

Consumer Protection and Risk Management: What Builds Trust and Perceived Safety?

Background

Digital financial services are the principal instrument through which low- and middle-income countries pursue financial inclusion, bringing hundreds of millions of people into contact with formal finance at a fraction of the cost of branch banking.

That achievement rests on an assumption easily overlooked: a person will only place money into a system they believe will give it back. For a first-time user on a thin income, one failed transaction, an unexplained fee or an unreachable complaints line is decisive evidence that the system is unsafe.

Consumer protection and risk management are the policy levers aimed most directly at that mechanism. This brief asks what the assembled evidence shows about the claim that they build confidence.

Scope of the Synthesis

This brief consolidates four earlier sub-briefs covering eleven sources mapped to a single EGM cell: interventions classified as consumer protection and risk management, and outcomes classified as trust and perceived safety. The evidence base comprises one PRISMA systematic review, three quantitative primary studies, two cross-sectional surveys, a legal and regulatory case study, a multi-country case synthesis, a practitioner handbook, a national strategy mid-term review and a regional qualitative synthesis — covering more than thirty countries across Sub-Saharan Africa, South and South-East Asia and Latin America, with evidence from 2003 to 2025.

Interventions span prudential safeguarding of funds, regulatory design and supervision, AML/CFT and tiered due diligence, price and commission transparency, agent vetting, accreditation, training and supervision, liquidity assurance, complaints and redress, data protection and digital identity, interoperability and consumer capability. Outcomes are user trust and perceived safety, together with revealed-preference proxies including over-the-counter transacting, retreat to cash and dormancy.

2. Synthesis of Findings

Thirteen mechanisms are documented; sub-section numbering follows the full brief.

2.1 Prudential safeguarding of customer funds — positive

The most consistent positive evidence concerns structural protection of customer money. Kenya permitted launch in 2007 on condition that funds sat in a pooled trust account at a commercial bank with no intermediation; Sri Lanka later required ring-fenced custodian accounts, real-time reconciliation and a trust instrument surviving insolvency. Both markets scaled, but neither case isolates safeguarding from concurrent licensing and interoperability reforms.

2.2 Regulatory clarity, sequencing and visible due diligence — positive

Where mandates are fragmented across central banks, telecommunications and consumer agencies, users who suffer loss have no route to redress, and it is the absence of recourse rather than the loss that erodes confidence. Kenya adds sequencing — forbearance during piloting, then AML obligations, sector guidelines and a consolidated payments statute — and shows the regulator's own conduct working as a

trust instrument, with central bank and ministry statements setting out the due diligence performed.

2.3 Reliability, liquidity and operational risk — the dominant driver of perceived risk

The two most cited consumer risks across sixteen countries were not fraud or privacy but service downtime and insufficient agent liquidity, both of which induce risky coping such as leaving cash with an agent to complete later. In the only quantitative test, a one standard-deviation gain in a DR Congo agent's liquidity score was associated with roughly 53 to 65 additional cash-in transactions per agent-month against a mean of about 200, and around 21 under agent fixed effects. Almost all explanatory power loaded on cash float, not electronic float — the half providers cannot monitor remotely.

2.4 Price and tariff disclosure at the point of service — negative on practice

About 75% of 116 Ghanaian agents endorsed tariff posting; enumerators observed a posted tariff at 9% of outlets and about 35% admitted overcharging — a lower bound given social desirability pressure. Agents accept the norm and compliance still fails, which points away from awareness campaigns and towards monitoring, enforcement and outlet economics.

2.5 Contract transparency and agent economics — an upstream protection failure

Asked whether they understood how their cash-in commission is computed, about 27% of agents said yes; asked to narrate it, only 5% were accurate and complete and 51% could not describe it at all — self-assessed knowledge exceeding demonstrated knowledge roughly fivefold, with 91% reporting commissions routinely lower than expected. Mozambique records the same mechanism from the supervisory side, with earnings too low to make the business attractive leading agents to extract extra fees. Incentive architecture is a protection instrument, not a back-office choice.

2.6 Complaints, redress and responsiveness — most cited failure, least measured

Unclear dispute options cost users time, money and airtime, and the consequence was withdrawal — confinement to over-the-counter transacting, and non-users concluding from others' struggles that services were too risky. Myanmar supplies the only estimate: service quality, measured as immediate attention when problems arise, had a significant positive effect on trust ($\beta = 0.301$, $p < 0.01$) and satisfaction ($\beta = 0.478$, $p < 0.001$), while scoring lowest of all twenty indicators.

2.7 Visible accreditation and branding — positive, with quantified associations

In DR Congo, branding scores were among the strongest predictors of agent activity: a one standard-deviation gain was associated with roughly 40 to 48 additional cash-in transactions per month, concentrated on the official institutional sign rather than general visibility. Branding functions as an anti-impersonation device rather than marketing, and mandated non-exclusivity may dilute the signal.

2.8 Vetting, training and monitoring — monitoring quantified, the rest untested

Extensive documentary vetting protects consumers but suppresses network scale, and market characteristics explained far more variation in agent activity than any personal characteristic. Standardised checklists at every visit with mystery-shopper verification were predictive, raising model explanatory power to roughly 25%. Training is named the first line of defence against fraud, yet no source estimates its effect.

2.9 AML/CFT, KYC and transaction controls — integrity shown, access design-dependent

Kenya combined identity verification at every transaction, automated monitoring, hard limits and signed agent log books while reaching 63% of adults — the strongest demonstration that integrity controls and inclusion can be complements. The counter-cases show design dependence: individual agent registration and full originator capture constrained scaling in the Philippines, and where only 58% hold a national identity document full due diligence operates as exclusion. Banks would not use existing flexibility until tiers were formally defined, because discretion carrying sanction risk goes unused.

2.10 Data protection, privacy and digital identity — perceived risk blocks the enablers

Complex interfaces drive customers to share PINs with agents or relatives, and data-handling disclosures sit online in language few can parse. Perceived risk can obstruct inclusion outright: national identity proposals were opposed for two decades on privacy grounds, leaving verification difficult for everyone. Retail cyber risk is supervised far more lightly than high-value payment systems.

2.11 Consumer capability and education — no demonstrated direct effect on trust

Colombian digital literacy programmes were not significant as a direct predictor ($\beta = 0.08$, $p = 0.298$); Mozambique's financial knowledge score was flat at 4.0 over three years against a rising target; and in Myanmar enabling conditions including training support had no significant direct effect on trust. Capability reads as necessary infrastructure for safe use rather than a direct lever, failing when fragmented, unmeasured and unlinked to the risks users face.

2.12 Interoperability — the only estimated association with trust

Tanzanian users rated trust and reliability at 4.05 of 5, with interoperability a significant positive predictor ($\beta = 0.298$, $p < 0.05$, $R^2 = 0.35$). Three qualifications are essential: the intervention is interoperability rather than a protection instrument; the source is a non-peer-reviewed preprint with inconsistent regression reporting; and the design cannot separate trust as consequence from trust as precondition.

2.13 Provider reputation — the mechanism no regulator can legislate

In Kenya, dealers became agents and consumers experimented with an unfamiliar system because they trusted the operator's brand. The sharpest illustration inverts technical and perceived safety: the platforms underlying mobile money cannot support the security associated with card encryption, yet the public trusted mobile money over cards — perceived safety follows familiarity and reputation rather than cryptographic strength.

Table 1. Direction of evidence in this cell

Mechanism	Direction of evidence
2.1 Prudential safeguarding of funds	Positive (case narrative)
2.2 Regulatory clarity and visible due diligence	Positive (case)
2.3 Reliability, uptime and agent liquidity	Positive (strongest; agent FE)
2.4 Point-of-service tariff disclosure	Negative on practice
2.5 Contract and commission transparency	Positive (association)
2.6 Complaints, redress and responsiveness	Positive (SEM); absence damaging
2.7 Visible accreditation and branding	Positive (quantified)
2.8 Agent vetting and training	Not tested
2.8 Supervisory monitoring on checklists	Positive (association)
2.9 AML/CFT, KYC and transaction controls	Integrity shown; access design-dependent
2.10 Data protection and digital identity	Perceived risk blocks enablers
2.11 Consumer capability and education	No direct effect
2.12 Interoperability	Positive (single preprint)
2.13 Provider reputation and brand	Positive (case, unmeasured)

“Not tested” denotes absence of evidence, not evidence of absence.

3. Cross-Cutting Trends and Insights

- **Trust is a precondition, almost never a measurement.** Eleven sources place it at the centre of the chain from access

to use; two measure it, and no indicator framework in the cell includes a perceived-safety measure.

- **The negative evidence is far stronger than the positive.** Protection failure erodes trust in recurring, identifiable ways with visible behavioural consequences, while protection success is inferred from co-occurrence. Preventing documented failures is the highest-confidence recommendation available.
- **Distrust is usually a rational risk assessment.** It traces to banking crises, fraud experience and observation of others' losses, so persuasion underperforms verifiable change in underlying risk.
- **Reported trust is a poor proxy for protection.** Users rate trust at 4.05 of 5 in one market while outlets in another post tariffs at 9% and a third of agents concede overcharging. The one time perception was tested against an objective benchmark, it failed fivefold.
- **Norm endorsement is not compliance, and channel volume is not disclosure.** Three quarters of agents endorse tariff posting and one in eleven does it; four provider communication channels coexist with 5% demonstrated comprehension.
- **Protection and commercial viability are complements at the agent level.** Obligations placed on commercially unviable agents are honoured nominally at best.
- **The protection–access trade-off is real but design-dependent.** Free-service mandates, registration requirements and full due diligence in undocumented populations each reduced access, yet Kenya paired a complete control stack with growth to 63% of adults.

4. What Works

No approach has been evaluated against a measured trust outcome; these are design propositions, not verified effects.

- Ring-fencing customer funds** in trust or custodian accounts with real-time reconciliation — the risk users fear most and the one a supervisor can most readily verify.
- Regulatory due diligence made public**, including independent technical assessment, post-launch audit and official assurance on operational safety.
- Treating reliability, uptime and liquidity as protection obligations**, through master-agent responsibility for float, remote monitoring and overdraft facilities.
- Fast, competent handling of consumer problems** — the only component with a directly estimated effect on trust — with supervisor-specified redress and published complaints statistics.
- Uniform, publicly displayed tariffs** verified by observation rather than self-report, and verifiable commission statements for front-line agents.
- Visible accreditation and traceable supervisory monitoring**, quality-assured by mystery shopping, alongside proportionate tiered due diligence with alternative identity evidence.

Four conditions for success

- **Verify at the receiving end.** Assess disclosure and training by demonstrated comprehension and observed conduct, not channels used.
- **Align agent economics with conduct.** Thin or opaque margins place compliance costs on the actor best able to recover them from customers.
- **Make exit possible.** Interoperability and portability let the market enforce conduct standards alongside the regulator.

- **Build redress before measuring trust.** A trust score collected where no complaint channel functions measures unfamiliarity with failure.

5. What Does Not Work

- Standalone, uncoordinated financial literacy campaigns**, where the failure is fragmentation and absent measurement rather than education as a concept.
- Protection rules without market conduct supervision capacity:** laws and fee notices coexisting with a draft supervision methodology and unpublished complaints statistics.
- Voluntary compliance verified by self-report**, trust scores as evidence that protection exists, and disclosure as the primary instrument where literacy is low.
- Blanket free-service mandates and compliance-driven due diligence**, which erode agent revenue and push integrity costs onto the agent layer.
- Regulating mobile money by analogy to banking law**, reactive prohibitions, and monitoring assigned to staff with competing commercial targets.
- Agent-set pricing and recruiting agents ahead of customers**, along with commission triggers that invite gaming rather than preventing registration fraud.

6. Challenges

- **Measurement and data.** Trust has no baseline, and no source reports complaint volumes, resolution times or funds recovered.
- **Causal identification.** All designs are cross-sectional or descriptive, and transaction activity conflates trust with convenience and price.
- **Structural agency risk in the last mile.** The provider carries the brand and obligation while an independent business controls the encounter.
- **Agent economics and the vetting–scale trade-off.** Arrears, modest variable revenue and demanding documentation exclude the community-embedded retailers that carry local trust.
- **Enforcement and fragmentation.** Tariff posting requires observation at tens of thousands of dispersed outlets, and mandates cut across agencies with no accountable owner.
- **Identity, infrastructure and cybersecurity.** Documentation excludes where most lack papers, and outages and a cost of roughly US\$1,400 per agent constrain rural networks.

Quality caveats on the included sources

No source uses a counterfactual or longitudinal design, so no causal effect on trust can be established. One quantitative source is a non-peer-reviewed preprint with inconsistent regression output; one case study has an author affiliated to the operator studied; one rests on 25 microenterprises with an inconsistent stated design; and one Ghanaian brief lacks a stated author, institution and date. Coverage is concentrated in a few districts and cities.

7. Areas for Further Research

The first three are first-order: without them no intervention in this cell can be evaluated against trust at all.

- Direct, validated measurement of trust and perceived safety**, fielded to users and non-users at baseline and follow-up and disaggregated by gender, income, age and location.

- b. **Calibration of trust against realised harm**, pairing reported trust with mystery shopping, transaction audits and matched agent–customer sampling.
- c. **Redress performance measurement**: complaint volumes, share resolved, resolution times and value recovered, and which designs restore confidence.
- d. **Counterfactual evaluation of discrete instruments**, randomising commission statements, tariff display, complaints mechanisms and monitoring intensity.
- e. **Agent remuneration design and consumer harm**, testing whether commission levels and transparency predict overcharging and whether reform reduces it.
- f. **Enforcement models and the protection–access frontier**, quantifying net effects of mandates, registration requirements and due diligence on inclusion and trust jointly.
- g. **Trust dynamics after failure and the reputation channel**, including how far incidents propagate through social networks and what restores confidence.
- h. **Differential exposure and under-represented contexts**, by gender, age, disability, literacy and rural residence, and in fragile settings and newer products.

8. Conclusion

Across eleven sources, three continents and two decades, the relationship between consumer protection and trust is asserted far more often than it is evidenced. The cell supports a qualitative conclusion and refuses a quantitative one: protection and risk management are central to whether these services are used rather than merely available, but the claim rests on mechanism, testimony and case narrative, not measured effects.

What the evidence establishes is asymmetric and useful. Protection failure erodes trust in identifiable ways — services that do not work when needed, agents without cash, prices never published, complaints that go nowhere — with visible consequences in retreat to over-the-counter transacting, retreat to cash and non-users deciding the system is too risky. Where protection appears to have built trust, the effective measures were structural and prudential rather than educational: ring-fenced funds, publicised regulatory due diligence, supervisor-specified redress, reliability treated as an obligation and visible accreditation.

Three findings cut across contexts as different as Kinshasa in 2013, Nairobi in 2007, Yangoon in 2020 and Ghanaian and Tanzanian agent markets today. Trust is inferred from observable reliability and judged at the point of failure. Consumer caution is rational, so it responds to verifiable changes in risk rather than persuasion. And trust is used simultaneously as the outcome of interest and as the evidence that protection exists — a circularity made concrete by self-assessed understanding exceeding demonstrated understanding fivefold.

Implications by audience

- **Policymakers and regulators.** Sequence prudential safeguarding before conduct rules, make tiers explicit, build complaints data infrastructure early, enforce price disclosure rather than raise awareness further, extend disclosure upstream to the provider–agent relationship, and test measures for access effects first.
- **Practitioners and providers.** Uptime, float management and interface simplicity are consumer protection, not operations; agent margins are a protection variable; and disclosure should be tested by comprehension at the receiving end.
- **Researchers and funders.** Anchor the outcome — measure trust with validated instruments alongside observed conduct and redress performance, with staged variation in provider-controlled instruments.

Overall assessment

Consumer protection and risk management are necessary conditions for trustworthy digital financial services whose effect on trust remains unmeasured. Reported trust is high in markets where price disclosure demonstrably fails and a third of agents concede overcharging, so it indicates user experience rather than user protection.

About this Evidence Brief

This brief is a consolidated, cell-wise summary of eleven sources mapped to the cell “Consumer protection and risk management → Trust and perceived safety” 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

Sources Synthesised

- Cull, R., Giné, X., Harten, S., Heitmann, S., & Rusu, A. B. (2018). Agent banking in a highly under-developed financial sector: Evidence from DR Congo. *World Development*.
- Torres Ortega, J. M., Guzmán Murillo, H. J., & Blanco Troncoso, A. L. (2024). Digital payment infrastructure accessibility and microenterprises in Barranquilla, Colombia. *J. Infrastructure, Policy and Development*, 8(9), 6433.
- Riley, T. A., & Kulathunga, A. (2017). Bringing e-money to the poor: Successes and failures. *World Bank*.
- Tun, P. M. (2020). Building a theoretical research model for trust development: Mobile financial services in Myanmar. *SEAM*, 14(2), 173–193.
- Davidson, N., & Leishman, P. (n.d.). Building, incentivising and managing a network of mobile money agents. *GSMA*.
- World Bank & AFI. (2020). Mozambique national financial inclusion strategy 2016–2022: Mid-term review.
- Buku, M. W., & Meredith, M. W. (2013). Safaricom and M-PESA in Kenya: Financial inclusion and financial integrity. *Wash. J. Law, Tech. & Arts*, 8(3), 375–400.
- Sylvester, M. M., & Motloung, O. M. (2025). Digital financial inclusion and sustainable economic development in Sub-Saharan Africa. *OIDA IJSD*, 18(12), 1173–1184.
- When agents do not understand their commissions: Contract clarity in Ghana’s mobile money market (n.d.). Survey of 116 agents; author, institution and date not stated in the source supplied.
- Raphael, C. (2025). Interoperable digital financial services and financial inclusion in Tanzania. SSRN preprint 5976164. Not peer reviewed.
- Shahen, A. M., & Sharaf, M. F. (2025). Digital payment technologies and financial inclusion: A systematic literature review. *FinTech*, 4(4), 59.

Works cited within the included sources are reported as presented by them.