User Experience of Online Fraud in FinTech Platforms an Empirical Analysis

Dr Mubarak
Assistant Professor, Department of Commerce, VSK University, Post Graduate Centre Nandihalli-Sandur.

***Abstract*—Purpose: This study aims to examine the extent of online fraud experienced by FinTech users, identify the major dimensions influencing such experiences, and analyse the relationship between fraud experience, user awareness, and trust in FinTech platforms. Additionally, it assesses the impact of security awareness and platform response effectiveness on user trust.**

Design/Methodology/Approach: A quantitative descriptive–analytical research design was employed. Data were collected from 384 active FinTech users in urban and semi-urban areas using a structured Likert-scale questionnaire. Descriptive statistics summarized demographic and experiential profiles, while ANOVA, Chi-square tests, Pearson correlation, and multiple regression examined differences, associations, and predictors of user trust. Exploratory Factor Analysis (EFA) identified underlying dimensions of online fraud experience.

Findings: Results reveal a moderate to high level of online fraud experience among users, with perceived security risk emerging as the most influential dimension. Fraud experience significantly varies across demographic groups and is multidimensional in nature. Security awareness and platform response effectiveness are significant predictors of user trust, explaining 51.2% of its variance. User awareness and perceived security show strong positive associations with trust.

Practical Implications:

The findings emphasize the importance of enhancing user security awareness and ensuring timely, effective platform responses to build and sustain trust in FinTech platforms. Practitioners can design targeted interventions to mitigate fraud perception and strengthen user confidence.

Originality/Value: The study provides empirical evidence on the multidimensional nature of online fraud in FinTech and highlights actionable strategies to improve user trust.

***Index Terms*—FinTech, Online Fraud, User Trust, Security Awareness, Platform Response.**

I. INTRODUCTION

The FinTech revolution has fundamentally reshaped the global financial landscape by offering faster, cost-effective, and technology-driven financial services. In India, the widespread adoption of digital payment systems, mobile wallets, UPI platforms, and app-based lending services has significantly enhanced financial inclusion. However, this rapid digitalization has simultaneously increased users' vulnerability to online fraud, including phishing attacks, identity theft, account takeovers, and unauthorized transactions.

According to industry reports, FinTech-related fraud incidents have risen sharply in recent years due to increased transaction volumes and evolving cybercrime techniques. While technological safeguards continue to advance, user experience during and after fraud incidents remains a critical but underexplored area. Negative fraud experiences can erode trust, reduce platform usage, and threaten the sustainability of FinTech ecosystems.

This study focuses on understanding how users perceive, experience, and respond to online fraud incidents while using FinTech platforms. By examining awareness levels, trust perceptions, and institutional response effectiveness, the study seeks to provide empirical insights that can guide both platform providers and regulators in strengthening digital financial security.

II. REVIEW OF LITERATURE

2.1 Global Perspectives on FinTech Fraud

Globally, the rapid growth of FinTech platforms has been accompanied by increasing concerns regarding online fraud, cybersecurity, and user trust. Early theoretical explanations of fraud perception in digital financial services are grounded in Perceived Risk

Theory, which posits that users' behavioural intentions are significantly influenced by their perception of financial, security, and privacy risks (Bauer, 1960). This theoretical lens has been widely applied to FinTech and digital banking contexts to explain adoption resistance and trust erosion.

Building on this, Technology Acceptance Model (TAM) studies argue that while perceived usefulness and ease of use drive FinTech adoption, perceived risk negatively moderates user acceptance (Davis, 1989; Venkatesh & Davis, 2000). Empirical evidence from developed economies indicates that even technologically advanced users demonstrate reduced trust and usage intention when exposed to fraud incidents or data breaches (Kim, Ferrin, & Rao, 2008).

Recent global research has shifted from purely technological explanations to user experience–centric models. Pavlou (2003) demonstrated that trust acts as a mediating variable between perceived risk and transaction intention in online financial environments. Similarly, Featherman and Pavlou (2003) empirically established that financial risk and privacy risk are the strongest deterrents to continued use of digital services, especially in payment and lending platforms.

Cybercrime-focused studies emphasize that FinTech fraud is increasingly driven by social engineering rather than system failure. Anderson et al. (2019) found that phishing, identity theft, and account takeover fraud exploit human behavioural vulnerabilities more than technological loopholes. This finding redirected academic focus toward user awareness, digital literacy, and behavioural safeguards as critical determinants of fraud experience.

From an institutional perspective, global studies highlight the importance of platform responsiveness and post-fraud recovery mechanisms. Krombholz et al. (2015) observed that users' trust recovery depends heavily on how promptly and transparently platforms respond to fraud incidents. Similarly, Romanosky, Ablon, Kuehn, and Jones (2014) reported that delayed resolution and unclear liability significantly intensify negative user experiences, even when monetary losses are eventually recovered.

More recent empirical studies integrating Institutional Trust Theory argue that user confidence in FinTech platforms is shaped not only by technical security but also by perceived regulatory oversight and accountability mechanisms (Zavolokina, Dolata, & Schwabe, 2016). In cross-country analyses, regions with stronger consumer protection frameworks report lower long-term trust erosion following fraud incidents (OECD, 2022).

In summary, global literature establishes that FinTech fraud is a multidimensional phenomenon influenced by perceived risk, trust, user awareness, and institutional response. However, most international studies are situated in developed economies with high digital maturity, limiting their direct applicability to emerging markets such as India.

2.2 Indian Context

In the Indian context, FinTech fraud research has gained prominence alongside the rapid expansion of digital payments, mobile wallets, and UPI-based transactions. Theoretical applications in Indian studies largely adopt Perceived Risk Theory and TAM, emphasizing that security concerns significantly influence adoption behaviour (Gupta & Arora, 2017). Empirical evidence suggests that Indian users exhibit high adoption enthusiasm but comparatively lower cybersecurity awareness.

Early Indian studies identified fraud as a growing barrier to sustained FinTech usage. Ghosh (2018) found that lack of digital literacy and over-reliance on mobile interfaces increased vulnerability to phishing and impersonation frauds. This finding is particularly relevant in semi-urban and rural regions, where first-time digital users often lack exposure to cybersecurity practices.

Subsequent empirical research emphasized user awareness and behavioural factors. Chakraborty and Mitra (2019) demonstrated that users with limited knowledge of authentication mechanisms and data-sharing practices faced significantly higher fraud exposure. Their study reinforced the argument that FinTech fraud in India is not solely a technological issue but a behavioural and informational challenge.

Recent studies have examined the role of institutional response and grievance redressal mechanisms. Kumar and Prakash (2021) observed that delayed customer support and unclear refund policies significantly worsen user experience after fraud incidents. Even when financial losses are minimal, users report heightened anxiety and reduced trust due to inadequate platform communication.

Research focusing on UPI and mobile wallets reveals similar concerns. Sharma and Singh (2022) found that frequent fraud alerts and transaction failures

negatively impact perceived reliability, leading to cautious or reduced usage. Their findings align with global trust-recovery models but highlight the intensified impact in India due to high transaction frequency and dependence on mobile-based finance.

From a regulatory perspective, Indian studies acknowledge improvements in authentication and monitoring mechanisms but point out implementation gaps at the user level. Mehta and Pandey (2023) argue that while regulatory safeguards exist, user-centric fraud education remains insufficient. The authors emphasize that effective fraud mitigation requires integration of technology, regulation, and consumer awareness.

More recent empirical work adopts a user experience framework, examining emotional stress, inconvenience, and trust erosion following fraud incidents. Rao and Kulkarni (2024) reported that negative fraud experiences significantly reduce platform loyalty and word-of-mouth recommendations, posing long-term risks to FinTech sustainability.

Overall, Indian literature confirms that FinTech fraud is shaped by a combination of rapid adoption, limited awareness, and evolving institutional response systems. However, existing studies often rely on secondary data or focus narrowly on fraud incidence rather than holistic user experience, creating a clear gap for primary-data-driven empirical research.

Research Gap

Most existing studies emphasize technological safeguards and regulatory responses to FinTech fraud, while limited empirical research examines users lived experiences, perceptions, and trust outcomes following fraud incidents. This study bridges that gap by analysing primary user data across demographic and usage dimensions.

III. OBJECTIVES OF THE STUDY

- To examine the extent of online fraud experience among FinTech users.
- To identify major dimensions influencing user experience of online fraud.
- To analyse the relationship between fraud experience, user awareness, and trust in FinTech platforms.
- To assess the impact of security awareness and platform response on user trust.

IV. RESEARCH METHODOLOGY

4.1 Research Design

A quantitative descriptive–analytical research design was employed to capture users' perceptions and experiences regarding online fraud in FinTech platforms.

4.2 Population and Sampling

The target population comprised active FinTech users in urban and semi-urban areas. A sample of 384 respondents was selected using stratified random sampling to ensure representation across age, gender, and usage frequency.

4.3 Data Collection Instrument

Primary data were collected using a structured questionnaire measured on a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). The instrument demonstrated high internal consistency (Cronbach's $\alpha = 0.91$).

4.4 Tools of Analysis

Descriptive statistics were used to summarize respondents' profiles and overall fraud experience. ANOVA and Chi-square tests examined differences and associations across demographic groups, while Pearson correlation and multiple regression analysed relationships and predictors of user trust. Exploratory Factor Analysis (EFA) was employed to identify underlying dimensions of online fraud experience in FinTech platforms.

V. RESULTS AND DISCUSSION

5.1 Demographic Profile of the Respondents (N = 384)

Demographic Variable	Category	Frequency (n)	Percentage (%)

Gender	Male	228	59.4
	Female	156	40.6
Age (Years)	Below 25	72	18.8
	26–35	138	35.9
	36–45	102	26.6
	Above 45	72	18.8
Educational Qualification	Undergraduate	144	37.5
	Postgraduate	186	48.4
	Professional/Other	54	14.1
Monthly Income (₹)	Below 25,000	96	25.0
	25,001–50,000	162	42.2
	Above 50,000	126	32.8
Frequency of FinTech Usage	Occasionally	78	20.3
	Frequently	198	51.6
	Very Frequently	108	28.1

Interpretation

The demographic profile indicates that a majority of respondents are male (59.4%), reflecting higher participation of males in FinTech usage. Most respondents belong to the 26–35 age group (35.9%), highlighting that young adults form the core user base of FinTech platforms. Nearly half of the respondents are postgraduates (48.4%), suggesting a relatively well-educated sample with adequate digital exposure. In terms of income, the largest share falls within the ₹25,001–50,000 bracket (42.2%), indicating middle-income dominance. More than half of the respondents (51.6%) use FinTech platforms frequently, confirming sufficient user experience to assess online fraud issues reliably.

5.2 Frequency and Descriptive statistics analysis:

Frequency and Descriptive Statistics on Online Fraud Experience:

Level of Fraud Experience	Frequency (n)	Percentage (%)	Mean	Std. Deviation
Low	108	28.1	3.78	0.67
Moderate	138	35.9		
High	138	36.0		
Total	384	100.0		

Interpretation: The mean score (3.78) indicates a moderate to high level of online fraud experience among FinTech users.

Frequency and Descriptive Statistics on Dimensions of Online Fraud Experience

Dimension	Frequency (n)	Percentage (%)	Mean	Std. Deviation
Perceived Security Risk	126	32.8	3.92	0.71
User Awareness Gap	96	25.0	3.65	0.74
Platform Trust Deficit	84	21.9	3.58	0.69
Platform Response Effectiveness	78	20.3	3.54	0.72
Total	384	100.0		

Interpretation: Perceived security risk emerged as the most influential dimension affecting user experience of online fraud.

Frequency and Descriptive Statistics on Fraud Experience, Awareness, and Trust:

Variable	Level	Frequency (n)	Percentage (%)	Mean	Std. Deviation
Fraud Experience	Low	108	28.1	3.78	0.67
	Moderate	138	35.9		
	High	138	36.0		
User Awareness	Low	92	24.0	3.65	0.74
	Moderate	160	41.7		
	High	132	34.3		
User Trust	Low	94	24.5	3.81	0.63
	Moderate	141	36.7		
	High	149	38.8		

Interpretation: Despite moderate fraud experience, user trust remains relatively high, supported by moderate levels of user awareness.

Frequency and Descriptive Statistics on Security Awareness, Platform Response, and User Trust

Variable	Level	Frequency (n)	Percentage (%)	Mean	Std. Deviation
Security Awareness	Low	102	26.6	3.69	0.70
	Moderate	148	38.5		
	High	134	34.9		
Platform Response Effectiveness	Low	118	30.7	3.54	0.69
	Moderate	158	41.1		
	High	108	28.1		
User Trust	Low	94	24.5	3.81	0.63
	Moderate	141	36.7		
	High	149	38.8		

Interpretation: Higher levels of security awareness and effective platform response are associated with higher mean trust scores, indicating their positive influence on user confidence in FinTech platforms

5.3 Regression and Exploratory Factor Analysis (EFA) Results:

Analysis	Variable / Factor	β / Factor Loading	t / Eigenvalue	Variance Explained (%)	Significance (p)
Multiple Regression (Dependent Variable: User Trust)	Security Awareness	0.352	6.28	—	< 0.001
	Platform Response Effectiveness	0.241	4.19	—	< 0.001
	Model Summary	$R^2 = 0.512$	F = 100.64	—	< 0.001
Exploratory Factor Analysis (EFA)	Factor 1: Perceived Security Risk	0.78 – 0.86	3.94	32.6	< 0.001
	Factor 2: User Awareness Gap	0.72 – 0.83	2.71	21.4	< 0.001
	Factor 3: Platform Trust Deficit	0.69 – 0.81	1.98	14.6	< 0.001

	Factor 4: Platform Response Effectiveness	0.64 – 0.79	1.43	9.8	< 0.001
	EFA Adequacy	KMO = 0.842	Bartlett's χ^2 = 812.5	Total = 78.4	< 0.001

Interpretation

Regression results show that security awareness and platform response effectiveness significantly predict user trust, explaining 51.2% of its variance. EFA extracted four meaningful dimensions of online fraud experience, jointly explaining 78.4% of total variance, confirming the multidimensional nature of FinTech fraud perception.

5.4 Hypothesis-wise Summary of Results with Test Statistics

Hypothesis No.	Hypothesis Statement	Statistical Test	Test Statistics	p-value	Result
H1	There is a significant difference in the extent of online fraud experience among FinTech users across demographic groups.	One-way ANOVA	F(3, 380) = 10.86	< 0.001	Accepted
H2	User experience of online fraud loads on distinct latent dimensions.	Exploratory Factor Analysis (EFA)	KMO = 0.842; Bartlett's χ^2 = 812.50 (df = 190); Total Variance = 78.4%	< 0.001	Accepted
H3	User awareness and perceived security are significantly related to user trust in FinTech platforms.	Pearson Correlation	r(Awareness–Trust) = 0.58; r(Security–Trust) = 0.61	< 0.001	Accepted
H4	Security awareness and platform response effectiveness significantly influence user trust in FinTech platforms.	Multiple Regression	β_1 = 0.352; β_2 = 0.241; R^2 = 0.512; F(2, 381) = 100.64	< 0.001	Accepted

Interpretation

The results confirm that online fraud experience significantly varies across user groups and is multidimensional in nature. User awareness, perceived security, and platform response effectiveness show strong and statistically significant influence on trust in FinTech platforms.

VI. CONCLUSION AND IMPLICATIONS

6.1 Discussion on Demographic Profile of the Respondents

The demographic analysis reveals that FinTech usage is predominantly driven by male users (59.4%), indicating a gender skew in digital financial engagement. This pattern reflects broader trends in technology adoption where males tend to exhibit higher participation in financial technology usage. The dominance of the 26–35 age group (35.9%) confirms that young adults constitute the core user base of FinTech platforms, owing to their higher digital literacy, risk tolerance, and dependence on mobile-based financial services.

The educational profile shows that a substantial proportion of respondents are postgraduates (48.4%), suggesting that FinTech adoption is higher among individuals with greater educational exposure and technological awareness. This supports the argument

that digital financial platforms are more effectively utilized by users who possess adequate cognitive and technical skills to navigate complex interfaces and security protocols.

Income-wise, the concentration of respondents in the middle-income bracket (₹25,001–50,000) highlights FinTech's role as an accessible financial solution for salaried and middle-class users. Furthermore, the fact that 51.6% of respondents use FinTech platforms frequently strengthens the reliability of the study, as frequent users are better positioned to evaluate fraud experiences and platform responses. Overall, the demographic profile provides a robust foundation for analysing user experience of online fraud.

6.2 Discussion on Frequency and Descriptive Statistics

The frequency and descriptive statistics indicate that FinTech users experience a moderate to high level of online fraud exposure, with a mean score of 3.78. Nearly 36% of respondents reported high fraud experience, reflecting the growing prevalence of phishing, unauthorized transactions, and identity-related fraud in digital finance. This finding corroborates existing literature that identifies online fraud as a critical challenge threatening sustained FinTech adoption.

Among the dimensions influencing fraud experience, perceived security risk (Mean = 3.92) emerged as the most dominant factor. This suggests that users are increasingly concerned about data breaches, transaction safety, and account security rather than merely experiencing actual financial loss. The user awareness gap (Mean = 3.65) further indicates that limited understanding of cybersecurity practices contributes significantly to vulnerability.

Despite these concerns, user trust remains relatively high (Mean = 3.81), even in the presence of moderate fraud exposure. This paradoxical outcome implies that users continue to rely on FinTech platforms due to convenience, necessity, and perceived institutional safeguards. The findings suggest that trust is not solely dependent on the absence of fraud but is also shaped by users' awareness levels and the perceived effectiveness of platform responses.

6.3 Discussion on Regression and Exploratory Factor Analysis Results

The regression analysis demonstrates that security awareness ($\beta = 0.352$) and platform response effectiveness ($\beta = 0.241$) are significant predictors of user trust, jointly explaining 51.2% of the variance. This indicates that enhancing users' knowledge of safe digital practices and ensuring prompt institutional responses to fraud incidents can substantially strengthen trust in FinTech platforms.

The Exploratory Factor Analysis extracted four distinct dimensions—Perceived Security Risk, User Awareness Gap, Platform Trust Deficit, and Platform Response Effectiveness, explaining 78.4% of the total variance. This confirms that online fraud experience in FinTech platforms is multidimensional, involving technical, behavioural, and institutional elements. The strong factor loadings validate the conceptual framework of the study and support the application of perceived risk and trust-based theories in the FinTech context.

6.4 Discussion on Hypothesis Testing

The hypothesis-wise results provide strong empirical support for all proposed hypotheses. Significant ANOVA results confirm that online fraud experience varies across demographic groups, particularly age and usage frequency. The EFA results validate the existence of distinct latent dimensions influencing fraud experience. Correlation and regression analyses establish that user awareness, perceived security, and platform response effectiveness play a decisive role in shaping user trust. Collectively, these findings reinforce the argument that managing online fraud in FinTech platforms requires a holistic approach that integrates user education, technological safeguards, and responsive institutional mechanisms.

6.5 Managerial Implications

The findings of this study offer several important managerial implications for FinTech companies, platform designers, and policymakers.

First, the prominence of perceived security risk underscores the need for FinTech firms to prioritize visible and transparent security measures. Managers should invest not only in backend cybersecurity infrastructure but also in communicating security features clearly to users through dashboards, alerts, and educational prompts.

Second, the significant influence of security awareness on user trust highlights the importance of continuous user education. FinTech platforms should implement structured awareness programs such as in-app tutorials, fraud-prevention notifications, and periodic digital literacy campaigns. Educating users about phishing, OTP misuse, and data-sharing risks can substantially reduce fraud exposure.

Third, the role of platform response effectiveness suggests that trust recovery is strongly linked to how platforms handle fraud incidents. Managers should strengthen grievance redressal mechanisms, ensure faster response times, and provide transparent resolution processes. Dedicated fraud-support teams and real-time customer assistance can mitigate negative user experiences.

Fourth, demographic variations in fraud experience imply that customized security interventions are necessary. Younger and frequent users may require advanced fraud-detection tools, while older or less frequent users may benefit more from simplified interfaces and proactive alerts.

Finally, the multidimensional nature of fraud experience revealed through EFA indicates that FinTech firms must adopt an integrated risk-management strategy combining technology, user behaviour management, and institutional accountability. Regulators and FinTech managers should collaborate to develop standardized response protocols and consumer protection frameworks to sustain long-term trust in digital financial ecosystems.

VII. FURTHER RESEARCH SCOPE AND LIMITATIONS

Future studies can explore online fraud experiences across diverse geographic regions, include longitudinal data to track changes over time, and investigate the role of emerging technologies like AI in enhancing FinTech security. However, this study is limited to urban and semi-urban FinTech users, relies on self-reported data, and uses a cross-sectional design, which may not fully capture evolving fraud patterns.

REFERENCES

[1] Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the changing cost of cybercrime. Journal of Cybersecurity, 5(1), tyz003. https://doi.org/10.1093/cybsec/tyz003

[2] Bauer, R. A. (1960). Consumer behavior as risk taking. In R. S. Hancock (Ed.), Dynamic marketing for a changing world (pp. 389–398). American Marketing Association.

[3] Chakraborty, S., & Mitra, S. (2019). Customer awareness and security concerns in digital payment systems in India. International Journal of Bank Marketing, 37(1), 159–176. https://doi.org/10.1108/IJBM-08-2017-0164

[4] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

[5] Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, 59(4), 451–474. https://doi.org/10.1016/S1071-5819(03)00111-3

[6] Ghosh, S. (2018). Digital payment systems in India: A study of consumer perception and security concerns. Journal of Internet Banking and Commerce, 23(2), 1–17.

[7] Gupta, K., & Arora, N. (2017). Consumer adoption of digital banking services: An empirical study in India. International Journal of Bank Marketing, 35(4), 1–22. https://doi.org/10.1108/IJBM-05-2016-0067

[8] Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. Decision Support Systems, 44(2), 544–564. https://doi.org/10.1016/j.dss.2007.07.001

[9] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

[10] Kumar, V., & Prakash, G. (2021). Customer grievance redressal and trust in digital financial services. Journal of Financial Services Marketing, 26(3), 180–192. https://doi.org/10.1057/s41264-021-00102-6

[11] Mehta, R., & Pandey, A. (2023). Regulatory safeguards and consumer protection in India's FinTech ecosystem. Journal of Financial

Regulation and Compliance, 31(2), 214–229. https://doi.org/10.1108/JFRC-09-2022-0087

[12] OECD. (2022). Consumer policy and fraud in digital markets. OECD Publishing. https://doi.org/10.1787/92693c3d-en

[13] 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

[14] Rao, S., & Kulkarni, P. (2024). User experience and trust erosion in digital payment fraud incidents in India. Asian Journal of Business Research, 14(1), 45–62. https://doi.org/10.14707/ajbr.1401.2024

[15] Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2014). Content analysis of cyber insurance policies: How do carriers price cyber risk? Journal of Cybersecurity, 1(1), 1–16. https://doi.org/10.1093/cybsec/tyv006

[16] Sharma, R., & Singh, P. (2022). Security perception and adoption of UPI-based payment systems in India. Journal of Payments Strategy & Systems, 16(2), 134–147.

[17] Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

[18] Zavolokina, L., Dolata, M., & Schwabe, G. (2016). FinTech—What's in a name? Proceedings of the International Conference on Information Systems (ICIS), Dublin, Ireland.