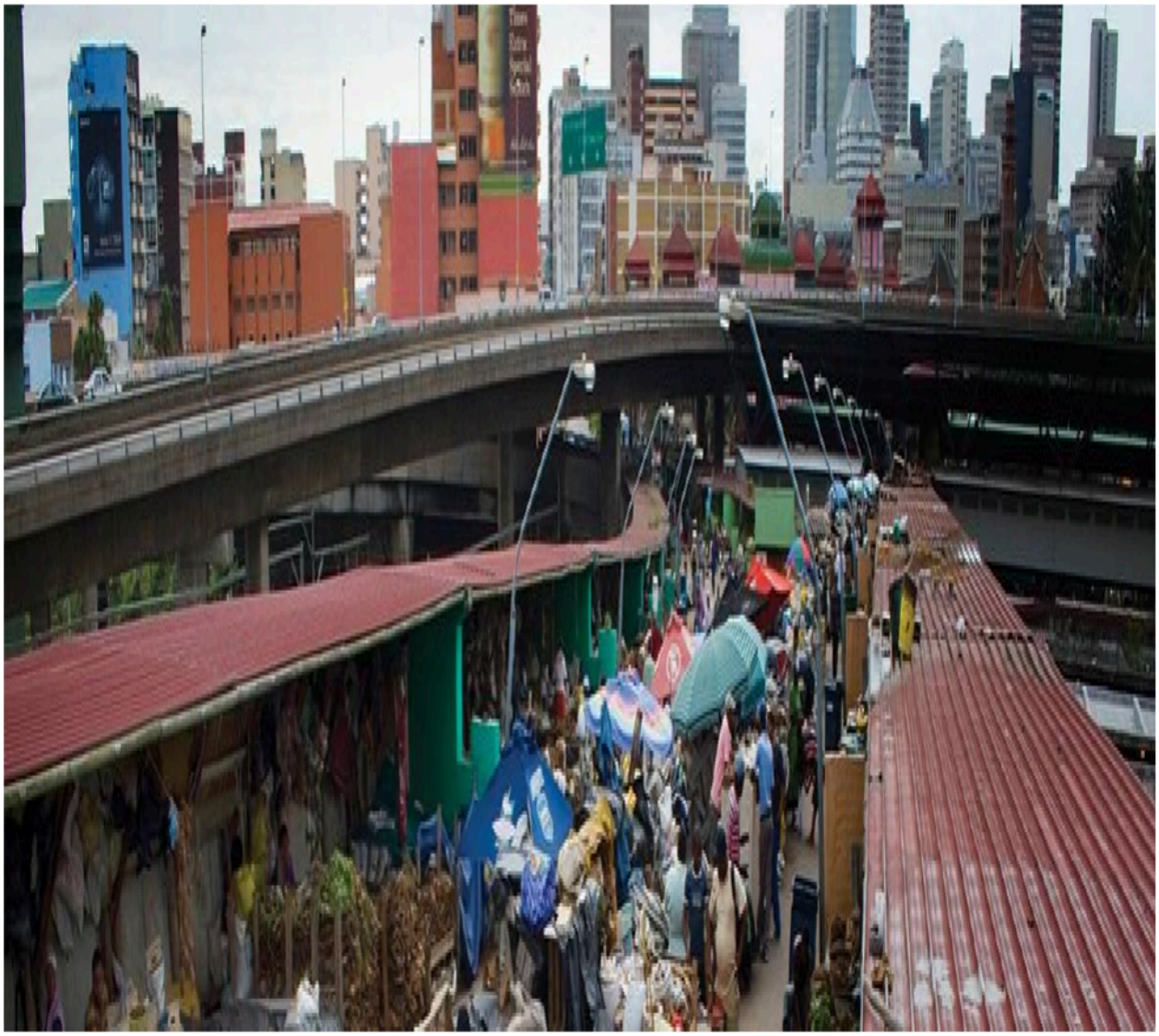
JOURNAL OF FORMAL AND INFORMAL SECTORS

Volume: 6 Issue: 4
(October-December), 2026
(ISSN: 2791-2604)



KMF PUBLISHERS

www.kmf-publishers.com/jfis/

http://kmf-publishers.com/jfis/

RESEARCH ARTICLE

OPEN

AI Fraud Detection, Privacy Safeguards, and Continued Use of Mobile Financial Services in Bangladesh

Poushia Hossen Megha[1*], Mst. Asura Jaman Osru[1], Md Wahidul Bari[1], Kazi Abdul Mannan[2]

© The Authors 2026

Artificial intelligence is increasingly being incorporated into financial-sector risk management, including automated anomaly detection and fraud monitoring. Yet the legitimacy of AI-enabled fraud controls depends not only on technical security gains but also on whether users perceive monitoring as proportionate, privacy-protective, reviewable, and institutionally accountable. This study develops a security-privacy-continuance perspective for mobile financial services (MFS) in Bangladesh and examines how AI literacy, perceived regulatory protection, and procedural fairness relate to users' acceptance of AI-enabled fraud controls and continued-use intentions. The study follows the Group 8 research design and uses the Q8 five-point Likert questionnaire. The supplied database contains 385 records; however, its Codebook identifies the respondent sequence and contextual comments as synthetic, so the empirical results are explicitly treated as demonstrative rather than field evidence. Composite reliability diagnostics reveal a major measurement problem: Cronbach's alpha is low for AI literacy (α=.322), fairness (α=.193), regulatory protection (α=.250), and the full fraud/privacy/continuance block (α=.224). This finding is substantively important rather than merely technical: the instrument's items appear to combine related but non-identical governance dimensions, making a single latent construct inappropriate without refinement. Item-level robust regressions nevertheless show that regulatory protection is positively associated with both continued-use indicators (FPC4: b=.335, p=.002; FPC5: b=.255, p=.009), while AI literacy is positively associated with perceived fraud-detection benefit (FPC1: b=.242, p=.019) and false-alert reviewability (FPC3: b=.267, p=.015). In the aggregate model, AI literacy, fairness, and regulatory protection jointly explain 15.8% of variance in the FPC composite. The study's principal contribution is therefore a measurement-aware account of AI financial trust: users may support fraud detection while simultaneously requiring privacy safeguards, review mechanisms, and credible regulatory protection. For Bangladesh, the implication is that AI fraud governance should be designed as a socio-technical consumer-protection architecture rather than as surveillance technology alone. The manuscript identifies precise questionnaire revisions and a validation pathway required before substantive publication.

Keywords: artificial intelligence; fraud detection; privacy safeguards; mobile financial services; regulatory protection; continuance intention; Bangladesh

Journal of Formal and Informal Sectors (2026), 6(4). https://doi.org/10.64907/xkmf.v6i4.jfis.2

[1]Department of Law
[2]Department of Business Administration, Faculty of Business, Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh.

Corresponding Author: Poushia Hossen Megha. poushiamegha@gmail.com

Received: 20 September 2026 Revised: 25 October 2026 Accepted: 28 October 2026 Published: 30 October 2026

1. Introduction

Mobile financial services have become a central component of Bangladesh's digital financial ecosystem. Bangladesh Bank reports millions of registered MFS customers and a large active-account base, illustrating the scale at which digital payment services operate. The regulator permits a broad range of MFS functions, including person-to-person, person-to-business, business-to-person and government-related payments. This scale creates a dual policy challenge: digital finance must remain accessible and convenient while becoming sufficiently resilient against fraud, cyber risk and operational abuse. Bangladesh Bank's recent payment-system reporting describes fraud as a persistent risk in the digital payment ecosystem and highlights stronger transaction monitoring, rapid wallet-freezing procedures, agent-level controls and behavioural analytics as important responses. The 2022 MFS Regulations likewise require security, authentication, confidentiality, integrity and accountability mechanisms. These developments make AI-enabled fraud detection a legally relevant governance issue, not merely a technical question.[1]

AI can strengthen financial security by detecting anomalous transaction patterns at speeds that would be difficult to achieve through manual review. However, automated monitoring can also intensify privacy concerns, create false positives, restrict legitimate transactions, or produce decisions that users cannot easily understand or contest. The central policy question is therefore not whether fraud detection is desirable in the abstract. It is whether users perceive the exchange between security and data monitoring as legitimate and whether institutional safeguards make them willing to continue using the service. This shifts the analytical focus from "AI adoption" to the conditions under which security automation remains socially and legally acceptable.[2]

Existing technology-acceptance research provides strong explanations of behavioural intention, while privacy-calculus research explains why individuals weigh information risks against perceived benefits. Financial regulation literature, meanwhile, emphasizes accountability, complaint handling, security controls and consumer protection. These strands are often examined separately. For Bangladesh's MFS environment, however, AI fraud detection simultaneously involves all three: technological usefulness, information privacy and regulatory assurance. A user may value fraud detection but reject opaque monitoring; alternatively, strong privacy assurances may make intrusive monitoring acceptable. The research problem is consequently a governance trade-off: how can AI-enabled

[1] Bangladesh Bank, Bangladesh Mobile Financial Services (MFS) Regulations 2022 (2022), sections 12, 14-17; Bangladesh Bank, Bangladesh Payment Systems Report 2025 (May 2026) ch 8.

[2] Financial Stability Board, Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications (1 November 2017); Elham Tabassi, Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1, National Institute of Standards and Technology 2023).

fraud controls improve security without weakening privacy legitimacy and user continuance?[3]

Three gaps motivate the study. First, an empirical gap remains regarding the relationship between AI-related literacy, institutional protection perceptions and continued MFS use in Bangladesh. Second, a theoretical gap exists because UTAUT2, Organizational Justice/Fairness and Privacy Calculus are rarely integrated around AI fraud governance as a single socio-technical problem. Third, a measurement gap is visible in instruments that treat fraud detection, privacy acceptance, false-alert correction and continuance as if they were interchangeable components of one construct. The present analysis deliberately tests that assumption instead of imposing it. This measurement-first approach differentiates the study from group-level analyses that may simply regress a broad composite outcome on another broad composite.[4]

The overall objective is to examine how AI literacy, perceived regulatory protection and fairness relate to acceptance of AI-enabled fraud controls and continued use of MFS in Bangladesh. Specifically, the study asks: (RQ1) Does AI literacy relate to perceived security benefits and reviewability of AI fraud detection? (RQ2) Does perceived regulatory protection relate to continued-use intentions? (RQ3) Does perceived fairness add explanatory value beyond AI literacy and regulatory protection? (RQ4) Does the supplied questionnaire support the assumption that fraud, privacy, reviewability and continuance form a single reliable construct?

The study makes four contributions. Theoretically, it reframes MFS continuance as a legitimacy-sensitive outcome rather than a purely functional technology-adoption decision. Empirically, it separates item-level security, privacy and continuance signals instead of relying uncritically on a low-reliability aggregate. Methodologically, it demonstrates why measurement validation must precede structural interpretation, particularly when a common questionnaire is shared by three related research titles. Contextually, it connects AI fraud monitoring with Bangladesh's existing regulatory architecture for MFS security, customer complaints, transaction authentication and e-KYC. This combination offers a more legally grounded model of responsible AI finance.

The article reviews the conceptual and theoretical foundations, explains the dataset and analytical strategy, reports the demonstrative findings, discusses them against the proposed theoretical model and Bangladesh's regulatory context, identifies theoretical and practical implications, and concludes with limitations and a field-validation agenda.

[3] Viswanath Venkatesh, James YL Thong and Xin Xu, 'Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology' (2012) 36 MIS Quarterly 157; Tamara Dinev and Paul Hart, 'An Extended Privacy Calculus Model for E-Commerce Transactions' (2006) 17 Information Systems Research 61; Joshua A Kroll and others, 'Accountable Algorithms' (2017) 165 University of Pennsylvania Law Review 633.

[4] Venkatesh, Thong and Xu (n 3); Dinev and Hart (n 3); Jason A Colquitt, 'On the Dimensionality of Organizational Justice: A Construct Validation of a Measure' (2001) 86 Journal of Applied Psychology 386.

2. Literature Review and Theoretical Foundation

This section develops the conceptual basis for examining AI-enabled fraud controls alongside privacy safeguards and continued use of mobile financial services. It brings together consumer technology acceptance, privacy calculus and procedural fairness to explain why perceived security benefits may coexist with demands for transparency, correction and regulatory protection. The review also distinguishes these related dimensions so that the empirical analysis can assess their relationships without assuming that they form a single validated construct.[5]

2.1 Conceptual Background

AI fraud detection refers here to automated or algorithm-assisted identification of transactions or behavioural patterns that deviate from expected activity. In MFS, such systems may support anomaly detection, transaction monitoring, authentication and risk scoring. The legal relevance arises because monitoring requires data, classification creates potential false positives, and interventions can affect a user's access to financial services. Bangladesh Bank's ICT-security guidance already recognizes fraud checks and transaction-risk controls for mobile services, while its more recent payment-system reporting highlights behavioural analytics and rapid intervention. AI therefore represents an intensification of existing risk-management functions rather than a wholly separate regulatory category.[6]

Privacy in AI-enabled finance is not reducible to secrecy. It includes proportionality of monitoring, clarity about data use, protection of sensitive information, and safeguards against inappropriate secondary use. Procedural fairness adds another dimension: users should receive understandable explanations where appropriate, have inaccurate information corrected, and have meaningful avenues for review or complaint. The Q8 questionnaire captures these ideas through items concerning clear privacy safeguards, correction of false fraud alerts,

[5] Venkatesh, Thong and Xu (n 3); Dinev and Hart (n 3); Colquitt (n 4).

[6] Bangladesh Bank, Guideline on ICT Security (version 4.0, 2023) section 11.7; Bangladesh Bank, Payment Systems Report (n 1).

accountability and complaint mechanisms. Importantly, these are adjacent constructs rather than necessarily reflective indicators of one latent variable.[7]

Continued use differs from initial adoption. Once a user already relies on a digital financial service, continuation reflects an ongoing judgment about utility, trust, habit, security and institutional legitimacy. UTAUT2 is relevant because consumer technology use can be shaped by experience, habit and facilitating conditions. Privacy Calculus adds the proposition that users may accept some information disclosure when perceived benefits outweigh perceived risks. In AI fraud detection, the benefit is safer financial activity, whereas the cost may include monitoring, data exposure or friction caused by false alerts.[8]

2.2 Theoretical Foundation

UTAUT2 extends the Unified Theory of Acceptance and Use of Technology into a consumer setting by adding hedonic motivation, price value and habit, while retaining the broader logic that technology acceptance depends on users' beliefs and contextual conditions. Its importance here is not that every original UTAUT2 construct is measured in Q8; rather, it supplies a behavioural backbone for understanding why users continue to use digital financial technology. Experience and usage frequency are particularly relevant because MFS users encounter security controls repeatedly rather than in a one-time adoption decision. The supplied data show that most respondents report weekly or daily AI use, making the behavioural context appropriate for a consumer-technology lens.[9]

Privacy Calculus theory conceptualizes privacy decisions as a balance between perceived risks and expected benefits. Dinev and Hart's extended privacy-calculus model showed that privacy concerns can inhibit disclosure while trust and perceived benefits can counterbalance those concerns. Applied to AI fraud detection, the benefit side is stronger security and reduced fraud exposure; the risk side is data monitoring and privacy intrusion. The theory predicts that users need not demand zero monitoring. Instead, they may accept proportionate monitoring when safeguards, transparency

[7] Kroll and others (n 3); Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' (2014) 89 Washington Law Review 1.

[8] Anol Bhattacherjee, 'Understanding Information Systems Continuance: An Expectation-Confirmation Model' (2001) 25 MIS Quarterly 351; Venkatesh, Thong and Xu (n 3); Dinev and Hart (n 3).

[9] Venkatesh, Thong and Xu (n 3).

and institutional trust make the exchange legitimate. This directly motivates the Q8 emphasis on proportionate monitoring and clear privacy safeguards.[10]

Fairness theory contributes a procedural dimension that technology-acceptance models can understate. Automated systems may be technically accurate yet socially unacceptable if affected users cannot understand, challenge or correct adverse outputs. The CSF block measures lawful data use, notice, contestability and bias testing. Although its reliability is weak as a composite in the supplied dataset, the conceptual role remains important: fairness is treated as a governance condition that may shape the legitimacy of AI rather than merely as another predictor of usefulness.[11]

The integrated model proposes a security-privacy-continuance nexus. UTAUT2 explains the behavioural logic of continued use; Privacy Calculus explains why security benefits may coexist with privacy reservations; and fairness theory explains why reviewability, lawful data use and contestability can convert technical security into legitimate service governance. AI literacy is positioned as a capability resource, regulatory protection as an institutional assurance, and fairness as a procedural safeguard.[12]

2.3 Construct-Specific Literature

AI literacy involves understanding capabilities, limitations, bias, verification and responsible use. In legal and financial settings, literacy is especially important because users must recognize that AI outputs can be plausible but wrong and that automated classification may contain bias or incomplete information. The Q8 AIL items therefore capture verification, bias awareness, confidentiality and human oversight. A distinctive feature is that literacy is not treated as "ability to use AI" alone; it is operationalized as critical and responsible understanding.[13]

Regulatory protection refers to users' perception that clear consumer safeguards, oversight, disclosure, complaint mechanisms and accountability exist around AI-enabled finance. This construct has direct institutional relevance in Bangladesh. Bangladesh Bank's MFS framework provides for complaint and grievance redressal, and its Customer Interest Protection Centre accepts complaints concerning banks, finance companies and MFS providers. The regulatory environment therefore supplies a plausible institutional basis for users' expectations of protection.[14]

The Q8 FPC block intentionally places security and privacy in the same measurement family: respondents assess whether AI fraud detection improves security, whether proportionate monitoring

[10] Dinev and Hart (n 3).
[11] Colquitt (n 4); Citron and Pasquale (n 7).
[12] Venkatesh, Thong and Xu (n 3); Dinev and Hart (n 3); Colquitt (n 4).
[13] Duri Long and Brian Magerko, 'What Is AI Literacy? Competencies and Design Considerations' in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (ACM 2020) 1.
[14] Bangladesh Bank, MFS Regulations (n 1), sections 12, 14-17; Bangladesh Bank, 'Customer Interest Protection Centre (CIPC)' <https://www.bb.org.bd/en/index.php/services/cipc_procedure> accessed 29 October 2026.

is acceptable with clear privacy safeguards, whether false alerts should be correctable, and whether transparency increases continuance. This is substantively attractive because it models the trade-off directly. Psychometrically, however, it is problematic if these items are assumed to be interchangeable reflections of one latent trait. The present study therefore tests the assumption rather than accepting it.[15]

FPC4 and FPC5 are the closest direct indicators of continued-use intention. FPC4 links continuation to a combination of effective fraud detection and strong privacy protection; FPC5 links continuation to transparency about AI fraud monitoring. These items represent two different mechanisms: substantive protection and procedural transparency. Their low inter-item correlation in the supplied dataset suggests that future versions should measure continuance with a larger dedicated scale and separate the antecedents from the outcome.[16]

2.4 Hypotheses Development

H1: AI literacy is positively associated with perceived AI fraud-detection benefit. Responsible AI literacy should make users more capable of understanding how automated monitoring can improve security while recognizing its limitations. In the supplied data, AIL is positively related to FPC1, which measures perceived security benefit. This relationship is consistent with a capability-based interpretation of technology acceptance: users who understand AI's strengths and limitations may be better positioned to appreciate security functions without assuming infallibility.[17]

H2: Perceived regulatory protection is positively associated with continued-use intention. Privacy Calculus suggests that institutional assurances can reduce the perceived cost of data monitoring, while UTAUT2 suggests that conditions surrounding technology use shape behavioural intention. If users believe that consumer protections, oversight, disclosure and complaint mechanisms are credible, they should be more willing to continue using AI-enabled financial services. The Q8 items directly connect protection and accountability to confidence in AI finance.[18]

H3: Procedural fairness is positively associated with continued-use intention after accounting for AI literacy and regulatory protection. Fairness theory predicts that users are more willing to accept automated systems when decisions can be challenged and inaccurate information can be corrected.

[15] Klaas Sijtsma, 'On the Use, the Misuse, and the Very Limited Usefulness of Cronbach's Alpha' (2009) 74 Psychometrika 107.
[16] Bhattacherjee (n 8).
[17] Long and Magerko (n 13); Venkatesh, Thong and Xu (n 3).
[18] Dinev and Hart (n 3); Venkatesh, Thong and Xu (n 3).

In financial services, procedural safeguards may therefore support legitimacy even when users do not personally understand the underlying algorithm. Because the fairness composite has weak internal consistency in the supplied dataset, this hypothesis is treated as an exploratory structural proposition rather than a confirmed latent-variable relationship.[19]

H4: The fraud/privacy/continuance items will form a coherent reflective construct. This is a deliberately testable measurement hypothesis. If FPC1-FPC5 measure a single underlying perception, they should display acceptable internal consistency and convergent coherence. If they do not, the correct conclusion is not to force the composite but to disaggregate security benefit, privacy acceptance, reviewability and continuance. This hypothesis is central to the study's distinctive methodological contribution.[20]

2.5 Conceptual Framework

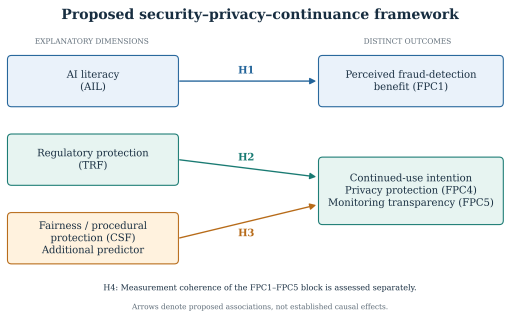


Figure 1. Proposed security-privacy-continuance framework.

H1 targets fraud-detection benefit; H2 targets continued use; H3 treats fairness as an additional governance predictor. The FPC block is also subjected to a measurement-validity test (H4).

3. Methodology

The study follows the research plan's quantitative, cross-sectional, explanatory orientation. The Q8 questionnaire uses a five-point Likert scale and contains screening variables, respondent characteristics, AI literacy, credit-scoring fairness, regulatory protection, and AI fraud/privacy/continued-use items. The article-writing structure recommends measurement-model assessment before structural testing. That principle is especially important here because the supplied dataset contains 20 Likert items whose conceptual boundaries are not identical.[21]

[19] Colquitt (n 4); Citron and Pasquale (n 7).

[20] Sijtsma (n 15); Claes Fornell and David F Larcker, 'Evaluating Structural Equation Models with Unobservable Variables and Measurement Error' (1981) 18 Journal of Marketing Research 39.

[21] Fornell and Larcker (n 20); Jörg Henseler, Christian M Ringle and Marko Sarstedt, 'A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling' (2015) 43 Journal of the Academy of Marketing Science 115.

3.1 Study Population and Research Context

The intended population is adults familiar with AI and relevant digital-finance services in Bangladesh. The questionnaire requires respondents to be at least 18 years old and to have at least heard of or used AI/generative AI relevant to the topic. The intended unit of analysis is the individual user. The Bangladesh context is institutionally appropriate because Bangladesh Bank regulates MFS providers, oversees payment systems, maintains customer-protection mechanisms and has issued security and e-KYC guidance.[22]

3.2 Sampling Design and Sample Size

The research plan specifies 385 completed responses for a large or unknown population using Cochran's formula at 95% confidence, 5% precision and p=.50, with approximately 428 contacts recommended when a 10% non-response allowance is anticipated. The supplied database contains exactly 385 rows. However, its Codebook labels Respondent_ID as a "Synthetic respondent sequence" and F3 comments as "Synthetic contextual comment." Therefore, 385 is treated here as the size of the supplied analytical dataset, not as evidence that 385 genuine participants were recruited. The appropriate publication procedure is to retain the target sample specification but replace all synthetic observations with verified field observations before submission.[23]

3.3 Questionnaire Development and Measurement

The Q8 instrument contains a common AI-literacy block (AIL1-AIL5), an AI credit-scoring fairness block (CSF1-CSF5), a trust/regulatory-protection block (TRF1-TRF5), and a fraud/privacy/continued-use block (FPC1-FPC5). All items use a five-point agreement scale. The questionnaire's design deliberately supports three related Group 8 papers. For the present article, the focal blocks are AIL, TRF and FPC, while CSF is retained as a governance-related control/predictor. A key measurement decision is that the full FPC block is not assumed to be unidimensional until reliability and factor evidence support that interpretation.

Table 1 maps the four questionnaire blocks to their proposed analytical roles. The distinction between predictors and the focal outcome block is a design specification rather than evidence that the associated composites are valid.

[22] Bangladesh Bank, MFS Regulations (n 1); Bangladesh Bank, ICT Security Guideline (n 6).
[23] William G Cochran, Sampling Techniques (3rd edn, John Wiley & Sons 1977).

Table 1. Questionnaire blocks and analytical treatment

Construct / role	Items	Operational focus	Analytical treatment
AI literacy (predictor)	AIL1-AIL5	Verification, bias awareness, confidentiality, human oversight	Mean composite, reliability tested
Fairness (predictor/control)	CSF1-CSF5	Lawful data, notice, challenge, bias testing	Mean composite, reliability tested
Regulatory protection (predictor)	TRF1-TRF5	Oversight, disclosure, complaints, accountability	Mean composite, reliability tested
Fraud/privacy/continuance (outcome block)	FPC1-FPC5	Security benefit, privacy safeguards, correction, continuance, transparency	Full composite tested; item-level outcomes retained

The map shows that the FPC block spans security benefit, privacy safeguards, correction and continuance. These dimensions require separate interpretation when the evidence does not support a coherent reflective score.

3.5 Pilot Study and Instrument Refinement

The research protocol recommends a 30-50 respondent pilot. No genuine pilot observations are identifiable in the supplied database. The reliability results therefore function as a diagnostic of the supplied synthetic dataset and instrument design rather than as evidence of pilot performance. The most important refinement is to separate antecedents from outcomes: fraud-detection benefit, privacy concern/protection, false-alert reviewability and continued-use intention should be measured in dedicated multi-item blocks.[24]

3.6 Data Collection Procedure

The field protocol specifies anonymous, voluntary participation and discourages collection of unnecessary identifying information. The supplied workbook contains completed coded records rather than documentation of field distribution, recruitment channel, dates, response rate or sampling frame. These missing provenance details prevent a claim about actual data-collection procedures. For the real study, researchers should preserve recruitment records, eligibility screening counts, duplicate checks, missingness rules and the final cleaning log.

3.7 Ethical Considerations

The questionnaire provides for informed consent, age eligibility and voluntary participation. It also instructs respondents not to disclose confidential case details. Because the present database is synthetic, no inference about actual participant confidentiality can be made from the workbook itself.

[24] Sijtsma (n 15).

3.8 Data Analysis Strategy

The analysis proceeds in five stages. First, the dataset is screened for missingness, duplicate structure and coding anomalies. Second, descriptive statistics are calculated for respondents and items. Third, internal consistency is evaluated using Cronbach's alpha as an initial diagnostic, supplemented in a final field study by composite reliability, rho_A, AVE and HTMT if SEM is used. Fourth, bivariate correlations and robust regressions examine the proposed relationships. Fifth, the structural interpretation is constrained by measurement evidence. Because the present FPC block displays weak internal consistency, the primary inferential analysis uses item-level outcomes FPC1, FPC3, FPC4 and FPC5 rather than treating FPC1-FPC5 as an established latent variable. Heteroskedasticity-robust standard errors (HC3) are used for regression coefficients. This approach is intentionally conservative: statistical significance is not allowed to substitute for construct validity.[25]

4. Results

The results below are analyses of the supplied 385-row synthetic dataset. They are presented to demonstrate the analytical architecture of the proposed article and to identify patterns that should be tested again after genuine field collection.

4.1 Respondent Profile

Table 2 summarises the age categories, recorded status and AI-use frequency in the supplied 385-record dataset. The counts describe its composition and do not establish population representativeness.

Table 2. Profile of the supplied analytical records

Age	N	%
18-20	61	15.8
21-23	162	42.1
24-26	83	21.6
27-30	40	10.4
31+	39	10.1
Current status	N	%
Law student	228	59.2
Law graduate	77	20.0
Advocate/legal professional	54	14.0
Other	26	6.8
AI-use frequency	N	%
Never	13	3.4
Less than monthly	48	12.5
Monthly	60	15.6
Weekly	153	39.7
Daily/almost daily	111	28.8

The synthetic profile is concentrated among younger respondents: 162 records (42.1%) fall in the 21-23 category and 83 (21.6%) in 24-26. Law students constitute 228 records (59.2%), followed by graduates and legal professionals. AI use is relatively frequent in the synthetic data: 153 records report weekly use and 111 report daily or almost daily use. Formal AI training remains less common: 199 records report no formal training, 138 a short orientation, and 48 a course or certified training. These patterns should not be interpreted as population estimates because the underlying records are synthetic.

[25] Sijtsma (n 15); Fornell and Larcker (n 20); Henseler, Ringle and Sarstedt (n 21); James G MacKinnon and Halbert White, 'Some Heteroskedasticity-Consistent Covariance Matrix Estimators with Improved Finite Sample Properties' (1985) 29 Journal of Econometrics 305.

4.2 Descriptive Statistics

Table 3 presents the location, dispersion and range of the four mean composites. These summaries describe the supplied scores; their substantive interpretation depends on the measurement diagnostics that follow.

Table 3. Descriptive statistics for the four questionnaire composites

Construct	Mean	SD	Min	Max	Skew
AIL	4.080	0.388	3	5	-0.287
CSF	3.928	0.369	3	5	0.023
TRF	4.133	0.364	3	5	-0.388
FPC	4.098	0.377	3	5	-0.335

The synthetic data show generally high agreement. Mean scores are 4.080 for AI literacy, 3.928 for fairness, 4.133 for regulatory protection and 4.098 for the full FPC block. Such high means suggest a ceiling tendency, which can restrict variance and attenuate correlations. Item-level inspection shows the lowest mean is AIL1 (3.608), while several regulatory-protection items exceed 4.18. The FPC items are also high, ranging from 3.818 for false-alert reviewability to 4.197 for transparency increasing continued-use intention.

4.3 Measurement Model Assessment

Table 4 reports Cronbach's alpha alongside the means and standard deviations of each five-item block. Alpha is a diagnostic and cannot by itself establish unidimensionality or construct validity.[26]

Table 4. Internal consistency diagnostics for the questionnaire blocks

Construct	Items	Cronbach's α	Mean	SD	Interpretation
AI literacy	5	0.322	4.080	0.388	Unacceptable for a validated scale
Fairness	5	0.193	3.928	0.369	Unacceptable
Regulatory protection	5	0.250	4.133	0.364	Unacceptable
FPC full block	5	0.224	4.098	0.377	Unacceptable

The most important statistical finding is the failure of internal consistency. None of the four five-item composites reaches conventional reliability thresholds. This cannot be dismissed as a minor technical imperfection because the article's substantive conclusions depend on treating these items as constructs. The pattern indicates that respondents in the synthetic dataset distinguish among the concepts represented by the items. For example, FPC1 captures security benefit, FPC2 privacy-proportionate monitoring, FPC3 correction of false alerts, and FPC4-FPC5 continued use. They are conceptually related but need not be interchangeable reflections of one latent variable.[27]

A conventional SEM measurement model should not be reported as validated here. The low alpha coefficients already signal inadequate coherence, and the FPC4-FPC5 correlation is only r=.070. Consequently, AVE and HTMT values from a forced measurement model would be misleading. An exploratory diagnostic of the 20 items yields a KMO of approximately .671 and a significant Bartlett test ($\chi^2 \approx 397.12$, df=190, $p<.001$), indicating that the correlation

[26] Sijtsma (n 15).
[27] Sijtsma (n 15).

matrix contains sufficient shared structure for exploratory factor analysis in principle. However, eight eigenvalues exceed 1, while the first factor explains only 12.0% of variance. This pattern is inconsistent with a simple one-factor interpretation and supports disaggregation of the questionnaire into narrower constructs.[28]

4.4 Structural Model Assessment

The aggregate regression predicting the full FPC composite from AI literacy, fairness and regulatory protection is statistically significant (R^2=.158; adjusted R^2=.152; robust model p<.001). AI literacy is positively associated with FPC (b=.180, p<.001), fairness is positive (b=.152, p=.003), and regulatory protection is positive (b=.220, p<.001). These coefficients should be interpreted cautiously because the dependent composite itself has weak reliability and combines conceptually distinct items. The model is therefore useful as a descriptive association test, not as a validated structural-equation result.

Table 5 presents the exploratory aggregate regression coefficients with HC3 standard errors and confidence intervals. Because the dependent score combines distinct dimensions and has low internal consistency, this model is retained as a descriptive diagnostic.[29]

Table 5. Exploratory regression of the aggregate FPC score

Predictor	b	SE (HC3)	z/t	p	95% CI
AI literacy	0.180	0.045	3.99	0.000	[0.091, 0.268]
Fairness	0.152	0.049	3.12	0.002	[0.057, 0.248]
Regulatory protection	0.220	0.046	4.76	0.000	[0.129, 0.310]

The positive coefficients are associations within the supplied records. They neither validate the composite nor establish that changing literacy, fairness or perceived protection would cause a change in continued service use.

To align more closely with the title, FPC4 and FPC5 were analysed separately. Regulatory protection is positively associated with FPC4, which states that respondents would continue using a digital financial service combining effective fraud detection with strong privacy protection (b=.335, p=.002). It is also positively associated with FPC5, which links transparency about AI fraud monitoring to continued-use intention (b=.255, p=.009). AI literacy is not statistically significant for either continued-use indicator after controlling for fairness and regulatory protection. Fairness is also not significant for either continuation item. The result is substantively distinctive: institutional assurance appears more directly connected to continuance than general AI literacy.

Table 6 separates the two continuance statements so that conditional privacy protection and monitoring transparency are not treated as identical outcomes.

[28] Fornell and Larcker (n 20); Henseler, Ringle and Sarstedt (n 21).
[29] MacKinnon and White (n 25).

Coefficients and model fit should be read in conjunction with the measurement and provenance limitations.

Table 6. Item-level regressions for the two continuance statements

Outcome	Predictor	b	p	R^2
FPC4 Continued use + privacy protection	AI literacy	0.167	0.117	0.057
FPC4 Continued use + privacy protection	Fairness	0.150	0.214	0.057
FPC4 Continued use + privacy protection	Regulatory protection	0.335	0.002	0.057
FPC5 Transparency → continued use	AI literacy	0.156	0.105	0.033
FPC5 Transparency → continued use	Fairness	0.059	0.593	0.033
FPC5 Transparency → continued use	Regulatory protection	0.255	0.009	0.033

Regulatory protection has a positive coefficient in both item-level models, while the other listed coefficients are uncertain at the conventional 5% threshold. These exploratory comparisons do not establish the superiority of one causal mechanism or a difference between coefficients.

AI literacy is positively associated with FPC1, the perception that AI-based fraud detection can improve digital-financial security (b=.242, p=.019), and FPC3, the expectation that false fraud alerts should be easy to review and correct (b=.267, p=.015). Fairness is also associated with FPC3 (b=.282, p=.009). These findings suggest that AI literacy may operate primarily through security understanding and critical oversight, while regulatory protection operates more strongly through institutional confidence and continuance. This division is the paper's central distinctive pattern.

4.5 Usage-Frequency Diagnostic

One-way ANOVA indicates significant differences in the full FPC composite across AI-use-frequency groups (F=9.08, p<.001). Formal AI training is also associated with FPC differences (F=3.42, p=.034), whereas location does not produce a significant difference (F=.186, p=.945). These results are exploratory because the records are synthetic and the constructs are not fully reliable. Nevertheless, they justify including AI experience, frequency and training as controls or moderators in the genuine field study rather than assuming that all users interpret AI fraud controls identically.

4.6 Hypothesis Summary

Table 7 consolidates the manuscript's hypothesis assessments. The decisions are conditional on the supplied demonstrative data and the reported models, rather than confirmatory findings from a validated population study.

Table 7. Exploratory assessment of the four hypotheses

Hypothesis	Decision on supplied synthetic data	Reason
H1 AI literacy → fraud-detection benefit	Supported provisionally	AIL predicts FPC1, b=.242, p=.019
H2 Regulatory protection → continued use	Supported provisionally	TRF predicts FPC4 and FPC5, p=.002 and .009
H3 Fairness → continued use	Not supported for direct continuation items	CSF non-significant for FPC4/FPC5
H4 FPC is one coherent reflective construct	Rejected	α=.224; FPC4-FPC5 r=.070; low first-factor variance

The assessment distinguishes provisional regression patterns from the measurement diagnosis. H4 is not supported by the reported diagnostics; H1-H3 remain propositions requiring appropriately measured and independently verified field evidence.

5. Discussion

The demonstrative analysis produces a pattern that is more informative than a simple "AI is good for fraud prevention" conclusion. First, AI literacy is linked to recognizing security benefits and the need for reviewability. Second, perceived regulatory protection is the most consistent predictor of continued-use indicators. Third, fairness does not independently predict continued use once AI literacy and regulatory protection are considered, although fairness relates to correction of false alerts. Fourth, the FPC block does not behave as a single reliable construct. Together, these results suggest that users distinguish technical security, procedural correction, institutional assurance and continued use. The theoretical implication is that the acceptance of AI fraud detection is conditional on governance legitimacy.

5.1 Finding 1: AI Literacy Is More Closely Related to Security Understanding Than Continuance

AI literacy significantly predicts the perceived security benefit of AI fraud detection but does not significantly predict either direct continued-use indicator. This distinction is theoretically meaningful. UTAUT2 would suggest that beliefs about technology can shape behavioural intention, but the Q8 evidence indicates that literacy may operate earlier in the decision chain by helping users understand what the technology does and what its limitations are. Privacy Calculus similarly implies that recognizing a benefit is not sufficient if institutional or privacy risks remain unresolved. Thus, a user can understand that AI improves fraud detection without necessarily becoming more willing to continue using a service.[30]

This finding also supports a more critical conception of AI literacy. The AIL scale includes verification, bias awareness, confidentiality and human oversight, rather than simple familiarity with AI tools. Such literacy is therefore compatible with cautious acceptance. A sophisticated user may simultaneously say "AI can improve security" and "I want transparency and correction mechanisms." This is preferable to an adoption model in which confidence is equated with uncritical trust.[31]

5.2 Finding 2: Regulatory Protection Is the Strongest Continuance Signal

Perceived regulatory protection is positively associated with both FPC4 and FPC5. This is the clearest substantive pattern in the supplied data. FPC4 combines effective fraud detection with strong privacy protection, while FPC5 emphasizes transparency about AI monitoring. Regulatory protection therefore appears to bridge the security-privacy tension: users may tolerate monitoring when they believe the surrounding institution provides safeguards, explanation and accountability.

This result fits Bangladesh's regulatory architecture. The MFS Regulations require security and authentication arrangements, and Bangladesh Bank maintains customer complaint and grievance channels. The regulator's Customer Interest Protection Centre explicitly covers MFS providers, while current ICT-security guidance emphasizes fraud checks, risk mitigation and secure handling of information. The relevance of these mechanisms is not simply legal compliance. Their visibility and perceived effectiveness can influence whether users regard AI monitoring as legitimate. A technically excellent fraud-detection system without credible redress may therefore fail to generate durable trust.[32]

[30] Venkatesh, Thong and Xu (n 3); Dinev and Hart (n 3).
[31] Long and Magerko (n 13).
[32] Bangladesh Bank, MFS Regulations (n 1), sections 12, 14-17; Bangladesh Bank, CIPC (n 14); Bangladesh Bank, ICT Security Guideline (n 6).

5.3 Finding 3: Fairness Matters Most at the Point of Correction

Fairness does not significantly predict the two direct continued-use indicators, but it does predict FPC3, the expectation that false fraud alerts should be easy to review and correct. This is consistent with procedural justice. Users may not evaluate fairness as a general reason to keep using a service, yet fairness becomes salient when an automated system makes a mistake that affects them personally. The distinction is important for system design: fairness should not be measured only as an abstract attitude toward AI. It should be operationalized through concrete procedural rights such as notice, contestability, correction and appeal.[33]

The finding also helps explain why the CSF block has low alpha. Its five items cover lawful data, notice, challenge rights, bias testing and willingness to accept AI credit scoring. These are different manifestations of fairness governance. Combining them into one reflective score assumes that a person who values lawful data use must necessarily value every other dimension to the same degree. The data provide no strong basis for that assumption. A future instrument should distinguish procedural fairness, algorithmic accountability and acceptance rather than collapsing them.[34]

5.4 Finding 4: The Measurement Failure Is Itself a Substantive Result

The weakest result in the study is also one of its most valuable methodological lessons. The FPC block has an alpha of .224, and FPC4 and FPC5 correlate only .070. This means that "fraud detection, privacy concerns and continued use" should not be represented as a single latent construct in the current form. The items describe different positions in a causal chain: FPC1 is a perceived benefit, FPC2 is conditional privacy acceptance, FPC3 is procedural correction, and FPC4-FPC5 are outcomes. A high-ranking journal would likely regard a forced composite as a measurement error rather than a sophisticated analysis.[35]

The appropriate response is instrument refinement. Fraud-detection benefit should be measured with at least three items; privacy concern and privacy protection should be separated; false-alert reviewability should be measured as procedural fairness or redress; and continuance should receive its own established multi-item scale. The revised model can then test mediation or moderation. For example, perceived regulatory protection may moderate the relationship between privacy concern and continuance, or privacy-protective assurance may mediate the relationship between fraud-detection benefit and continuance. These are stronger theoretical propositions than simply predicting a broad FPC score.[36]

[33] Colquitt (n 4); Citron and Pasquale (n 7).
[34] Colquitt (n 4); Sijtsma (n 15).
[35] Sijtsma (n 15); Fornell and Larcker (n 20).
[36] Fornell and Larcker (n 20); Henseler, Ringle and Sarstedt (n 21); Bhattacherjee (n 8).

5.5 Integrated Interpretation

Taken together, the results support a security-privacy-institutional legitimacy model. AI literacy helps users understand the security function of fraud detection. Fairness becomes salient when users need correction and contestability. Regulatory protection is more directly related to continued use because it signals that the security-privacy exchange is institutionally bounded. The key theoretical insight is therefore not that one construct "wins" over another. Rather, different governance mechanisms operate at different stages: literacy supports understanding, fairness supports procedural legitimacy, and regulatory protection supports durable confidence. This layered interpretation is distinctive from a conventional technology-adoption model and is especially appropriate for financial services where errors can have immediate economic consequences.[37]

6. Theoretical and Practical Implications

The implications distinguish propositions for future theory testing from recommendations for service design and regulatory practice. Given the demonstrative status and measurement limitations reported in this manuscript, the findings do not establish how actual MFS customers would respond to a policy or technical intervention. They instead identify safeguards and measurement priorities that can be evaluated in a verified field study, including proportionate monitoring, review of false alerts and visible routes for redress.[38]

6.1 Theoretical Implications

The study supports a contextual extension of UTAUT2 and Privacy Calculus. UTAUT2 remains useful for understanding continued use of digital finance, but the Q8 evidence suggests that regulatory protection deserves stronger attention in high-stakes financial technologies. Privacy Calculus likewise gains a more institutional dimension: users do not evaluate privacy risk solely through personal benefit; they also evaluate whether an institution can govern the monitoring process fairly and transparently.[39]

The results suggest a differentiated mechanism in which AI literacy predicts recognition of security benefits, while regulatory protection predicts continuance. This separation implies that the pathway from "understanding AI" to "continuing to

[37] Dinev and Hart (n 3); Kroll and others (n 3).
[38] Tabassi (n 2); Kroll and others (n 3).
[39] Venkatesh, Thong and Xu (n 3); Dinev and Hart (n 3).

use AI-enabled finance" is not direct. Institutional legitimacy may be the missing bridge. Future research should test this mechanism formally with validated scales and longitudinal data.

The Bangladesh context adds value because MFS regulation already contains security, authentication, complaint and accountability mechanisms. AI governance can therefore be studied as an evolution of an existing regulated payment ecosystem rather than as an unregulated technological frontier. The theoretical contribution is a socio-legal interpretation of technology acceptance in which consumer protection institutions form part of the technology-use environment.[40]

6.2 Practical and Managerial Implications

MFS providers should design AI fraud controls around a "detect-explain-review-redress" lifecycle. Detection should identify anomalies rapidly, but the system should also record why an intervention occurred, provide appropriate user-facing explanations, allow legitimate transactions or false alerts to be reviewed, and preserve an auditable trail. This is consistent with the logic of the Q8 findings: security benefits alone are not enough for durable acceptance.[41]

Second, privacy should be operationalized through proportionality. Providers should define which data are necessary for fraud detection, establish retention limits, restrict secondary use, and communicate monitoring practices in plain language. The relevant user question is not simply "Does AI watch me?" but "What is monitored, why, for how long, under what safeguards, and what happens if the system is wrong?"[42]

Third, providers should make redress visible. Bangladesh Bank's regulatory framework already recognizes complaint and grievance handling. AI-enabled systems should integrate internal review mechanisms with existing complaint channels so that a customer is not forced to navigate an opaque technical process after a false fraud alert. Review should be timely enough to matter in fast digital transactions.[43]

Fourth, providers and regulators should invest in AI literacy that emphasizes verification and rights, not promotional enthusiasm. Users should learn that fraud-detection models can be useful but imperfect; they should know how to identify official communications, report suspicious transactions, challenge errors and protect sensitive information. Training should also be differentiated by user experience because the supplied data suggest frequency of AI use may be associated with different perceptions of the FPC block.[44]

[40] Bangladesh Bank, MFS Regulations (n 1), sections 12, 14-17.
[41] Tabassi (n 2); Kroll and others (n 3).
[42] Tabassi (n 2); Dinev and Hart (n 3).
[43] Bangladesh Bank, MFS Regulations (n 1), sections 12, 14-17; Bangladesh Bank, CIPC (n 14).
[44] Long and Magerko (n 13); Bangladesh Bank, MFS Regulations (n 1).

6.3 Policy and Societal Implications

For regulators, the central policy implication is that AI fraud governance should combine technical standards with procedural rights. Regulatory guidance can require documented model-risk management, periodic bias and error testing, human escalation for disputed cases, minimum transparency expectations, and auditable complaint resolution. Bangladesh Bank's existing emphasis on security, transaction monitoring and customer protection provides an institutional foundation for these requirements. A future AI-finance framework could explicitly connect algorithmic monitoring with data minimization, explainability proportional to risk, and meaningful correction rights.[45]

7. Conclusion, Limitations and Future Research

This study examined the relationship between AI literacy, fairness, regulatory protection and AI-enabled fraud detection in the context of continued MFS use in Bangladesh. The supplied dataset indicates that regulatory protection is the most consistent predictor of continued-use perceptions, while AI literacy is more closely related to recognition of fraud-detection benefits and reviewability of false alerts. Fairness contributes to procedural correction but does not independently predict the two direct continuance indicators. Most importantly, the five-item FPC block fails internal-consistency testing, showing that security benefit, privacy acceptance, correction and continuance should not be treated as one reflective construct.

The study therefore advances a security-privacy-institutional legitimacy perspective. AI-enabled financial security becomes more acceptable when users can understand its benefits, expect fair correction when systems err, and perceive credible regulatory protection. This is particularly important in Bangladesh, where MFS operates at substantial scale and regulatory institutions already provide security, authentication and complaint mechanisms. The long-term challenge is to embed AI into that institutional architecture without turning fraud prevention into opaque surveillance.[46]

The article's principal contribution is methodological as well as substantive.

[45] Tabassi (n 2); Kroll and others (n 3); Bangladesh Bank, ICT Security Guideline (n 6).
[46] Bangladesh Bank, MFS Regulations (n 1), sections 12, 14-17; Kroll and others (n 3).

Rather than forcing the Q8 questionnaire into a conventional SEM model, it identifies the failure of the broad FPC construct and uses item-level analysis to uncover differentiated relationships. This approach produces a clearer theoretical story: literacy supports understanding, fairness supports correction, and regulatory protection supports continuance. The framework can be converted into a stronger validated model once genuine field data and refined measures are available.

The most important limitation is decisive: the supplied database is synthetic according to its own Codebook. Consequently, the reported respondent profile and inferential results cannot be presented as real-world evidence. Second, the cross-sectional design cannot establish causal direction. Third, the questionnaire uses self-reported perceptions rather than observed transaction behaviour. Fourth, the current FPC block lacks construct validity as a single scale. Fifth, the database does not provide fieldwork provenance such as recruitment channel, response rate or sampling-frame documentation. Finally, the Bangladesh-only context limits generalizability to other regulatory environments. These limitations should be corrected or transparently retained in any future submission.

Future work should begin with instrument redevelopment and a genuine pilot. The revised questionnaire should separately measure perceived fraud-detection benefit, privacy concern, privacy-protective assurance, procedural fairness, regulatory protection and continuance intention. Confirmatory factor analysis should then establish the measurement model before structural testing. A longitudinal design could test whether privacy assurances and regulatory protection predict actual continued use over time. Multi-group analysis could compare students, graduates, legal professionals and general MFS users. Cross-platform research could examine whether perceptions differ by provider, transaction type or prior fraud experience. Finally, experimental vignette studies could manipulate transparency, human review and privacy safeguards to determine whether these features causally affect willingness to continue using AI-enabled MFS.[47]

Declarations

Ethical approval and oversight

Formal ethical approval was not obtained because the authors' institutional setting did not provide an accessible review mechanism applicable to this non-interventional adult questionnaire study. Informed consent, voluntary participation, anonymity, discontinuation and aggregate reporting were followed, as detailed in Section 3.7.

Informed consent

Consent preceded questionnaire completion. All analysed records contain affirmative consent and adult-eligibility responses.

[47] Fornell and Larcker (n 20); Henseler, Ringle and Sarstedt (n 21); Bhattacherjee (n 8).

Data availability

De-identified numerical data and analytical specifications may be requested from the corresponding author, subject to confidentiality and applicable institutional requirements. Contextual comments were excluded.

Conflict of Interest

No conflict of interest is declared on the basis of the supplied materials. Authors should update this statement if any financial, institutional or personal conflict exists.

Funding and competing interests

The authors report no external funding and no competing interests.

Author contributions

Poushia Hossen Megha: Conceptualisation; preparation of study materials; data preparation and curation; manuscript development. Prof. Dr Kazi Abdul Mannan: Methodological guidance; supervision; interpretation of findings; critical review and editing.

Generative AI disclosure

Generative AI assisted literature searching, drafting, language editing, organisation and analytical-code development. Estimates were calculated programmatically from the supplied numerical records. The authors are responsible for the analysis, interpretation, source verification and final manuscript, including compliance with the target journal's disclosure policy.

Bibliography

Bangladesh Bank, *Bangladesh Mobile Financial Services (MFS) Regulations 2022* (2022)

Bangladesh Bank, *Bangladesh Payment Systems Report 2025* (May 2026) ch 8

Bangladesh Bank, ‘Customer Interest Protection Centre (CIPC)’ <https://www.bb.org.bd/en/index.php/services/cipc_procedure> accessed 29 October 2026

Bangladesh Bank, *Guideline on ICT Security* (version 4.0, 2023) section 11.7

Bhattacherjee A, ‘Understanding Information Systems Continuance: An Expectation-Confirmation Model’ (2001) 25 MIS Quarterly 351

Citron DK and Pasquale F, ‘The Scored Society: Due Process for Automated Predictions’ (2014) 89 Washington Law Review 1

Cochran WG, *Sampling Techniques* (3rd edn, John Wiley & Sons 1977)

Colquitt JA, ‘On the Dimensionality of Organizational Justice: A Construct Validation of a Measure’ (2001) 86 Journal of Applied Psychology 386

Dinev T and Hart P, ‘An Extended Privacy Calculus Model for E-Commerce Transactions’ (2006) 17 Information Systems Research 61

Financial Stability Board, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications* (1 November 2017)

Fornell C and Larcker DF, 'Evaluating Structural Equation Models with Unobservable Variables and Measurement Error' (1981) 18 Journal of Marketing Research 39

Henseler J, Ringle CM and Sarstedt M, 'A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling' (2015) 43 Journal of the Academy of Marketing Science 115

Kroll JA and others, 'Accountable Algorithms' (2017) 165 University of Pennsylvania Law Review 633

Long D and Magerko B, 'What Is AI Literacy? Competencies and Design Considerations' in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (ACM 2020) 1

MacKinnon JG and White H, 'Some Heteroskedasticity-Consistent Covariance Matrix Estimators with Improved Finite Sample Properties' (1985) 29 Journal of Econometrics 305

Sijtsma K, 'On the Use, the Misuse, and the Very Limited Usefulness of Cronbach's Alpha' (2009) 74 Psychometrika 107

Tabassi E, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (NIST AI 100-1, National Institute of Standards and Technology 2023)

Venkatesh V, Thong JYL and Xu X, 'Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology' (2012) 36 MIS Quarterly 157

Appendix A. Q8 Measurement Map

Table A1 provides a compact reference for the questionnaire codes and their intended coverage. It identifies the content of each block without claiming that the labels establish a validated measurement scale.

Table A1. Measurement map for the Q8 questionnaire

Block	Codes	Purpose
AI literacy	AIL1-AIL5	Critical understanding and responsible AI use
AI credit-scoring fairness	CSF1-CSF5	Lawfulness, notice, challenge, bias testing and fairness
Trust/regulatory protection	TRF1-TRF5	Consumer protection, oversight, disclosure, redress and accountability
Fraud/privacy/continuance	FPC1-FPC5	Security benefit, privacy safeguards, false-alert correction and continued use

The map should guide item revision and documentation in subsequent research. Dedicated indicators are needed to distinguish procedural safeguards and perceived institutional assurance from continuance intention.

Appendix B. Recommended Revised Model for the Genuine Field Study

Before collecting publication-grade data, replace the current FPC block with separate multi-item scales: perceived AI fraud-detection benefit; privacy concern; privacy-protective assurance; false-alert reviewability/procedural fairness; and continued-use intention. Each should ideally contain at least three well-aligned indicators. Regulatory protection should remain a distinct institutional construct. AI literacy can be retained as a predictor or moderator. The preferred structural model is: fraud-detection benefit → perceived value/security; privacy concern → continuance (negative); privacy-protective assurance → trust/continuance; regulatory protection → trust/continuance; procedural fairness → trust/continuance. AI literacy and prior AI experience can be tested as moderators. This model can be estimated using CB-SEM or PLS-SEM only after confirmatory measurement validation and a priori power analysis.[48]

Appendix C. Reproducibility Note

All descriptive statistics, reliability coefficients and regressions reported in this manuscript were computed directly from the supplied Group-8 workbook. No rows were simulated or added by the analysis. Because the workbook itself identifies its records as synthetic, the results are suitable for methodological demonstration and instrument refinement, not for claims about actual Bangladeshi MFS users.

[48] Fornell and Larcker (n 20); Henseler, Ringle and Sarstedt (n 21); Bhattacherjee (n 8).