Trust by design

A user protection framework designed to support financial health

Across markets, digital financial services are expanding rapidly, enabling more people to save, pay, borrow and receive funds through mobile and digital channels. This progress is important, but access alone does not ensure financial health. When users face unclear terms, hidden fees, fraud, data misuse, or slow redress, trust can weaken and engagement may decline.

This practical, expertise-led framework translates market insights into shared principles. It showcases scalable industry practices and ways to take coordinated action across providers, ecosystem partners and policymakers, ultimately driving global financial health.

Financial inclusion goes beyond just access. It's about enabling safe, confident and ongoing use of financial services by people and small businesses. Embedding strong safeguards across the user journey turns access into confident, long-term use.

Key opportunities to build trust and engagement

Security and clear recourse build confidence

Users are more likely to engage with confidence when they know their funds and data are secure, and when clear recourse is available if something goes wrong.

Transparency and protection promote trust

Hidden fees, data misuse, fraud and weak redress mechanisms can undermine confidence and stall adoption.

Larger digital footprints call for better safeguards

Data, automation and AI can expand access, but without responsible usage and strong safeguards, they can amplify risk at scale.

Intentional design strengthens outcomes

Building products with consumer protection in mind from day one embeds safeguards - like risk-based friction, user testing and recovery mechanisms - from the start.

64%
of consumers said their confidence in a brand or service would significantly increase if it adopted advanced security.[1]

1 in 5
unbanked adults across low-and middle-income economies cited distrust in financial institutions.[2]

~1 in 5
consumers with a phone have encountered a scam, undermining confidence in digital services.[3]

91%
of customers rate **data security, fraud protection,** and **privacy** as must-haves.[4]

Advancing financial health through collective action

The **Global Financial Health Coalition** advances financial health by convening C-suite leaders to shape and share practical insights, proven methods, and innovative use cases that help people and small business move from access to lasting financial health.

1
User value
Connecting individuals and small businesses to relevant, accessible, and useful financial tools.

2
User protection
Safeguarding users through responsible design, transparency and strong protections.

3
User empowerment
Enabling informed, confident use through education, control and clear recourse.

The **Global Financial Health Coalition** delivers on this mission by focusing on three priorities:

- Sharing best practices
- Advancing inclusive innovation
- Strengthening trust in financial services

Foundational components of user protection[5]

1
Transparency
Users need clear and timely information to make informed decisions.

2
Data responsibility
User data should be collected and used only for legitimate purposes with safeguards, transparency and user rights.

3
User recourse and rights
Users should be able to raise concerns, resolve disputes and access timely, fair redress.

4
Security and protection
Users should be helped to be protected against loss and misuse through safeguards, monitoring and responsive action.

1. Transparency

User protection must be integrated into product design, testing, marketing and distribution, ensuring suitability for users' needs, risks, capabilities and context. Terms must be clear and easy to navigate and users must be informed of both their rights and how to protect themselves. Services should be designed with time-constrained consumers and small businesses in mind.

How to ensure transparency

Elevate scalable practices such as practical disclosures and support ongoing dialogue with policymakers. This can strengthen how transparency and choice are implemented within existing regulatory frameworks.

Member example

Mastercard's Connect Plus gives consumers a single dashboard to see who has access to their financial data and to grant or revoke consent in real time – **putting transparency and choice directly in the hands of end users.[6]**

Member example

Airtel Africa strengthens customer and stakeholder trust by embedding responsible data use and rigorous data governance across its operations, ensuring personal data is processed lawfully, transparently, and only for clearly defined purposes, supported by ISO-aligned **security controls and continuous monitoring and testing.[7]**

2. Data privacy and responsibility

Privacy must be integral to all product design, with data minimization, strong third-party vendor management, and fraud prevention built in from the beginning.

How to treat data responsibly

Surface practical models such as staged consent, in-journey explanations, financial education for MSMEs and cyber risk management practices. Efforts must be made to help users understand, control and protect their data.

3. User recourse and rights

Trusted recourse channels should be embedded within the provider interface. The customer journey shouldn't just be designed around moments of success, but also for when things go wrong.

How to empower users

Define what good recourse looks like in practice from day one, including accessible dispute resolution mechanisms, visibility, speed, clarity and rights-based escalation.

Member example

GSMA research across 34 countries found that **96% of mobile money providers detect fraud primarily through customer complaints**, yet over half question the effectiveness of their fraud management systems - making accessible, well-resourced user reporting channels both the industry's primary detection mechanism and its most critical gap to close.[8]

DANA Protection embeds user recourse directly into the platform through in-app reporting, investigation, and a 100% money-back guarantee for unauthorized transactions – contributing to a **70% reduction in account-hacking attempts** and nearly 80% in-app satisfaction (CSAT) in 2025.[9]

Member example

DaviPlata identifies transaction friction in real time, resolving issues before claims arise. This has supported **2M customers and recovered $84M in cash-in** within the transaction flow. 804K additional customers have been assisted following app errors and 247K after authentication failures.[10]

4. Security, fraud and scam protection

As social-media-driven scams continue to grow, providers are increasingly turning to in-app recourse, stronger user awareness and financial education. AI-enabled tools can help identify vulnerabilities and protect users more quickly.

How to protect payments

Convene cross-sector action on emerging scam threats and spotlight scalable prevention models for SMEs and first-time digital users.

Build trust through stronger protection

An opportunity to improve financial health outcomes and create lasting business value

The shift is clear. As an industry, we must move from simply enabling access to building confidence. Organizations that embed trust through clear design, strong safeguards and effective recourse will drive more meaningful, sustained engagement.

Here's how:

1
Act now to turn principles into practice and drive real impact

2
Adopt, map and embed user protection framework across the user journey

3
Prioritize high-risk moments

4
Measure trust as an outcome

Interested in learning more? Contact us at **Global.Financial.Health.Coalition@mastercard.com**

Sources and notes:

1. Thales, 2025 Digital Trust Index, 2025
2. World Bank, The Global Findex Database 2025
3. GSMI, Findex 2025: Why Financial Inclusion Needs to be More Responsible, 2025
4. Accenture, Navigating Cybersecurity in Banking, 2025
5. Providers should remain accountable for fair outcomes by maintaining appropriate safeguards, redress and reimbursement pathways, and ensuring that AI-enabled decisions are transparent, explainable, subject to human oversight, and open to user challenge. "Fair" in this context draws from the Consumer Financial Protection Bureau's Consumer Protection (2022), which establish that "all financial consumers should be treated equitably, honestly and fairly at all stages of their relationship with financial services providers," and that fair treatment should be integral to the governance and corporate culture of all providers.
6. Mastercard, Mastercard debuts new open banking powered tools, 2026
7. Airtel Africa, Data security, 2026 (this data point was given directly to Mastercard)
8. GSMA, Mobile money fraud typologies and mitigation strategies, 2026
9. DANA 2025 (this data point was given directly to Mastercard)
10. DaviPlata 2026 (this data point was given directly to Mastercard)