DECODIS

Digital Portfolios of the Poor

Nigeria Findings

Decodis | May 2026

Summary

The most recent financial and digital inclusion data shows weakness in digital financial use despite widespread access to digital devices and broad use of digital applications. In Nigeria, growth in uptake of digitally enabled accounts; payments well behind Kenya. Does this reflect a lack of digital trust?

We asked ourselves whether and how digital trust may be driving patterns in digital financial usage and whether it applies across applications and segments. The Digital Portfolios of the Poor project set out to understand the digital trust philosophies of low-income people in India, Kenya, Nigeria, and Pakistan.

For this research, it was important to have this type of "qualitative data at quantitative scale" to allow for an inductive analysis of how respondents voiced their own perspectives without pre-specification of responses. Yet it was also important to have a large sample to test where a type of response was idiosyncratic across a few respondents or across the entire sample.

To achieve this, surveys were collected through automated voice interviews conducted in local languages, with AI-powered qualitative analysis used to surface the motivations, frustrations, and emotions that surveys alone rarely capture.

Key findings are:

- Smartphone access was high at 76%, with relatively less phone sharing than the other countries in the study.
- WhatsApp and YouTube were the most widely used apps, with payment app and online banking use notably lower among women (24% and 14%) than men (41% and 25%).
- Nigeria's digital risk landscape is shaped by four distinct concerns:
    - Account hacking
    - Middleman distrust, focused on bank employees
    - Transaction failures, where payment senders fear lose of reputation if a payment does not go through.
    - Physical theft of carrying a phone

- Ideas for solutions were developed with three digital financial service providers to create cross-organization changes to increase trust across their full customer base.

Sample and Methodology

The Nigerian findings draw on 960 respondents across Kano, Lagos, and Enugu, surveyed in Hausa, Yoruba, and Igbo. The survey comprised 4 modules, covering 133 voice response questions and 94 keypad response questions, with respondents also reacting to audio skits designed to draw out qualitative perspectives on trust in a depersonalized way.

Device Access and Ownership

76% of respondents had access to a smartphone and 72% reported ownership, with feature phone access at 13% and basic phone at 10%. Nigeria had notably less phone sharing than the other countries in the study, though more than half of smartphone owners still reported needing to share their device with others in the household. As in other countries, ownership was a broad concept — many respondents described feeling a sense of ownership simply by virtue of regular access. 57% of respondents reported access to two devices, though the degree of access to the second device was not measured.

	Smartphone	Feature phone	Basic phone
N	726	126	94
Access	76%	13%	10%
Ownership	72%	11%	9%
→ Owners who share phone	55%	50%	44%

Note: Ownership figures reflect self-reported data. Many respondents equated regular access with ownership. Sharing rates remain substantial despite Nigeria having lower sharing levels than other study countries.

Application Use

WhatsApp and YouTube were the most widely used applications, with broadly similar rates between men and women. The most striking gender gap was in Facebook use — used by 32% of women compared to 59% of men — which may reflect greater concern among women about posting and public visibility online. Payment app and online banking use was notably lower among women (24% and 14% respectively) than men (41% and 25%), despite broadly

comparable levels of WhatsApp and YouTube use, suggesting that the gender gap in digital financial services is not primarily a question of device access or general digital engagement.

Application	Women	Men
WhatsApp	80%	86%
YouTube	74%	80%
SMS	61%	69%
Facebook	32%	59%
Games	31%	30%
Payment apps	24%	41%
Truecaller	25%	31%
Online banking	14%	25%
Instagram	20%	29%

Trust Archetypes

The findings revealed three statistically distinct digital trust archetypes, derived from an inductive analysis of how respondents described their own experiences across four pillars: Risk Perception (what dangers people foresee), Risk Mitigation (how they act on those fears), Responsibility Perception (who they hold accountable), and Benefit Perception (why they engage with digital tools at all).

Control Seekers are the most digitally confident group. They are fully aware of digital risks, know how to mitigate them, and express confidence in their ability to do so. They hold themselves primarily responsible for their own protection and tend to believe others should take the same approach. They are the heaviest users of smartphones and a wide range of digital financial services, and value digital tools above all for the market reach and business opportunities they unlock.

Assurance Seekers have the most limited awareness of digital risks and are often unable to articulate specific threats or identify who should be responsible for their protection. They engage with digital tools by habit rather than by informed choice, relying on family, friends, and community networks for guidance when things go wrong. Their engagement with digital tools is anchored in basic financial access and inclusion.

Protection Seekers are aware that digital risks exist — including scams, harassment, and image misuse — but feel uncertain about how to protect themselves. Rather than self-protecting, they look to an institution — a government, regulator, or platform — to bear primary responsibility for their safety online. Despite their concerns, they remain engaged in digital life and value the convenience and opportunities that digital tools provide.

Trust Archetypes in Nigeria Compared to Other Countries

Nigeria sits in the middle of the four-country trust confidence spectrum. With 36% Control Seekers, it sits well below Kenya (60%) but above India (12%) and Pakistan (22%), reflecting a digitally active but unevenly confident population. Its 47% Assurance Seeker share — the second highest after India — underscores that nearly half the population is navigating digital financial services without a reliable framework for understanding risk. Across all countries, the same four pillars underpinned the archetypes, though the specific fears, behaviours, and benefits that defined each pillar differed significantly by country context.

Country	Assurance Seekers	Protection Seekers	Control Seekers
Kenya (N=992)	39%	1%	60%
India (N=939)	50%	38%	12%
Nigeria (N=953)	47%	17%	**36%**
Pakistan (N=544)	40%	38%	22%

Key Nigeria-Specific Findings

Risk Perception: Four Distinct Concerns

Nigerian respondents articulated four distinct categories of digital risk, more granular than those expressed in other countries. Account hacking — the fear of someone accessing a wallet or bank account — was the most widely cited risk across all archetypes. Middleman distrust was a distinctly Nigerian concern: respondents described a belief that bank or telecom employees had access to their account details and could steal from them directly — a risk framed as institutional rather than external. Transaction failures were also a significant concern: given that telecom systems in Nigeria can be unstable, respondents worried that payment confirmation might not arrive, damaging their reputation with customers or suppliers. Physical theft — the fear that taking a phone out in public to conduct a transaction would attract thieves — was a concern specific to Nigeria and did not appear prominently in the other three countries.

Risk Mitigation: Different Strategies Across Archetypes

How respondents managed risk differed meaningfully across archetypes. Assurance Seekers primarily relied on cautious sharing — limiting transactions to people they knew or defaulting to cash — and were largely unable to articulate more active protective strategies. Protection Seekers were the only archetype to describe external verification as a strategy: checking with someone else before acting on a digital interaction, suggesting a level of digital awareness that went beyond avoidance but had not yet reached self-sufficiency. Control Seekers described the most active approach, combining cautious sharing with app verification features and — uniquely among all archetypes — transaction monitoring: actively watching incoming and outgoing payment records to detect anomalies. They were also the only archetype to describe responsibility in purely personal terms, without referencing institutions or platforms.

Benefit Perception: Market Reach and Income Generation

Across all archetypes, the primary benefit of digital tools was articulated in terms of income generation and market reach — the ability to connect with customers beyond foot traffic, promote goods and services, and conduct transactions without visiting a bank branch. This is distinct from India and Pakistan, where convenience was the dominant benefit, and reflects the more commercially active digital landscape of Nigeria's urban centres. Physical safety — the ability to reach friends and family in an emergency — was also mentioned as a benefit, particularly among Protection Seekers, pointing to a layer of utility that goes beyond financial transactions.

Provider Workshops

The Nigeria findings were tested in workshops with three digital financial service providers: Source Microfinance Bank, a digital microfinance bank focused on low-income clients; esusu.africa, a FinTech company digitising traditional thrift savings and microcredit systems; and AjoCard, a FinTech focused on making it easy for the underserved and unbanked to manage money and make payments securely. Each workshop brought together senior staff from across institutional departments — including product development, marketing, customer experience, compliance, and leadership — and worked through problem identification, solution design, and actionable proposals for both Control Seekers and Assurance Seekers.

Institution	Solutions for Control Seekers	Solutions for Assurance Seekers
Source Microfinance Bank	Reframe messaging from 'tech-driven banking' to 'community-rooted empowerment'. Build in-app dispute clarity and flexible repayment options. Run scam detection awareness campaigns.	Share testimonials from long-term users. Build subtle gamification into the savings journey (e.g. "3 months saved without withdrawal" badge). Launch a 'Voices of Trust' peer referral campaign.

esusu.africa	Develop back-end logic to flag users with 3+ failed syncs and route to proactive agent follow-up. Expand receipt messaging to WhatsApp and email.	Equip field-facing partners to explain connectivity issues as temporary and fixable. Give agents visual guides showing what a network issue looks like and what to do.
AjoCard	Develop a User Trust Index reported at board level. Design product journeys for different digital comfort levels with safe exit points and re-entry cues.	Co-create marketing content with real users from different regions. Activate a weekly pain-point pulse reporting system. Prioritise partnerships with organisations users already trust — religious networks, women's cooperatives.

Solutions were generated by institution staff in half-day workshops using the trust philosophy framework. Each institution produced short, medium, and long-term proposals with defined measures of success.

Conclusion

Understanding how customers think about digital financial services — the risks they perceive, the protections they expect, and the benefits they value — is critical to building services that people will actually trust and use. Trust is not a single thing, and it cannot be addressed with a single intervention. Customers fall into different trust archetypes as an amalgamation of their environment, their experiences, and their own personality traits — including risk tolerance, confidence, and the degree to which they hold themselves or others responsible for their digital safety.

The three archetypes identified in this study — Control Seekers, Assurance Seekers, and Protection Seekers — represent fundamentally different starting points for any trust-building effort. A Control Seeker needs transparency, recourse, and tools that match their intentionality. An Assurance Seeker needs plain-language guidance, peer-rooted reassurance, and pathways into digital confidence that do not assume knowledge they do not yet have. A Protection Seeker needs to see institutions taking responsibility — not just in words but in visible, credible action.

By workshopping across archetypes and across provider functions simultaneously, institutions are better positioned to identify practical, cross-cutting interventions that build trust at scale. The Nigeria workshops demonstrated that when product teams, marketing leads, compliance staff, and customer experience teams work through the same customer reality together, the solutions they generate are more concrete, more feasible, and more likely to reach the customers who need them most. Moving from insight to institution-wide action — rather than isolated product fixes — is the real opportunity that this framework makes possible.

Data collected from 960 respondents across Nigeria using automated voice interviews and AI-powered qualitative analysis. Conducted by Decodis in partnership with the Henry J. Leir Institute at Tufts University.