

RETAIL FINANCE DISTRIBUTION: EVIDENCE BRIEF

Digital Consumer Protection and Transaction Security in Mobile Money: Evidence from Kenya, Indonesia, and Burkina Faso

Background

Mobile money services have become a critical channel for extending financial services to underserved populations in developing countries. The rapid growth of mobile money has introduced significant risks related to transaction security, fraud, and consumer vulnerability. This brief, drawn from Evidence and Gap Map for the Retail Finance and Distribution Initiative, examines the relationship between consumer protection and risk management interventions and their effect on transaction security, risk reduction, and fraud prevention in mobile money ecosystems. The synthesis covers evidence from Kenya, Indonesia, and Burkina Faso.

Scope of the Synthesis

This brief synthesises findings from studies examining the effect of consumer protection and risk management on transaction security, risk, and fraud in mobile money services. The synthesis covers studies from Kenya, Indonesia, and Burkina Faso, spanning 2013 to 2023. The evidence includes regression analyses, mediation analyses, surveys, case studies, and technical analyses.

1. Synthesis of the Findings

1.1 Digital Consumer Protection as a Mediator

In Indonesia, Budiyo and Sukamulja (2023) surveyed 425 respondents from productive age communities in Yogyakarta Province and found that digital customer protection significantly mediates the relationship between mobile money usage and financial inclusion. Mobile money usage significantly affects digital customer protection, and digital customer protection significantly affects financial inclusion. The indirect effect was 0.236, with a Sobel test Z-value of 6.468, confirming partial mediation.

Digital customer protection scored 84.44%, and financial inclusion scored 84.01%, with the access dimension highest at 86.45%. The Pearson correlation between mobile money usage and digital customer protection was 0.651, indicating a strong positive relationship. Mobile money usage is dominated by

payment activities (56%), followed by remittances (33%), savings/investment (5%), withdrawals (4%), and financing (2%). This finding underscores that consumer protection frameworks act as a mediator between technology adoption and financial inclusion outcomes. Strengthening consumer protection enhances trust, which promotes inclusion and reduces vulnerability to fraud.

1.2 USSD Security Vulnerabilities

Agbezouts, Urien, and Dandjinou (2019) documented critical security weaknesses in USSD-based mobile money systems. USSD remains the preferred communication channel for mobile money because it works without internet connectivity. However, much of USSD security relies on GSM security with no end-to-end encryption. Encryption is limited to the MS and BTS channel.

Specific vulnerabilities include PIN characters not masked; PINs are only 4-digit numerals, easy to guess; data is not encrypted between customer and server;

no message integrity checks; periodic PIN changes are not enforced; system default PINs are permitted; and server security policies leave vulnerabilities exploitable for attacks.

The authors proposed a blockchain-based solution to address these vulnerabilities: encrypting data across the communication channel; calculating message digests for integrity checks; increasing PIN character domain; masking PIN entries; enforcing periodic PIN changes; prohibiting year-of-birth PINs; and restricting default PINs. This highlights that fundamental USSD security weaknesses require both technological solutions (encryption, integrity checks) and policy changes (PIN complexity, mandatory periodic changes).

1.3 M-PESA's AML and Risk Management Framework

Buku and Meredith (2013) documented M-PESA's comprehensive consumer protection framework in Kenya, which has maintained compliance with all applicable AML regulations and remained largely immune from corruption or misuse. When the banking industry lobbied for an audit in 2008, M-PESA was declared safe with minimal fraud uncovered. The framework evolved through key regulatory milestones: the Central Bank of Kenya imposed almost no safeguards on the pilot to avoid stifling innovation; the 2009 Proceeds of Crime & Anti-Money Laundering Act criminalised money laundering and made FATF Recommendations mandatory; and the 2011 National Payment Systems Act brought all payment service providers into one regulatory framework.

Before authorisation, Safaricom provides comprehensive agent training covering AML, CTF, and KYC procedures, with staff receiving formal and web-based AML awareness training adapted from the Vodafone Group policy and annually audited. M-PESA customers and agents are subject to comprehensive KYC verification, including automated watch-list screening, with retail agents required to validate customer identity during each transaction using a national ID card. Transactional controls include limits of KES70,000 (US\$900) per transaction, KES140,000 (US\$1,800) daily, KES100,000 (US\$800) holding, and an automated Transaction Monitoring System.

Outcomes include 15.2 million customers (63% of Kenya's adults), over two million daily transactions (90% of all mobile money transactions in Kenya), and

M-PESA processing more transactions domestically than Western Union globally. This demonstrates that effective consumer protection and risk management require a multi-layered approach combining regulatory oversight, comprehensive agent training, robust KYC procedures, and automated transaction monitoring.

2. Cross-Cutting Trends and Insights

Key cross-cutting trends and insights include:

- a. Digital consumer protection mediates trust and inclusion: Consumer protection frameworks strengthen user trust and mediate mobile money usage and financial inclusion (Budiyo & Sukamulja, 2023).
- b. USSD has inherent security weaknesses: Lack of end-to-end encryption, 4-digit numeric PINs, and weak server policies create significant vulnerabilities (Agbezouts et al., 2019).
- c. Multi-layered AML frameworks are essential: Effective fraud prevention requires regulatory oversight, agent training, KYC procedures, and automated transaction monitoring (Buku & Meredith, 2013).
- d. Transaction limits reduce fraud risk: Per-transaction, daily, and holding limits on mobile money accounts help mitigate fraud (Buku & Meredith, 2013).
- e. Agent training builds trust: Comprehensive training covering AML, CTF, and KYC procedures before agent authorisation is essential (Buku & Meredith, 2013).
- f. Consumer training is critical: Consumer training was identified as the biggest challenge to countrywide M-PESA implementation (Buku & Meredith, 2013).

3. What Works

- a. Digital consumer protection frameworks: Mediate mobile money usage and financial inclusion; 84.44% excellent rating (Budiyo & Sukamulja, 2023).
- b. Blockchain-based transaction recording: Increases security, trust, and traceability; allows all stakeholders to verify operations independently (Agbezouts et al., 2019).

- c. Comprehensive agent training: Covers AML, CTF, and KYC procedures before authorisation; annually audited (Buku & Meredith, 2013).
- d. KYC and identity verification: Validates customer identity using national ID during each transaction; automated watch-list screening (Buku & Meredith, 2013).
- e. Automated transaction monitoring: Detects suspicious activity through exception parameters and pattern analysis (Buku & Meredith, 2013).

4. What Doesn't Work

- a. USSD without encryption: Data transmitted without end-to-end security, vulnerable to interception (Agbezoutsu et al., 2019).
- b. 4-digit numeric PINs: Easy to guess, visible to onlookers, weak against brute-force attacks (Agbezoutsu et al., 2019).
- c. No mandatory PIN changes: Security policies don't enforce periodic PIN changes (Agbezoutsu et al., 2019).
- d. Default PINs allowed: System default PINs permitted, creating security vulnerabilities (Agbezoutsu et al., 2019).
- e. No message integrity checks: No mechanisms to verify messages haven't been altered in transit (Agbezoutsu et al., 2019).

5. Challenges

- a. USSD security vulnerabilities: Lack of end-to-end encryption, weak PIN security (4-digit numeric only), and inadequate server policies create significant risks (Agbezoutsu et al., 2019).
- b. Fraud and social engineering: Mobile money fraud often involves impersonation, phishing, and social engineering scams targeting unsuspecting subscribers (Agbezoutsu et al., 2019; Buku & Meredith, 2013).
- c. Regulatory gaps: Inconsistent regulatory frameworks across jurisdictions create compliance challenges; premature regulation can stifle innovation (Buku & Meredith, 2013).
- d. Agent training needs: Inadequate training on fraud detection and prevention leaves agents

and customers vulnerable; consumer training was identified as the biggest challenge (Buku & Meredith, 2013).

- e. Consumer awareness deficits: Many users lack adequate security knowledge, making them vulnerable to fraud (Budiyono & Sukamulja, 2023).
- f. Platform interoperability: Lack of federation between mobile money platforms limits traceability and creates security gaps (Agbezoutsu et al., 2019).

6. Areas for Further Research

- a. Blockchain implementation effectiveness: Empirical studies on blockchain-based mobile money solutions for fraud reduction and user trust.
- b. Cross-country regulatory comparison: Comparative analysis of consumer protection frameworks and their effectiveness in reducing mobile money fraud.
- c. Agent training impact: Longitudinal studies on effectiveness of agent training programs in reducing fraud incidents.
- d. Consumer education effectiveness: Impact assessment of financial literacy programs on fraud awareness and prevention.
- e. USSD security enhancements: Development and testing of enhanced security protocols for USSD-based mobile money systems.
- f. Digital customer protection impact: Further research on how digital customer protection affects user trust and sense of security.
- g. Interoperability and security: Effects of platform federation on traceability and fraud prevention.

7. Conclusion

Consumer protection and risk management interventions are essential for ensuring transaction security, reducing fraud risk, and maintaining trust in mobile money ecosystems. The evidence consistently demonstrates that comprehensive, multi-layered approaches are most effective. A coordinated, multi-stakeholder approach involving regulators, service providers, agents, and consumers is essential to build secure, trustworthy, and inclusive mobile money

ecosystems.

For policymakers and practitioners: implement robust digital consumer protection frameworks; explore blockchain-based security solutions; require comprehensive agent training covering AML, CTF, and KYC procedures; enforce mandatory KYC verification using national ID; implement automated transaction monitoring with exception-based alerts; establish transaction limits; develop consumer education programs on fraud awareness and prevention; and strengthen regulatory frameworks with sector-specific guidelines.

About this Evidence Brief

This evidence brief is a summary of studies of the cell “Consumer protection & risk management → Transaction security, risk, and fraud” from ICED’s Evidence and Gap Map of the Retail Finance Distribution Initiative.

For the full map, visit www.iced-eval.org/evidence-and-gap-maps

References

- Agbezouts, K.E., Urien, P., & Dandjinou, T.M. (2019). Towards Blockchain Services For Mobile Money Traceability and Federation. 2019 3rd Cyber Security in Networking Conference (CSNet).
- Budiyono, E.F.C.S., & Sukamulja, S. (2023). Digital Customer Protection: Mediator between Mobile Money Usage and Financial Inclusion. Media Ekonomi dan Manajemen, 38(1), 205-233.
- Buku, M.W., & Meredith, M.W. (2013). Safaricom and M-PESA in Kenya: Financial Inclusion and Financial Integrity. Washington Journal of Law, Technology & Arts, 8(3), 375-400.