dawar, N., & Pillutla, M. M. (2000). Impact of product-harm crises on brand equity: The moderating role of consumer expectations. Journal of Marketing Research, 37(2), 215–226. https://doi.org/10.1509/jmkr.37.2.215.18729

Devlin, J. F., Roy, S. K., Sekhon, H., Moin, S. M. A., & Sahiner, M. (2025). Trust and FinTech: A review and research agenda. Electronic Markets, 35, Article 62. https://doi.org/10.1007/s12525-025-00769-2

Folkes, V. S. (1984). Consumer reactions to product failure: An attributional approach. Journal of Consumer Research, 10(4), 398–409. https://doi.org/10.1086/208978

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51–90. https://doi.org/10.2307/30036519

Grégoire, Y., & Fisher, R. J. (2008). Customer betrayal and retaliation: When your best customers become your worst enemies. Journal of the Academy of Marketing Science, 36(2), 247–261. https://doi.org/10.1007/s11747-007-0054-0

Grégoire, Y., Tripp, T. M., & Legoux, R. (2009). When customer love turns into lasting hate: The effects of relationship strength and time on customer revenge and avoidance. Journal of Marketing, 73(6), 18–32. https://doi.org/10.1509/jmkg.73.6.18

Hennig-Thurau, T., Gwinner, K. P., Walsh, G., & Gremler, D. D. (2004). Electronic word-of-mouth via consumer-opinion platforms: What motivates consumers to articulate themselves on the Internet? Journal of Interactive Marketing, 18(1), 38–52. https://doi.org/10.1002/dir.10073

Hofmann, C. (2020). The changing concept of money: A threat to the monetary system or an opportunity for the financial sector? European Business Organization Law Review, 21, 37–68. https://doi.org/10.1007/s40804-020-00182-z

Kanyurhi, E. B., Bugandwa Mungu Akonkwa, D., Lusheke, B. M., Cubaka, P. M., Karhamikire, P. K., & Bucekuderhwa Bashige, C. (2024). When unethical practices harm relationship outcomes: Testing the influence of consumer-perceived unethical behaviour on trust and satisfaction in the banking sector. International Journal of Bank Marketing, 42(6), 1178–1211. https://doi.org/10.1108/IJBM-03-2023-0163

Keaveney, S. M. (1995). Customer switching behavior in service industries: An exploratory study. Journal of Marketing, 59(2), 71–82. https://doi.org/10.1177/002224299505900206

Khamitov, M., Grégoire, Y., & Suri, A. (2020). A systematic review of brand transgression, service failure recovery and product-harm crisis: Integration and guiding insights. Journal of the Academy of Marketing Science, 48(3), 519–542. https://doi.org/10.1007/s11747-019-00679-1

Laeeque, S. H., & Samdani, H. (2026). The moral calculus of food delivery: How algorithmic dehumanization and CSR shape boycotts through ethical judgments and moral outrage. International Journal of Ethics and Systems, ahead-of-print, 1–30. https://doi.org/10.1108/IJOES-06-2025-0338

Lewicki, R. J., & Bunker, B. B. (1996). Developing and maintaining trust in work relationships. In R. Kramer & T. Tyler (Eds.), Trust in organizations: Frontiers of theory and research (pp. 114–139). Sage. https://doi.org/10.4135/9781452243610.n7

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. MIS Quarterly, 33(1), 71–90. https://doi.org/10.2307/20650279

Magnini, V. P., Honeycutt, E. D., & Cross, A. T. (2010). Application of fairness theory to service failures and recovery. Journal of Service Research, 13(3), 323–338. https://doi.org/10.1177/1094670509348918

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734. https://doi.org/10.5465/amr.1995.9508080335

McKnight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. ACM Transactions on Management Information Systems, 2(2), Article 12, 1–25. https://doi.org/10.1145/1985347.1985353

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. Journal of Marketing, 58(3), 20–38. https://doi.org/10.1177/002224299405800302

Ozturkcan, S., & Bozdağ, A. A. (2025). Responsible AI in marketing: AI booing and AI washing cycle of AI mistrust. International Journal of Market Research, 67(6), 696–722. https://doi.org/10.1177/14707853251306565

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce, 7(3), 101–134. https://doi.org/10.1080/10864415.2003.11044275

Ram, S. (1989). Successful innovation using strategies to reduce consumer resistance: An empirical test. Journal of Product Innovation Management, 6(1), 20–34. https://doi.org/10.1111/1540-5885.610020

Ram, S., & Sheth, J. N. (1989). Consumer resistance to innovations: The marketing problem and its solutions. Journal of Consumer Marketing, 6(2), 5–14. https://doi.org/10.1108/EUM0000000002542

Roehm, M. L., & Tybout, A. M. (2006). When will a brand scandal spill over, and how should competitors respond? Journal of Marketing Research, 43(3), 366–373. https://doi.org/10.1509/jmkr.43.3.366

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. Academy of Management Review, 23(3), 393–404. https://doi.org/10.5465/amr.1998.926617

Saibaba, S. (2024). Examining the determinants of mobile banking app continuance intention in India: An extension of the IS success model. Journal of Internet Commerce, 23(1), 50–89. https://doi.org/10.1080/15332861.2023.2236428

Sirdeshmukh, D., Singh, J., & Sabol, B. (2002). Consumer trust, value, and loyalty in relational exchanges. Journal of Marketing, 66(1), 15–37. https://doi.org/10.1509/jmkg.66.1.15.18449

Smith, A. K., Bolton, R. N., & Wagner, J. (1999). A model of customer satisfaction with service encounters involving failure and recovery. Journal of Marketing Research, 36(3), 356–372. https://doi.org/10.1177/002224379903600305

Tax, S. S., Brown, S. W., & Chandrashekaran, M. (1998). Customer evaluations of service complaint experiences: Implications for relationship marketing. Journal of Marketing, 62(2), 60–76. https://doi.org/10.1177/002224299806200205

Thompson, B. S., & Rust, S. (2023). Blocking blockchain: Examining the social, cultural, and institutional factors causing innovation resistance to digital technology in seafood supply chains. Technology in Society, 73, Article 102235. https://doi.org/10.1016/j.techsoc.2023.102235

Tomlinson, E. C., & Mryer, R. C. (2009). The role of causal attribution dimensions in trust repair. Academy of Management Review, 34(1), 85–104. https://doi.org/10.5465/amr.2009.35713291

Weiner, B. (1986). An attributional theory of motivation and emotion. Springer-Verlag. https://doi.org/10.1007/978-1-4612-4948-1