

Security and Surveillance: What Protects a Mobile Money Transaction?

Background

Digital payment technologies have become an important pathway to financial services for populations historically underserved by formal banking. In 2019, of 7.7 billion people globally, about 5.1 billion had access to a mobile phone while more than 1.7 billion adults remained unbanked.

WAEMU countries recorded a 10–30% increase in mobile money activity between 2014 and 2017, reaching some 6.9 million accounts and 351.6 million transactions annually, with an aggregate value of CFAF 3,933.4 billion — value transmitted through infrastructure not designed to secure financial transactions.

This brief examines what the evidence says about transaction security and fraud, covering both the controls that protect transactions and the traceability arrangements that determine who can audit and contest them.

Scope of the Synthesis

This brief synthesises the two sources that together constitute the available evidence in this cell: a PRISMA systematic literature review of 37 empirical studies drawn from 426 records and 112 full texts (Shahen & Sharaf, 2025; global, 2016–2025), and a primary vulnerability analysis with a proof-of-concept implementation on the Ethereum Ropsten test network (Agbezouts et al., 2019; Burkina Faso and WAEMU, current to 2019).

Interventions examined are channel and cryptographic controls, authentication controls including PIN policy and biometrics, ledger-based traceability permitting multi-stakeholder audit, platform federation and interoperability, and regulatory instruments covering issuance oversight, KYC and data protection. Outcomes examined are transaction integrity and confidentiality, authentication strength, tamper evidence and auditability, the capacity to contest transactions, user trust, and reported fraud and data incidents. Confidence in this cell is low: findings are directional and hypothesis-generating rather than established causal effects.

1. Synthesis of Findings

Table 1. Direction and strength of evidence by theme

Theme	Direction and basis
Channel and infrastructure security	Consistently negative — existing systems assessed as insecure; documented vulnerability taxonomy
Authentication and PIN management	Negative on current practice; remedies are design prescriptions only
Surveillance, traceability and tamper evidence	Positive in principle, technically demonstrated, unevaluated in real-world settings

Theme	Direction and basis
Security as a determinant of trust and usage	Consistent and positive, but security enters as a mediator rather than an outcome
Governance, regulation and institutions	Convergent recommendations across both sources; no implementation evaluation

Neither source reports fraud incidence, monetary losses or dispute volumes.

1.1 Channel and Infrastructure Security: A Documented Deficit

Agbezouts et al. (2019) establish that USSD security in operational mobile money systems relies substantially on GSM-level rather than application-layer protection. Encryption is largely confined to the link between the mobile station and the

base transceiver station, so transaction information traverses the remainder of the path — including the operator's network and application server — without transaction-specific confidentiality guarantees. No mechanism exists for verifying message integrity between customer and server.

Two structural characteristics compound this. USSD messages are limited to 182 bytes and are not stored on the handset, constraining in-band cryptographic information and leaving users without a locally retained record; sessions can also terminate under heavy usage. The comparison with SIM Toolkit is instructive: although characterised as more secure, it required SIM updates whenever changes were introduced, so security was in practice traded against ease of deployment.

The systematic review does not assess channel security directly but is consistent in direction, identifying cybersecurity concerns and low platform trust as constraints on adoption. Where it finds positive security attributes, these attach to newer layers such as blockchain-based tamper-resistant identity and biometrics rather than to legacy USSD (Shahen & Sharaf, 2025).

1.2 Authentication and PIN Management

This is the most specifically documented body of evidence in the cell. The weaknesses identified are individually well established and collectively consequential: PIN characters are not masked during entry; PINs are restricted to four numeric digits; periodic change is not enforced through server policy; system-default PINs may be permitted; and customers may use their year of birth, sharply reducing the effective search space for an attacker holding basic personal information (Agbezoutsis et al., 2019).

The corresponding countermeasures — channel encryption, message digests, an expanded PIN character domain, masked entry, and server-level enforcement of rotation with prohibition of birth years and defaults — are drawn from established security principles and prior modelling rather than from interventions whose effectiveness has been demonstrated. These are low-cost and enforceable at the server, which makes them well suited to rapid evaluation, but they remain unevaluated.

1.3 Surveillance, Traceability and Tamper Evidence

This dimension is distinctive because it is framed as a question of who controls the transaction record, not simply whether a record exists. Where operators are the sole source of traceability, customers have little alternative but to trust the operator's account of events; combined with low client literacy, this makes claims against operators hard to substantiate. A related concern is the absence of interoperability, which may shift value towards informal and less traceable channels (Agbezoutsis et al., 2019).

The proposed response is to enable traceability across stakeholders and to federate mobile money solutions, allowing each participant — consumers, operators, banks, agents, merchants and regulators — to audit at the appropriate level on a shared ledger. Tamper evidence derives from SHA-256 hash-linked blocks, such that altering published data changes the block hash and all subsequent hashes, with ledger copies replicated across nodes so that control is not concentrated in one participant.

The implementation is technically substantive but empirically narrow. A USSD instruction is encoded in UTF-8 and transmitted within an Ether transaction, and the authors report creating one such transaction on the Ropsten test network and retrieving its hash. The evidence therefore shows that USSD-formatted instructions can be written to and retrieved from a public blockchain. It does not show improved security or reduced fraud,

and reports nothing on field deployment, throughput, latency, cost, node governance or private-key custody.

1.4 Security as a Determinant of Trust, Adoption and Usage

The review's conceptual framework links digital payment technologies to financial inclusion through three pathways, one operating explicitly through security: secure and transparent transactions are expected to increase usage, while cybersecurity concerns and limited trust are identified as barriers to adoption alongside low digital literacy, inadequate infrastructure and affordability (Shahen & Sharaf, 2025).

Two qualifications matter. First, the finding that 68% of studies report positive effects, 24% mixed and 8% weak concerns the relationship between digital payment adoption and financial inclusion — not between security interventions and fraud — and cannot be read as evidence of fraud reduction. Second, most constituent studies rely on descriptive or cross-sectional data unable to establish causality, with substantial heterogeneity in how adoption and inclusion are measured. That security mediates adoption is plausible and repeatedly supported conceptually, but remains insufficiently identified causally.

1.5 Governance, Regulation and the Institutional Layer

Both sources position institutional arrangements alongside technical controls. The proposed federation architecture requires digital currency backing issued within a central-bank-regulated system, with operators providing equivalent value against the legacy currency and regulators participating as issuers and observers (Agbezoutsis et al., 2019). Security is therefore partly a function of who is authorised, who issues value and who holds audit authority.

The review reaches a compatible conclusion and differentiates priorities by income level: stronger consumer protection and cybersecurity alongside innovation-supportive regulation in high-income economies; interoperability, SME integration and data governance in middle-income economies; and expanded coverage and capability through network infrastructure, agent networks and digital literacy in low-income economies, with particular attention to women and rural populations (Shahen & Sharaf, 2025).

Table 2. Basis of support for proposed approaches

Approach	Basis of support
Authentication hardening (masking, expanded character domain, enforced rotation)	Design recommendation; not empirically evaluated
End-to-end encryption with message-digest integrity checks	Design recommendation consistent with the documented vulnerability profile
Distributed tamper-evident ledger recording	Demonstrated on a public testnet with a retrievable transaction
Multi-stakeholder traceability rights	Design proposal; not empirically evaluated
Platform federation and interoperability	Design proposal supported by documented interoperability gaps
Biometric authentication and	Identified in the review; no effect estimates

Approach	Basis of support
ledger-based digital identity	
Regulatory and governance instruments	Recommended across both sources; no implementation evaluation

No approach in this cell has been evaluated against measured fraud outcomes.

2. Cross-Cutting Trends and Insights

Key cross-cutting trends and insights include:

- Security is theorised as a means and rarely measured as an outcome: neither source reports fraud incidence, monetary losses, dispute volumes or before-and-after comparisons.
- Two security paradigms operate in parallel: hardening endpoints and channels, and pursuing ledger transparency and distributed auditability. They are complementary rather than competing.
- Custody of the transaction record is a governance question, not only a technical one: operator control over records is an accountability concern independent of cryptographic weakness.
- Literacy is a security variable: controls that depend on users detecting, interpreting and reporting anomalies perform less well where literacy is limited, regardless of technical strength.
- Interoperability has a substantive security dimension: fragmentation may push value outside formal, auditable systems.
- Reach and security are in tension: USSD carries transactions for precisely those users least able to migrate to application-based alternatives requiring 3G.
- Technology alone is insufficient: sustained change depends on the interaction between technology, social support and effective institutions (Shahen & Sharaf, 2025).

3. What Works

- Authentication hardening through PIN masking, an expanded character domain, enforced periodic change and prohibition of default and date-of-birth values — low-cost and enforceable at server level.
- End-to-end encryption with message-digest integrity checks across the transaction path, reducing reliance on GSM-link encryption alone.
- Distributed, tamper-evident ledger recording, where hash-linked blocks replicated across nodes make undetected alteration substantially harder.
- Multi-stakeholder traceability rights on a shared ledger, giving customers an independent basis for verifying and contesting transactions.
- Platform federation and interoperability, which keep cross-operator transfers inside the formal, recorded system.
- Regulatory and governance instruments — licensing of issuers, oversight of digital currency issuance, efficient KYC, and data and consumer protection standards.

4. What Does Not Work

- Treating GSM-layer security as sufficient for financial transactions: confidentiality limited to the mobile-station-to-base-station link leaves instructions insufficiently protected across most of their path.
- Permissive and unenforced authentication policies: four-digit unmasked PINs, optional rotation and acceptance of default or year-of-birth values arise from inadequate server-side enforcement rather than technical complexity.
- Operator-only recordkeeping as an accountability mechanism: trust in a single intermediary cannot substitute for independent verifiability.
- Application-based security upgrades as a universal solution: improvements available only through 3G applications risk bypassing the most exposed populations.
- Fragmented and non-interoperable platforms, which can push value outside formal, recorded systems.
- Technology-led approaches without institutional support, since digital technologies alone cannot overcome structural inequalities.
- Assessing security by the frequency with which problems are discussed: discussion frequency reflects reporting behaviour rather than incidence.

5. Challenges

- No baseline or outcome data: neither source reports fraud incidence, monetary losses or dispute volumes, leaving no basis for cost-benefit analysis.
- Weak and heterogeneous indicators: substantial variation in how digital payment use and inclusion are measured, and a proposed security indicator that does not measure incidence.
- Causal identification: countries with stronger institutions are both earlier adopters and better placed to achieve positive outcomes, making effects hard to separate from pre-existing advantage.
- Currency and coverage: direct technical evidence dates from 2019, the review covers only peer-reviewed English-language publications, and the traceability proposal rests on a single testnet transaction.
- Regulatory readiness: a currency-backed federated architecture would require central-bank-regulated digital currency issuance and regional regulator participation.
- Privacy, literacy and redress: expanded traceability increases scope for observation of individual payment behaviour while protection frameworks remain unevenly developed.
- Commercial incentives: USSD is strongly controlled by mobile network operators, so interventions redistributing auditability may meet incumbent resistance.

6. Areas for Further Research

- Measurement of fraud and security outcomes — agreed, comparable indicators of incidence, value at risk, loss per transaction, dispute rates and resolution times, disaggregated by channel, region, gender and income. This is the foundational gap.

- b. Impact evaluation of authentication hardening through quasi-experimental or staged-rollout designs, capturing usability consequences including lockouts, abandonment and credential sharing.
- c. The agent and human layer: agent-facilitated fraud, social engineering, SIM swapping, identity substitution at registration and collusion, none of which either source examines.
- d. Field deployment of ledger-based traceability at scale, measuring throughput, latency, transaction cost and whether multi-stakeholder auditability improves dispute resolution.
- e. Key custody and recovery for low-literacy, feature-phone users, an unresolved prerequisite for any distributed-ledger design in this context.
- f. Privacy-preserving traceability, determining whether tamper evidence and multi-party audit can be achieved without exposing individual payment histories.
- g. Differentiated exposure: whether fraud victimisation and access to redress vary by gender, age, literacy or rural residence.
- h. Cost-effectiveness and sequencing: which combination of channel hardening, authentication controls, ledger traceability, interoperability and regulatory reform reduces fraud most per unit cost, and in what order.

7. Conclusion

The evidence within this cell establishes the security problem with considerably greater clarity than it establishes the effectiveness of proposed solutions. On the problem side the diagnosis is specific and credible: the channel carrying a substantial proportion of mobile money value in West Africa relies predominantly on GSM-level encryption, provides no transaction-level integrity verification, permits four-digit unmasked numeric PINs including default and date-of-birth values, and leaves transaction records substantially under the control of the operator whose conduct a customer may subsequently wish to contest.

On the solution side a coherent package is identifiable — end-to-end encryption and integrity verification, strengthened PIN policy, distributed tamper-evident records with multi-stakeholder traceability, platform federation and an enabling regulatory architecture — but its effectiveness has been demonstrated only through technical proof-of-concept and design reasoning.

The central limitation is that transaction security and fraud are not directly measured within the available evidence base. Security is consistently presented as a mechanism through which digital payments build trust and support inclusion, but it is rarely operationalised as an outcome with measurable values. The review identifies the same limitation in the wider literature and names its consequence: when research prioritises easily measurable indicators while neglecting user safety and data privacy, it risks presenting an overly favourable picture of digital financial inclusion.

About this Evidence Brief

This evidence brief is a cell-wise summary of studies of the cell “Security and surveillance → Transaction security 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), 14–20. IEEE.
- Shahen, A. M., & Sharaf, M. F. (2025). The role of digital payment technologies in promoting financial inclusion: A systematic literature review. *FinTech*, 4(4), Article 59. <https://doi.org/10.3390/fintech4040059>