BRIDGFORTE

EXECUTIVE TABLE SERIES | No. 1

Trust Architecture in Platform-Led Finance

Structural Governance Imperatives for Nigeria's Digital Financial Ecosystem

Policy Framework Report

July 2026

In partnership with the UNDP Innovation Centre, Lagos, Nigeria

CONTENTS

Executive Summary

Digital financial systems are undergoing a **structural transition**. Real-time payments, digital identity, and artificial intelligence are becoming embedded in core financial infrastructure, reshaping how financial services are delivered and how risk is distributed across institutions, platforms, and shared infrastructure. As these interdependencies deepen, **confidence is no longer rooted in individual institutions or platforms, but in the strength of the infrastructure that binds the system together. The governance challenge this creates is not incidental. It is structural**, and it is emerging faster than the frameworks designed to manage it.

Nigeria sits at the leading edge of this transition. Over the past fifteen years, a combination of deliberate policy, shared infrastructure investment, responsive innovation, and private capital transformed its financial system from a predominantly bank-led model into a multi-layered, platform-driven ecosystem – one that today processes over **₦1.07 quadrillion** in electronic transactions annually and has earned a **'mature inclusivity'** rating from AfricaNenda, the only African system to do so. Yet this expansion has also exposed a second-order challenge: **confidence has not kept pace with access**, as reflected in persistent dispute-resolution failures, rising consumer complaints, and continued reliance on cash despite rapid digital growth.

This report draws on insights from a closed-door **Bridgforte Executive Table** convened in Lagos in February 2026, which brought together thirty senior leaders from across Nigeria's financial ecosystem. Drawing on structured polling, facilitated discussion, post-event survey data, and supporting research, the report examines where trust breaks down in platform-led financial systems, identifies the institutional architecture required to support **durable confidence**, and sets out priorities for coordinated system-level action.

Analytical Framework

The report applies the **Bridgforte Trust Architecture Framework** as its central analytical lens. The framework identifies five interdependent pillars of systemic confidence: **Infrastructure Integrity, Institutional Accountability, Technology Governance, Ecosystem Coordination, and Cultural Confidence**. Together, these pillars explain how confidence in digital financial systems is shaped not only by the performance of individual institutions, but also by the infrastructure, governance, and coordination arrangements that connect them. The framework therefore provides a system-level lens, operating across three relational axes **– Consumer to Institution, Institution to Institution, and Institution to Regulator –** for understanding how trust is produced, and where it breaks down, within platform-led financial systems.

Key Findings

- **Trust failures are operational before they are technological.** Service reliability and dispute resolution are the primary drivers of confidence erosion, far outweighing concerns about fraud, data privacy, and artificial intelligence. Structured polling ranked transaction failure and dispute resolution as the primary breakdown points, ahead of data privacy, cybersecurity, and AI decision-making. Systems are judged less by what they enable under normal conditions than by how they perform when they fail.

- **Identity infrastructure is the structural root of trust.** Fragmented identity systems undermine fraud prevention, consumer recourse, and institutional accountability. Identity must be treated as shared infrastructure – a public good – rather than an institutional compliance function.

- **Real-time payments introduce a design trade-off that has not been resolved.** Speed accelerates inclusion but amplifies fraud exposure when safeguards are not embedded within system architecture. The system's fraud problem is less about volume than consequence.

- **Artificial intelligence presents a governance challenge, not a technology challenge.** The principal risks lie in governance failures (data misuse, lack of explainability, and embedded bias) rather than in the technology itself. A governance window exists, and it should be used.

- **Financial institutions collaborate less effectively than the fraud networks targeting them.** This is a structural failure, not a moral one. Structured polling confirmed this pattern: institutional mistrust and competitive incentives ranked above legal, regulatory, and technological barriers. Yet, Nigeria's own track record demonstrates that when the stakes are systemic, institutions have chosen to build together.

- **Regulatory models are misaligned with the realities of platform-led systems.** In these systems, risk arises from interactions between actors rather than the behaviour of any single institution. Supervisory approaches must evolve from controlling institutional behaviour to governing system dynamics.

- **Trust-critical capabilities must be shared.** Fraud intelligence, cybersecurity, and consumer protection mechanisms are most effective when designed as shared system infrastructure rather than institution-specific functions.

- **The overall trust resilience assessment reflects all of the above.** When asked to rate overall trust resilience in Nigeria's financial ecosystem on a scale of 1 to 10, participants gave an average score of 5.4. In a system that depends on confidence, a midpoint assessment from the senior leaders closest to its performance is itself a finding.

Policy Implications and Recommendations

The findings point to **eight structural implications** that together reframe trust as a design problem rather than an institutional attribute. These implications span identity infrastructure, risk architecture, coordination mechanisms, regulatory governance, and the role of cultural confidence in sustaining active participation.

Ten recommendations are addressed to three audiences:

For regulators and government agencies: mandate interoperable identity infrastructure as shared public investment; establish mandatory fraud intelligence sharing with binding participation; publish binding AI governance standards including explainability and contestability requirements; and commit to a phased transition toward outcome-based supervision with standing industry-regulator dialogue mechanisms.

For financial institutions: treat dispute resolution as a strategic investment rather than a cost centre; adopt AI governance frameworks ahead of regulatory mandates; and take active leadership in building the cross-sector collaboration infrastructure the system currently lacks.

For development partners and research institutions: commission a longitudinal Trust Barometer for Nigeria's financial system; support the development of shared AI training datasets relevant to African financial systems; and facilitate cross-country learning that positions Nigeria as an exporter of governance frameworks, not only an adopter of global standards.

The direction these recommendations point to is already gaining official ground. The Central Bank's Payments System Vision 2028, published in June 2026, names trust among its guiding principles and commits to a National Payments Trust Index. This report sets out what systemic trust in platform-led finance consists of and where it breaks down – the architecture any credible attempt to measure it will have to reflect.

Collectively, these recommendations reflect a shift from institution-level optimisation to system-level design – from governing individual actors to designing the architecture that connects them.

NIGERIA'S DIGITAL FINANCE SNAPSHOT

The country's digital financial ecosystem has expanded rapidly, reflecting both scale and complexity.

320 million+

Active bank accounts as of March 2025, with 67.8 million unique BVN holders by end-2025 (NIBSS)

₦1.07 quad.

Electronic payment transactions in 2024 – 78% year-on-year increase, first time Nigeria crossed the quadrillion-naira threshold (NIBSS)

~11 billion

Real-time payment transactions via NIP, placing Nigeria among global leaders in instant payments (NIBSS)

₦71.5 trillion

Mobile money transactions in 2024, with 3.9 billion transaction volumes across 17 licensed operators (NIBSS)

₦25.85 billion

Digital payment fraud losses in 2025 – losses more than doubled since 2021 on the underlying trend; 2024 spike of ₦52.26bn driven by a single ₦31.1bn incident, exposing systemic vulnerability to catastrophic single-point failure (NIBSS Fraud Report, 2026)

> "The question for Nigeria's financial ecosystem is no longer how to move money. It is how to build the confidence that makes people willing to let go of cash."

Global Relevance

These challenges are not unique to Nigeria. India and Brazil, operators of the world's two largest instant payment systems, are confronting the same structural questions of friction and recourse, while Nigeria's Payments System Vision 2028 commits to measuring trust directly. Across markets, the gap between technical capability and public confidence is widening, and the Bridgforte Trust Architecture Framework is designed to be relevant across that landscape.

Looking Ahead

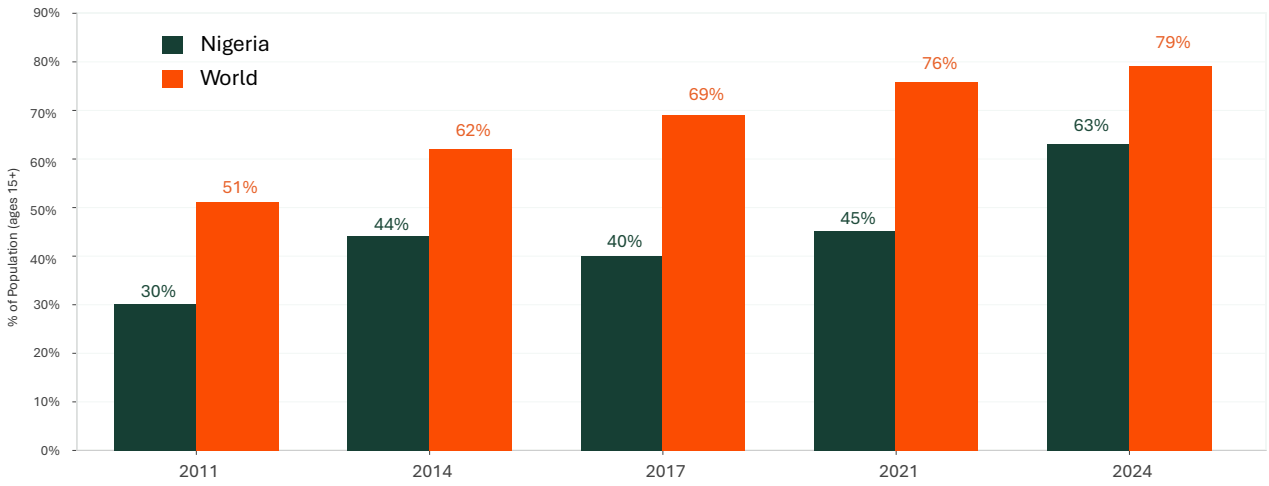
Bridgforte will continue to advance this work through its **Trust Lab** – a research and convening initiative, currently in development, dedicated to trust as a foundational condition of financial system design. The February 2026 Executive Table is the first in a series of structured convenings that will deepen analysis, test governance frameworks, and support coordinated action across the systems and institutions that shape digital financial confidence in Africa.

SECTION I | Introduction

The Confidence Gap in Digital Finance

Across many emerging markets, the first phase of digital financial transformation focused on expanding access: building payment rails, extending identity systems, licensing new providers, and widening participation in formal finance. That phase delivered significant gains – more accounts, widespread digital payments adoption, and financial services reaching populations the traditional banking model never served. Globally, the share of adults with a formal financial account rose from **51% in 2011** to **79% in 2024**, a gain representing **more than a billion people**. Notwithstanding, access has been uneven across populations, income levels, and geographies, and even where it has expanded, it has not reliably translated into sustained usage or durable participation.

Figure 1: Formal Account Ownership: Global Average and Nigeria, 2011–2024



Source: World Bank, Global Findex Database 2025 (data to 2024). Indicator: Account ownership at a financial institution or with a mobile-money-service provider (% of population ages 15+), FX.OWN.TOTL.ZS. worldbank.org/en/publication/globalfindex. Retrieved 2 June 2026. Nigeria figures are Findex estimates and differ from EFInA's Access to Financial Services survey, which uses a different methodology.

At the same time, digital finance has become more layered and interconnected: transactions, identity verification, and service delivery increasingly depend on shared infrastructure, multiple providers, and digital interfaces operating together. This shift reflects a structural change in how financial systems now operate. In an earlier era, a consumer's confidence was anchored in a specific institution – a bank, a branch, a relationship they could identify and hold accountable. In platform-led systems, a single transaction may traverse multiple institutions, infrastructure providers, and algorithmic processes. No single actor controls the full chain. When something goes wrong – a failed transaction, an unresolved dispute, a fraudulent charge – accountability is diffuse, recourse is unclear, and the consumer has no obvious counterpart to turn to. **Reliability, accountability, and user confidence now depend on how well systems coordinate:** how failures are resolved, how risks are shared, and how oversight adapts to interactions that cut across institutional boundaries. Where this architecture is incomplete or misaligned, trust can erode even when access expands and transaction volumes grow. This challenge manifests most acutely in **three areas**: how operational failures are handled when they occur, how artificial intelligence is governed as it is deployed at scale, and whether institutions can build the coordination required to address shared threats collectively.

These developments have introduced a new policy question. It is no longer only whether financial systems can bring people in, but whether they can retain their confidence once they are there.

Nigeria is an important case through which to examine this transition, not because it is typical, but because it has moved further and faster than most. A decade of deliberate policy, shared infrastructure investment, and private innovation transformed what was once a predominantly bank-led system into one of the most active digital financial ecosystems in the world, earning AfricaNenda's 'mature inclusivity' rating. The introduction of the Bank Verification Number in 2014 created a shared identity anchor. The **NIBSS Instant Payment** platform made real-time settlement possible at scale. The licensing of fintechs, payment service banks, and mobile money operators brought millions into formal financial activity. These were deliberate, coordinated achievements.

Nigeria's experience also shows that infrastructure expansion does not by itself produce lasting confidence. As the system has grown, the pressures have become more visible: dispute resolution remains uneven; accountability is often unclear across multi-party transactions; fraud losses remain significant even as case volumes have declined; and coordination across institutions has not developed at the same pace as the infrastructure on which they depend. These are the structural pressures of a system that has advanced rapidly (consequences of scale), and they pose a second-order question: **not whether the system works, but whether people will trust it enough to let go of cash.**

A system in which user confidence remains weak will not be used to its potential. Adoption may rise while reliance remains shallow. Product innovation may continue while the conditions for durable participation remain underdeveloped. These pressures carry implications beyond the financial sector. **Confidence gaps in financial infrastructure affect productivity, investment behaviour, and the velocity of economic activity** – not only the financial sector but the broader economy that depends on it. **The next phase of financial inclusion depends not only on the availability of services, but on the institutional conditions that sustain participation over time**; a shift from asking whether consumers have accounts to asking whether they trust the systems those accounts depend on, and whether that trust is sufficient to make digital finance their default rather than their fallback.

In February 2026, Bridgforte convened a closed-door Executive Table in Lagos, bringing together thirty senior decision-makers from across Nigeria's financial ecosystem, including banks, fintechs, payment infrastructure providers, regulators, and development finance institutions. The discussion was structured around **three interconnected dimensions** of the confidence challenge: operational failure and recourse; the governance of artificial intelligence in financial services, where supervisory frameworks are not keeping pace with deployment and new categories of risk and accountability gap are emerging; and the coordination barriers that prevent institutions from responding collectively to shared threats. This report draws on that discussion, together with structured polling, post-event survey evidence, and supporting research. It applies the **Bridgforte Trust Architecture Framework** – a **five-pillar analytical model** developed to examine the system-level conditions under which digital financial systems can command and retain public confidence – to interpret and synthesise those findings. While grounded in Nigeria's experience, the analytical framework is designed to be applicable across frontier and emerging market financial systems facing analogous structural challenges.

BRIDGFORTE

SECTION II | Background

Trust as an Infrastructure Problem

Nigeria's digital financial ecosystem is the product not of infrastructure alone, but of a deliberate sequence of policy choices, institutional investments, market responses, and private capital mobilisation over more than a decade. Since 2010, when Nigeria aligned itself with the Maya Declaration and adopted an 80% financial inclusion target, policy has provided both the strategic direction and the enabling conditions for ecosystem expansion. The National Financial Inclusion Strategy of 2012 established the regulatory framework that progressively licensed new categories of providers, and shared infrastructure investments made interoperability possible rather than optional. Innovation responded: fintechs, payment service banks, mobile money operators, and digital lenders built products and distribution models that the infrastructure made viable. Investment followed, directing capital toward an ecosystem whose policy foundations had reduced the cost and risk of participation and helped produce several of Africa's most prominent fintech enterprises. **The result was not simply a payments system. It was a layered, platform-driven financial ecosystem whose complexity now presents governance challenges that its original architecture was not designed to manage.**

At the technical core of that architecture sit four foundational shared infrastructure initiatives. The Nigeria Inter-Bank Settlement System (**NIBSS**), incorporated in 1993 and jointly owned by the Central Bank of Nigeria and all licensed deposit money banks, established the central switching and settlement layer that connects every financial institution in the country. The **NIBSS Instant Payment (NIP)** platform, launched in 2011, made real-time interbank transactions possible at scale. The **Bank Verification Number (BVN)**, introduced in 2014 through collaboration between NIBSS and the CBN, created a biometric identity anchor linking customers across institutions. The **Global Standing Instruction (GSI)** added a further accountability layer, enabling cross-institution loan recovery. Together, these initiatives were built not through competition but through deliberate collaboration between the CBN and Nigeria's banking sector: **a jointly owned, jointly governed model designed to serve the system as a whole rather than any single participant**[1].

That collaborative model is also significant beyond its technical achievements. It demonstrates that Nigeria's financial institutions, competitors in every other respect, have previously chosen to build together when the stakes were systemic. NIBSS itself is the institutional embodiment of that choice. **That model of deliberate collaboration established an institutional precedent for system-wide coordination, showing that shared infrastructure could be built collectively when the stakes were sufficiently high.**

These systems allow transactions to be completed seamlessly across banks, fintech platforms, and other service providers in real time. A fully interoperable mobile money framework connects licensed operators across both bank and non-bank channels, while a shared ATM network supports tens of thousands of terminals nationwide.[2] More recently, the introduction of **AfriGO**, developed by the CBN in partnership with NIBSS and launched in January 2023, has added a further layer to the payments ecosystem, positioning Nigeria as the first country in Africa to operate a central bank-led domestic card scheme.[3]

At the continental level, Nigeria has been a founding participant in the **Pan-African Payment and Settlement System (PAPSS)**, developed by Afreximbank in partnership with the African Union and the African Continental Free Trade Area (**AfCFTA**) Secretariat, and has played an active governance role since its launch in 2022.[4] These developments have extended the system beyond national boundaries, introducing cross-border interoperability as an additional and increasingly consequential dimension of system design.

On this foundation, the financial ecosystem has expanded in layers. Fintech platforms have improved user experience and accelerated transaction scale, agent networks have extended physical reach, mobile money operators have brought millions into formal financial activity, and digital lenders have expanded access to credit. Critically, the infrastructure model itself has evolved. The original shared utility model, publicly anchored and jointly owned, has been supplemented by a proliferation of proprietary switching and processing capacity. The CBN has granted full switching licences to private entities including Flutterwave, and major banking groups have established their own fintech switching arms. Paystack and Flutterwave have moved to acquire banking and open banking infrastructure assets ahead of Nigeria's open banking rollout. **The ecosystem's infrastructure is no longer exclusively shared; it is increasingly contested, proprietary, and commercially strategic.**

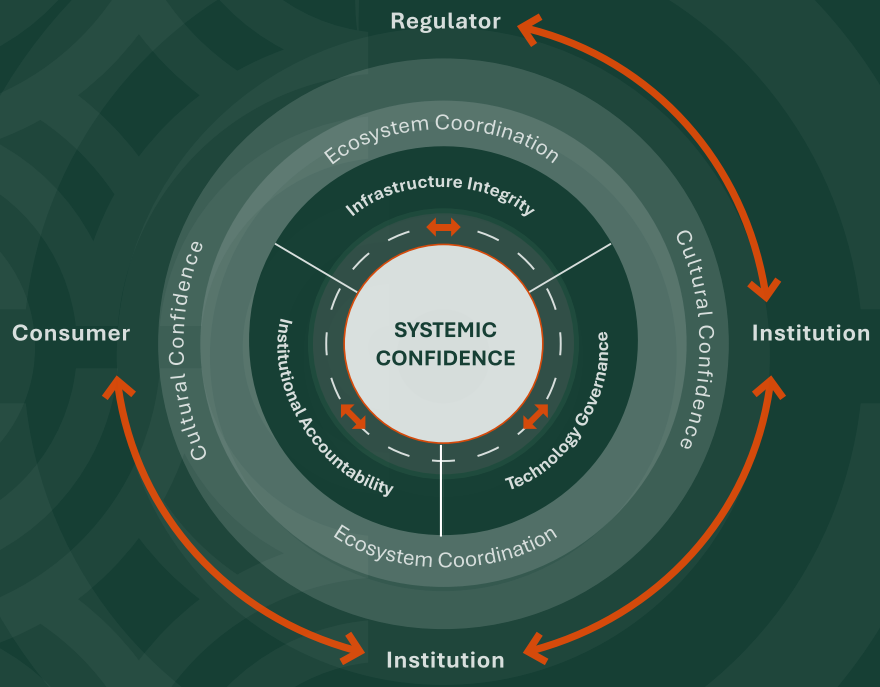
This evolution reflects genuine confidence in the system: private capital building infrastructure is a signal of maturity, not fragmentation. But it introduces a governance dimension that the original shared model did not face. When infrastructure was jointly owned and centrally governed, accountability was collective and oversight was relatively straightforward. As proprietary rails multiply alongside shared ones, transactions increasingly traverse multiple providers and systems, diffusing accountability, complicating oversight, and raising questions about interoperability that the original architecture was not designed to answer. **The coordination complexity this creates is not a peripheral feature of the ecosystem's development; it is the governance dimension this report addresses.**

This expansion has been accompanied by persistent and deepening operational pressures. Fraud losses rose steadily from **₦12.7 billion in 2021** to **₦17.67 billion in 2023**, reflecting the underlying vulnerability trend as transaction volumes expanded. In 2024, losses spiked to **₦52.26 billion** – largely driven by a single fraud incident of **₦31.1 billion** involving one institution, exposing systemic vulnerability to catastrophic single-point failure – before falling to **₦25.85 billion in 2025** following coordinated industry action. Even setting aside the 2024 outlier, losses roughly doubled between 2021 and 2025. The pattern of declining case volumes alongside rising loss values persists throughout: **the system is experiencing fewer but more damaging attacks.** Consumer complaints surged **143% in the first half of 2025**. Pricing opacity and hidden charges remain a persistent source of consumer friction, eroding confidence among users who cannot easily verify the true cost of services. Dispute resolution mechanisms have not kept pace with the scale and speed of digital payments: when failures occur, the path to resolution is often unclear, slow, and contested across institutional boundaries. In many cases, accountability for failures that span multiple institutions remains undefined.

Expanded reach has not translated uniformly into active usage or durable confidence across the system, suggesting that access and trust are no longer moving in parallel. According to **EFInA's Access to Financial Services in Nigeria Survey (2023)**, formal financial inclusion rose to **64% in 2023**, a notable increase from **56% in 2020**. However, approximately **40 million adult Nigerians** remain formally excluded, with exclusion rates considerably higher in rural areas and the north. **Growth in active usage has been slower than account ownership alone would suggest, indicating that expanded access has not translated uniformly into confident and active participation.**

These conditions provide the context within which questions of coordination, accountability, and system reliability in digital financial services must be understood. The system Nigeria has built is capable. The question this report addresses is whether it is, and can be designed to be, trusted.

BRIDGFORTE



SECTION III

The Bridgforte Trust Architecture Framework

Why a Trust Architecture Framework is Needed

Platform-led financial systems expose a problem that institution-level analysis cannot fully resolve. Institutional soundness remains necessary, but it is no longer sufficient to explain why confidence holds or fails. A consumer may interact with one provider while depending in practice on multiple infrastructures, intermediaries, and governance arrangements operating behind the interface. Confidence therefore depends not only on the conduct of individual institutions, but on the quality of the system connecting them.

If confidence failures are treated only as institutional failures – problems of individual performance, compliance, or product quality – the response will also be institution-centric: more regulation, better supervision, stronger firm-level consumer protection. These responses are necessary but insufficient. In platform-led systems, confidence also depends on the design of the shared infrastructure, accountability frameworks, and coordination mechanisms that connect actors across the system. **Existing categories such as inclusion, consumer protection, innovation, and stability each capture an important part of this picture. What they do not fully capture is the architecture through which confidence is sustained across interconnected systems. The Bridgforte Trust Architecture Framework is intended to address that analytical gap.**

Across facilitated discussion, structured polling, and post-event survey responses, participants at the Executive Table repeatedly described failures that did not sit neatly within any one institution or function. Trust breakdowns were discussed not only in terms of product design or institutional performance, but in terms of recourse, coordination, accountability, interoperability, and governance across shared systems. **The Framework is introduced here as a way of organising and interpreting those patterns.** It is neither a summary of participant opinion nor an abstract model imposed from outside the discussion. It is an analytical structure, grounded in the theoretical traditions set out below, through which the institutional conditions the discussion consistently surfaced can be understood. The Framework informed the design of the session and was in turn tested against what the discussion revealed.

DEFINITION OF TRUST ARCHITECTURE

Trust Architecture refers to the institutional configuration of a financial system that determines whether participants – including consumers, institutions, and regulators – can operate with confidence in the system as a whole, independent of their direct experience with any single actor within it. It describes the **shared arrangements** through which confidence is **built, sustained, and restored**: the infrastructure on which transactions depend, the accountability frameworks that assign responsibility when failures occur, the governance mechanisms that constrain automated systems, and the coordination structures that enable collective responses to shared threats. **Trust Architecture is not a property of any single institution in isolation, but of the system-level arrangements through which institutions interact. Financial stability, consumer protection, and regulatory compliance each presuppose something Trust Architecture makes explicit: the system must be designed to merit confidence with every transaction.**

Conceptual Foundations

The Framework draws on established traditions of thought on trust and institutions, while applying them to the realities of contemporary digital finance.

Niklas Luhmann provides the first foundation through his distinction between personal trust and system trust. As complexity increases, confidence shifts from direct familiarity with individual actors to reliance on institutional systems whose internal workings users cannot fully observe. In digital finance, this means that confidence is no longer secured primarily by a personal relationship with a bank, but by trust in the wider system through which transactions, identity, and recourse are managed.[5]

Anthony Giddens provides the second through his account of abstract systems and access points. In modern institutional life, confidence depends not only on back-end robustness, but on the interfaces through which people encounter systems in practice. In digital finance, these access points include onboarding, authentication, payment execution, dispute resolution, and recourse. Failures at these points can undermine confidence even when the underlying infrastructure remains technically functional.[6]

Douglass North provides the third through his emphasis on institutional configuration. Outcomes are shaped not only by the capabilities or intentions of individual actors, but by the rules, incentives, and structures within which they operate. Applied to digital financial systems, this means that confidence depends not only on institutional performance, but also on how shared infrastructure, accountability frameworks, and coordination mechanisms are designed across the system.[7]

Taken together, these contributions point to the same conclusion: in platform-led financial systems, trust is an architectural property. It is produced – or eroded – by the design of the system as a whole. The Bridgforte Trust Architecture Framework is built on that premise.

The Five Pillars of the Framework

The Bridgforte Trust Architecture Framework identifies **five interdependent pillars** of systemic confidence. Each addresses a distinct failure mode. None is sufficient in isolation. Together, they define the conditions under which digital financial systems can sustain confidence over time.

Table 1: The Framework at a Glance

Pillar	Addresses	Failure Mode	Institutional Implication
Infrastructure Integrity	Reliability of payment systems, identity architecture, and cybersecurity	Transaction failures and fragmented identity undermine foundational confidence	Shared infrastructure investment must be treated as a systemic priority
Institutional Accountability	Clarity of responsibility across multi-party transaction chains	Accountability diffusion creates consumer vulnerability and weakens system-level trust	Liability, recourse, and supervisory visibility must be clearly defined across institutional boundaries
Technology Governance	AI oversight, explainability, contestability, and auditability	Algorithmic opacity, embedded bias, and governance lag generate confidence deficits as AI scales	Governance of automated systems must be embedded early, not added after deployment
Ecosystem Coordination	Fraud intelligence sharing, cybersecurity collaboration, and structured regulatory dialogue	Institutions face shared threats but continue to respond in isolation	Collective defence mechanisms and neutral coordination structures are required for system resilience
Cultural Confidence	Consumer education, relational trust signals, transparency, and user experience	Technical robustness does not automatically translate into public confidence	Trust must be reinforced through both system performance and public experience

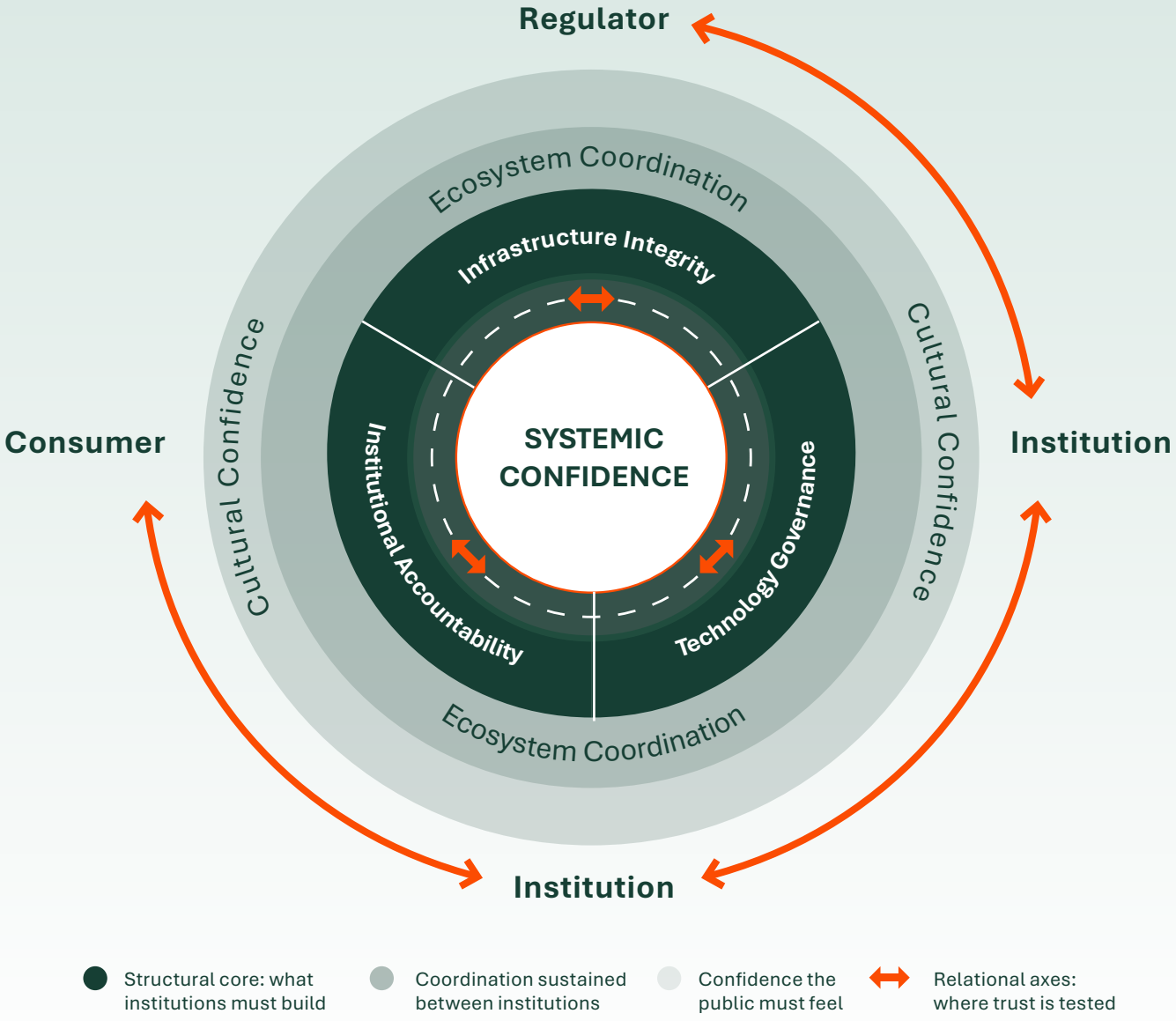
Source: Bridgforte analysis, informed by insights from the Bridgforte Executive Table (Lagos, February 2026), including structured participant polling and facilitated discussion.

The five pillars are interdependent. Weakness in any one places pressure on the others. Fragmented identity infrastructure undermines both Institutional Accountability and Ecosystem Coordination. Weak Technology Governance can erode Cultural Confidence. Poor Ecosystem Coordination amplifies the consequences of Infrastructure Integrity failures. **The pillars are therefore most usefully understood not as a checklist, but as a system – the analytical equivalent of the interconnected architecture they are designed to assess.**

Figure 2

The Bridgforte Trust Architecture Framework

Five Pillars of Systemic Confidence



The framework shows how systemic confidence is built, sustained and restored through five interdependent pillars and three relational axes. The pillars describe the structural conditions that produce confidence; the relational axes show where trust is experienced, tested and broken in practice.

Source: Bridgforte analysis, informed by insights from the Bridgforte Executive Table (Lagos, February 2026)

Applying the Framework Through Relational Axes

The Framework becomes operationally useful when applied to the relationships through which trust is experienced in practice. The Executive Table was therefore structured around **three relational axes: Consumer to Institution, Institution to Institution,** and **Institution to Regulator.**

The **Consumer to Institution** axis captures the point at which confidence becomes visible in everyday use: failed transactions, hidden charges, authentication problems, disputes, and recourse. When a consumer cannot resolve a failed transaction or identify who is responsible for a loss, the failure is architectural: it reflects the absence of clear liability frameworks and accessible recourse pathways, not merely poor customer service. Breakdowns along this axis map most directly to **Institutional Accountability**, while also bearing on Infrastructure Integrity and Cultural Confidence.

The **Institution to Institution** axis captures how actors coordinate across shared systems and shared threats. This includes fraud intelligence, interoperability, switching, cybersecurity, and multi-party responsibility. These are not failures of individual institutional capability alone; they are failures of shared architecture. Breakdowns along this axis map most directly to **Ecosystem Coordination**, with implications for Infrastructure Integrity.

The **Institution to Regulator** axis captures the relationship between regulated institutions and supervisory authorities. It includes rule clarity, regulatory responsiveness, supervisory dialogue, and the ability of oversight models to keep pace with technological and platform-based change. Breakdowns along this axis map most directly to **Institutional Accountability** and **Technology Governance.**

These relational axes do not replace the Framework's pillars. The pillars describe the structural conditions that produce confidence. The relational axes describe where confidence is experienced, tested, and broken in practice. Together, they provide the analytical architecture through which the Executive Table findings are interpreted in the sections that follow.

Positioning Relative to Existing Frameworks

The Bridgforte Trust Architecture Framework is intended to complement, not replace, existing approaches to financial system governance. This includes the **Alliance for Financial Inclusion's** digital financial services framework, which focuses on the regulatory pillars required for functionality, inclusion, and risk management; **CGAP's** work on consumer protection and responsible finance; and the operational resilience and stability standards associated with institutions such as the **Bank for International Settlements**, the **Financial Stability Board**, and the **G20 Global Partnership for Financial Inclusion**.

These frameworks each address important dimensions of financial system performance. The Bridgforte Framework operates at a different level of analysis. It does not ask only whether systems are functional, compliant, inclusive, or stable. **It asks whether the institutional conditions exist for those systems to remain credible once access has been established and transactions are occurring at scale.** The distinction is therefore additive rather than competitive. Bridgforte is not proposing an alternative to existing regulatory thinking. It is identifying an analytical layer that those frameworks do not fully address.

The same positioning applies to national strategy. Nigeria's Payments System Vision 2028 addresses the payments system, treating it as an ecosystem of stakeholders to be aligned around shared objectives, with trust among its guiding principles. The Bridgforte Framework is both wider and differently focused: its subject is platform-led finance as a whole (payments, but also the identity infrastructure, algorithmic decision-making and data governance through which financial services increasingly run) and it starts from the observation that in such systems, risk accumulates not within the institutions to be aligned but in the spaces between them, where no single actor is accountable and where trust is most easily lost. The Vision sets a national objective for trusted payments; the Framework examines where trust across the wider architecture is made and broken.

The sections that follow apply this framework to the operational realities, governance pressures, and coordination failures emerging within Nigeria's digital financial system. The aim is not to force observed patterns into an abstract model, but to clarify how they relate to the institutional conditions on which public confidence depends.

BRIDGFORTE

SECTION IV | Core Analysis

How Trust Breaks Down in Practice

The findings that follow are organised thematically to reflect the structure of the Executive Table discussion. Each theme is mapped to one or more pillars of the Bridgforte Trust Architecture Framework and to the three relational axes – Consumer to Institution, Institution to Institution, and Institution to Regulator – through which trust is formed, tested, and broken in practice. The purpose is not to describe individual institutional failures, but to identify the structural conditions that produce them. **The analysis that follows explains where those pressures are most visible and how they map onto the Framework.**

A. Where Trust Breaks Down: Operational Realities

Primary pillar: Institutional Accountability. Secondary pillar: Cultural Confidence
Primary relational axis: Consumer to Institution

The analysis begins with a distinction that recurred throughout the Executive Table: **financial inclusion is not equivalent to digital confidence**. Participants were clear that access alone is insufficient. A user may hold an account, transact digitally, and still remain uncertain whether the system will protect them when something goes wrong. Trust, in that sense, is not simply an attribute of products. It is an operating condition of the system itself.

Structured polling reinforced this point. Participants ranked **transaction failure / service reliability** and **dispute resolution and recourse** as the most significant trust breakdown points in the ecosystem, ahead of fraud, pricing opacity, KYC frictions, data privacy, and artificial intelligence. The ranking is analytically significant. It suggests that the most immediate drivers of confidence erosion are not the most technologically complex ones. They are the failures users encounter directly: payments that do not complete, charges that cannot be explained, losses that cannot be traced, and complaints that do not reach timely resolution.

Table 2: Trust Breakdown Points in Nigeria's Digital Financial Ecosystem (Participant Ranking)

#	Category	Score (out of 8)
1	Transaction failure / service reliability	6.8
2	Dispute resolution and recourse mechanisms	6.0
3	Fraud and scams	5.7
4	Pricing opacity or unexpected charges	5.1
5	Onboarding, KYC, and identity processes	4.5
6	Regulatory unpredictability	2.8
7	Data privacy and cybersecurity	2.1
8	AI decision-making	0.7

Source: Bridgforte Executive Table participant polling, Lagos, February 2026.
Scores reflect relative prioritisation across thirty participants and are indicative of ranking rather than precise magnitudes.

What matters for confidence is not simply whether systems fail, but how they behave when they do. Participants repeatedly returned to the view that failures are inevitable in complex financial systems; the critical determinant of trust is whether resolution is clear, timely, and fair. One participant cited Nigeria's Central Securities Clearing System as evidence that reliability and high transaction volumes can coexist. Yet in large parts of retail digital finance, when failures occur, the experience of recourse remains uneven – and it is that experience, amplified by social media, that shapes confidence.

Three related dynamics emerged strongly from the discussion.

Asymmetric Perception Dynamics

The majority of transactions may complete without incident, yet negative experiences shape public perception disproportionately. Customer satisfaction, however, is typically unexpressed, while frustration is amplified through social media, messaging platforms and word of mouth. **Confidence is therefore more sensitive to visible failure and poor recourse than to aggregate performance statistics.**

> "Satisfaction is structurally silent; frustration is structurally viral."

Cash as the Enduring Competitor

Despite the growth of digital payments, cash remains the formal financial system's most resilient competitor. This is not simply because cash is familiar, but because it offers certainty: immediacy, visibility, and control. In practice, **cash functions as a benchmark against which digital trust is judged.** Where fraud exposure, unexplained charges, or unresolved failures persist, users revert to cash not because digital channels are unavailable, but because they remain conditionally trusted.

The Informal Trust Paradox

Participants also pointed to the persistent strength of informal finance. Informal providers often command greater trust than formal institutions despite offering fewer legal protections and less sophisticated products. The explanation lies less in technical capability than in relational design: familiarity, responsiveness, empathy, and clear, socially embedded pathways for recourse. Formal systems have not yet translated these features into credible digital equivalents. **This highlights Cultural Confidence as a structural dimension of trust, not a behavioural anomaly.**

> **INCLUDED BUT VULNERABLE**
> People can be financially included but digitally excluded: inside the formal system, but vulnerable to it. This makes the trust challenge a matter of consumer protection and institutional accountability, not merely product design or technology adoption.

B. Identity Infrastructure as the Structural Root

Primary pillar: Infrastructure Integrity
Secondary pillars: Institutional Accountability; Ecosystem Coordination

Identity infrastructure emerged as the most consistently cited determinant of trust across the discussion. Participants identified fragmented KYC processes, inconsistent NIN implementation, and the inability to trace accounts to verified individuals as factors that simultaneously enable fraud, weaken consumer recourse, and diffuse institutional accountability. **That breadth of impact, spanning fraud prevention, consumer protection, and institutional governance at the same time, makes identity the highest-leverage point for system-level intervention.**

A key policy implication followed from this diagnosis: **identity should be treated as a public good, not an institutional compliance cost.** When identity functions as shared infrastructure rather than as a fragmented institutional process, it improves fraud prevention, reduces onboarding friction, strengthens consumer recourse, and clarifies accountability. Without reliable identity infrastructure, the financial system is constructing sophisticated products on an unstable foundation.

Nigeria possesses important components of a national identity architecture but has not yet achieved the interoperability and operational reliability required to deploy it as a trust anchor across institutions. The **BVN** and **NIN** systems represent significant foundational investments. The policy challenge is not their existence but their integration: the creation of a seamless verification environment that institutions can rely upon without duplicating effort or accepting inconsistent results. **This is, fundamentally, a transition from asset creation to system integration.**

A related observation concerned consumer perceptions of data privacy. Participants noted that many consumers express caution about sharing personal data with financial institutions while disclosing extensive information on social media platforms. This suggests that the trust challenge around data is not simply about disclosure, but about perceived value and control. Consumers will share data if they believe there is clear benefit and they retain meaningful agency over its use. The design of privacy practices – how institutions explain data use, what control mechanisms they offer, and how they respond to breaches – matters as much as the substance of those practices. **Trust in data privacy is therefore shaped not only by policy, but by institutional behaviour.**

Identity, in this sense, is not just an onboarding matter. It is a trust anchor.

C. Instant Payments: A Structural Design Tension

Primary pillar: Infrastructure Integrity Secondary pillar: Technology Governance

Real-time payments have been one of the major achievements of Nigeria's digital financial transformation. But they also reveal one of its central design tensions: the very qualities that make instant payments attractive – speed, immediacy, irrevocability, and convenience – also increase the consequences of failure when safeguards do not evolve alongside the infrastructure.

The challenge is not whether to pursue fast payments. Their inclusion and efficiency benefits are well established. The challenge is how to embed risk management within payment architecture without undermining the speed that drives adoption. **This is why the issue is best understood not as a product problem, but as a system-design problem.**

The fraud trend illustrates this clearly. Losses rose from **₦12.7 billion in 2021** to **₦17.67 billion in 2023**, then spiked to **₦52.26 billion in 2024**, driven largely by a single **₦31.1 billion** incident, before falling to **₦25.85 billion in 2025** following coordinated industry action. **The scale of that outlier exposed how much damage a single point of failure can impose on a fast-moving system.** Even setting aside the 2024 outlier, the pattern remains clear: fewer recorded incidents, but more damaging ones. **The system's fraud problem is less about volume than consequence.** Social engineering, account compromise, and fraudulent merchant transactions – fraud vectors structurally enabled by the speed and irrevocability of instant payments – have displaced higher-volume, lower-value attacks.

This matters because instant payments compress the time available for intervention. Once funds move beyond recall, losses are realised quickly and often irreversibly. Participants discussed a number of possible design responses, including behavioural anomaly detection, transaction velocity limits calibrated to risk, and narrowly targeted delays where defined thresholds are triggered. **The common principle was proportionality: risk controls should be embedded in the architecture itself, not layered on as blunt friction after the fact.**

> **EMBEDDING SAFETY IN FAST-PAYMENT DESIGN**
>
> The instant payments dilemma is not a reason to slow the development of real-time payment infrastructure. It points instead to the need to treat fraud prevention architecture as a founding requirement of fast-payment design. Safety mechanisms must be built into payment rails from inception, not retrofitted after fraud losses have accumulated.

D. Artificial Intelligence: Trust Amplifier and Systemic Risk

Primary pillar: Technology Governance

Artificial intelligence featured in the Executive Table less as a present crisis than as an emerging governance frontier. Discussion was anchored by a plausible scenario: a fabricated AI-generated video purporting to show the chief executive of a major Nigerian bank warning of liquidity stress. The scenario mattered not because it was dramatic, but because it illustrated how confidence could be destabilised system-wide without any underlying institutional weakness.

The issue is not simply technological capability. It is the asymmetry between the falling cost of generating convincing synthetic content and the rising institutional burden of verification. **Without rapid verification mechanisms – technical, institutional, and regulatory – misinformation alone could trigger systemic financial stress.** Where systems for verification, contestability, and coordinated response are weak, AI can amplify trust shocks even before it becomes deeply embedded in financial decision-making.

Current Perceptions Among Senior Practitioners

Seventy-two per cent of participants selected "too early to assess" when asked about AI's current trust impact – a distribution that confirms the watchful rather than crisis framing. Most did not describe AI as already eroding trust directly. Instead, they located the principal risks in **governance failure**: misuse of data, lack of explainability, biased decision-making, and inadequate mechanisms for challenge and redress. That indicates a limited but important governance window. Systems have not yet fully absorbed the consequences of AI deployment, which makes this a moment for institutional design rather than reactive damage control.

Table 3: Greatest Trust Risks from AI in Financial Services (Participant Assessment)

#	Category	Respondents
1	Data misuse or privacy breach	37%
2	Lack of explainability in automated decisions	32%
3	Bias in credit or pricing decisions	21%
4	Automated dispute handling	5%
5	Regulatory lag behind AI adoption	5%

Source: Bridgforte Executive Table participant polling, Lagos, February 2026.
Scores reflect relative prioritisation across thirty participants and are indicative of ranking rather than precise magnitudes.

Participants located the primary AI risks in governance – how AI is overseen, explained, and contested – rather than in the technology itself. Nine in ten participants located the greatest risk in data misuse, explainability failures, or embedded bias. The appropriate response is therefore not to slow adoption indiscriminately, but to strengthen the governance architecture around it.

The Dual-Use Challenge

The same algorithmic capability that powers fraud detection can also enable deepfake video generation. The same credit-scoring models that extend access to underbanked consumers can also embed and scale historical bias present in training data. Governance frameworks must address both sides of this duality. They cannot be designed only to promote beneficial applications; they must also constrain harmful ones. **The discussion suggests that governance, rather than capability, is the defining challenge of AI deployment in financial systems.**

As one participant observed, yesterday's inequities can become tomorrow's infrastructure unless institutions actively intervene to correct for historical bias in training data. This points to a governance requirement that extends beyond explainability. It requires active monitoring, regular auditing, and a willingness to modify or retire models whose real-world effects diverge from design intent. **The challenge is not whether AI is beneficial or harmful. It is whether its deployment is governed well enough to preserve confidence.**

The Board Governance Deficit

Three diagnostic questions emerged as a practical test of institutional AI readiness. Do boards exercise explicit oversight of AI model performance, including bias testing, performance drift monitoring, and explainability standards? How are institutions monitoring AI's differential impact across demographic segments? How are automated decisions explained to affected individuals, and through what mechanisms can those decisions be challenged?

The candid assessment in the room was that most boards are not yet equipped to answer these questions with confidence. **The gap between AI deployment and AI governance is not a technical gap; it is a structural one, and it is widening.**

THE EMERGING TRUST EQUATION IN THE AGE OF AI

Trust in AI-driven financial services **requires at least three institutional conditions** working in tandem: **explainability** (can the decision be understood by those affected?), **contestability** (can the decision be meaningfully challenged?), and **resolution** (can redress be obtained when the decision is wrong?). Together, these conditions define the requirements for AI-enabled financial systems to remain credible.

E. The Collaboration Paradox: Structural Barriers to Collective Defence

Primary pillar: Ecosystem Coordination
Secondary pillars: Infrastructure Integrity; Institutional Accountability
Primary relational axis: Institution to Institution

Perhaps the clearest structural insight to emerge from the Executive Table was that financial institutions often collaborate less effectively than the fraud networks targeting them. The cause is structural rather than moral. Criminal networks face no competitive barriers to information sharing. Financial institutions face many: competitive instinct, reputational risk, regulatory uncertainty around data exchange, and legal ambiguity about the permissibility of information-sharing arrangements. The result is a systemic weakness in **Ecosystem Coordination** rather than a series of isolated institutional failures.

The consequence is a structural asymmetry. Individual institutions invest heavily in their own defences while collective vulnerabilities continue to grow. Fraud intelligence that could allow one institution to protect many is instead siloed. Threat patterns that have appeared at one bank re-emerge at others weeks or months later because early warning signals are not shared quickly enough, or at all.

Table 4: Barriers to Collaboration in Nigeria's Financial Ecosystem (Participant Ranking)

#	Category	Score (out of 8)
1	Institutional mistrust between competitors	6.6
2	Competitive incentives to hoard information	6.5
3	Absence of leadership to convene collective action	4.6
4	Regulatory uncertainty around data sharing	3.3
5	Legal or data protection constraints	3.2
6	Cost and commercial viability concerns	2.8
7	Technological limitations	2.0
8	High operational costs	1.7

Source: Bridgforte Executive Table participant polling, Lagos, February 2026.
Scores reflect relative prioritisation across thirty participants and are indicative of ranking rather than precise magnitudes.

The ranking is revealing. Institutional mistrust and competitive incentives dominate the barrier landscape, while regulatory uncertainty, legal constraints, cost, and technology rank materially lower. **The primary barriers to collaboration are therefore relational and structural, not legal or technical.** Regulatory reform alone will not resolve them. They require institutional design: trust-building mechanisms, neutral intermediaries, and in some cases mandatory participation frameworks. **The binding constraint is not capability, but coordination architecture.**

The Bank-Fintech Fault Line

A specific collaboration gap was identified as particularly consequential: the persistent disconnect between banks and fintechs. Fintech-to-fintech and bank-to-bank coordination function reasonably well within their own categories. Bank-to-fintech collaboration remains much weaker, even though these institutions increasingly share operating environments, customer populations, and infrastructure. This fragmentation weakens both innovation efficiency and system resilience. **Trust failures increasingly emerge at the intersections between institution types, not only within them.**

Proven Precedents for Shared Infrastructure

Nigeria's most effective domestic trust infrastructure – including **BVN, NIBSS, and the GSI** – was built through cooperative investment rather than competitive differentiation. At the continental level, Nigeria's active participation in **PAPSS** reflects the same principle applied to cross-border payments. Each emerged from recognition that some infrastructure is more valuable as a shared utility than as a proprietary asset. The case for applying the same logic to fraud intelligence, cybersecurity capacity, and AI training data is therefore not merely theoretical; Nigeria's own track record suggests it is viable.

The **Nigeria Electronic Fraud Forum (NeFF)** has demonstrated since 2011 that cross-institutional fraud collaboration, when properly convened and backed by regulation, can produce measurable results. Open banking infrastructure, whose framework and operational guidelines are finalised and awaiting CBN go-live confirmation, will establish standardised data-sharing rails between banks and licensed third parties. But **NeFF** is advisory and voluntary, and open banking addresses data interoperability rather than the broader governance of shared threats. The financial system still lacks a standing cross-sector body with a mandate spanning all institution types and addressing trust as a systemic challenge beyond any single domain.

Concrete proposals emerging from the discussion included a **National Cybersecurity Centre** that would aggregate institutional budgets into shared continuous monitoring and threat response capability; an anonymised fraud data-sharing platform, potentially using distributed ledger technology, overseen by a neutral body with regulatory authority; and shared AI training datasets that would improve model accuracy while reducing cost burdens on individual institutions.

These precedents show that coordination failures are not inevitable. They are, at least in part, design choices. Collaboration must therefore be designed, not assumed.

F. Reimagining the Regulatory Relationship

Primary pillar: Institutional Accountability
Secondary pillar: Ecosystem Coordination
Primary relational axis: Institution to Regulator

A recurring theme in the Executive Table was the changing nature of the relationship between institutions and regulators. Participants did not primarily describe a crisis of legitimacy. Rather, they described a growing mismatch between supervisory models designed for discrete institutions and systems in which risk emerges through interaction, interdependence, and technological change.

Institutions often reported feeling heavily engaged on process, but less engaged on the underlying system questions that matter most: how accountability should be assigned across multi-party failures, how AI deployment should be governed, how regulatory dialogue should function in fast-moving areas of innovation, and how systemic risk should be addressed where no single actor fully contains it.

What emerged was a call for a philosophical shift in supervisory approach: from mandate-based regulation, which prescribes how institutions must operate, to **outcome-based supervision,** which defines what results the system must achieve while allowing greater flexibility in how institutions achieve them. This implies a move from controlling institutional behaviour to shaping system outcomes. Participants argued that innovation should help inform where regulation needs to go, rather than waiting for regulation to define the boundaries within which innovation is permitted.

At the same time, there was clear recognition of the constraints regulators face. Innovation is moving faster than regulatory understanding in many technological domains. Technical expertise is unevenly distributed within supervisory institutions. The volume of entities and products requiring oversight continues to expand faster than supervisory capacity. Participants were divided on the implications: some saw this capacity gap as grounds for greater industry self-regulation in defined areas; others argued that the regulator's mandate for systemic stability gives both the authority and the obligation to build capacity rapidly.

This capacity gap strengthens the case for structured dialogue: regulators need access to practitioner knowledge, and practitioners need regulatory engagement that is substantive rather than purely compliance-oriented. A practical proposal that commanded broad support was the creation of standing mechanisms between operators and regulators, not as crisis-driven consultations but as regular channels for substantive engagement. **Such dialogue requires a neutral convener trusted by all parties.** Sustained coordination between regulators and operators is itself part of trust architecture.

Clear liability frameworks for cross-institutional failures are a prerequisite for effective consumer protection. Where fraud originates in one institution, passes through another, and settles with a consumer served by a third, the current architecture often produces fragmented accountability rather than a unified response. **When responsibility cannot be explained across a multi-party transaction, redress becomes harder to secure and confidence weakens accordingly.**

The Overall Trust Assessment

The findings across each of these dimensions provide the context within which the room's overall assessment must be read. **After working through the specific failure dimensions discussed in this section, participants were asked to rate trust resilience in Nigeria's financial ecosystem on a scale of 1 to 10.** The average score was **5.4**. Scores clustered between **3 and 8**, with the largest single group selecting **5**.

A middling score might appear inconclusive. It is not. These are the chief executives, board directors, and senior institutional leaders closest to the system's performance and most invested in its credibility. Their collective assessment, after considering the failure dimensions surfaced in the discussion, was neither confidence nor alarm, but caution. In a system that depends on confidence, such caution speaks for itself.

The score therefore carries more than descriptive value. It reflects a measured and guarded assessment from the senior cohort responsible for Nigeria's financial infrastructure: a recognition that the system is capable, but that its confidence architecture remains uneven.

THE CONFIDENCE GAP

Trust is not a feature of the financial market. It is one of its operating conditions. The gap between what the system can do technically and what it can sustain in public confidence is the defining governance challenge of this phase of Nigeria's financial development.

Synthesis

Taken together, these themes point to a common conclusion. The most important trust failures in Nigeria's digital financial ecosystem are not isolated incidents or purely institutional weaknesses. They are interdependent failures arising at the intersection of **infrastructure, accountability, governance, and coordination**. This is why trust cannot be treated as a by-product of institutional performance alone. It is shaped by the system-level conditions through which institutions interact, users experience the system, and failures are resolved.

The next section turns from analysis to implication: what these findings mean for the design, governance, and regulation of digital financial systems.

BRIDGFORTE

SECTION V | Policy Implications

From Institutional Performance to System Design

The findings in Section IV reveal a consistent pattern across each of the six analytical dimensions examined: trust failures in platform-led financial systems are not primarily institutional failures. They arise in the shared arrangements, governance structures, and coordination mechanisms that connect institutions and determine how the system performs under pressure. The policy implications that follow reflect a corresponding shift: from institution-centric models of oversight, in which systemic confidence is treated as the aggregate of individual institutional performance, to system-level approaches that treat trust as a design property of the architecture as a whole.

These implications are addressed to the system rather than to any single actor. They do not prescribe specific interventions, but identify the structural changes in thinking, design, and governance that the evidence demands. They extend beyond Nigeria's immediate context and are relevant to any financial system undergoing rapid digital transformation.

1. Trust must be treated as a system design objective, not an institutional outcome

The traditional assumption in financial governance is that systemic confidence is built through the performance and integrity of individual institutions: that if each actor is well governed, financially sound, and consumer-oriented, public trust will follow. The findings challenge this assumption directly. Platform-led systems have fundamentally changed where accountability sits. When a transaction spans multiple actors and something goes wrong, no single institution is clearly responsible – and no single institution can fully remedy the failure. Trust at system level depends on the design of the shared arrangements between actors, not on the performance of any one of them.

Institutional soundness alone is no longer sufficient to generate systemic confidence. Trust must be deliberately designed into the system architecture through clear allocation of responsibility across multi-party transaction chains, reliable shared infrastructure, and governance frameworks capable of managing interdependencies across actors. This is not a refinement of existing approaches. It is a reorientation of the policy frame: from supervising institutions to designing systems.

2. Operational reliability and recourse are primary drivers of confidence

Prevailing assumptions about the drivers of financial confidence tend to focus on innovation, product quality, and access expansion. The Executive Table evidence tells a different story. Transaction failure and dispute resolution ranked at the top of every breakdown point assessment. Data privacy, cybersecurity, and AI decision-making ranked at the bottom.

This should pivot the focus of policy from enabling innovation to ensuring reliability. The credibility of digital financial systems rests heavily on how they respond when transactions fail, disputes arise, or consumers are exposed to loss, much more than on what they deliver when things go well. Effective recourse mechanisms, clear dispute resolution pathways, and transparent communication during system failures are therefore central, not peripheral, to financial system design.

3. Identity infrastructure is foundational to system integrity

Identity infrastructure emerged from the discussion as a critical enabler – and in its current state, a persistent inhibitor – of trust across multiple dimensions simultaneously. Fragmented KYC processes, inconsistent NIN implementation, and the inability to trace accounts to verified individuals enable fraud, weaken consumer recourse, and diffuse institutional accountability at the same time. No other single factor identified in the discussion operates across that breadth of system failure simultaneously.

Without a unified and interoperable identity layer, financial systems cannot reliably link transactions to verified individuals, enforce responsibility across institutions, or provide effective recourse to consumers. Identity must therefore be treated as shared infrastructure – a public good that underpins the integrity of the entire system – rather than as a compliance function managed independently by individual institutions. The policy challenge is not the creation of identity assets, which Nigeria already has in the BVN and NIN systems. It is their integration into a seamless, interoperable verification environment that the system as a whole can rely upon.

4. Risk management must be embedded within system architecture

The increasing speed and complexity of digital financial systems – particularly through real-time payments and AI-enabled decision-making – have fundamentally altered the nature of risk. Risks now emerge at the velocity and scale of the system, frequently outpacing the capacity of traditional

institution-level controls. Once funds move beyond recall in a real-time system, losses are realised immediately. Once an AI model embeds bias into a credit-scoring process, it scales at the rate of the model's deployment. The reactive risk management model in which institutions identify, assess, and respond to risks after they emerge, is structurally misaligned with the systems it is meant to govern.

This reality requires a shift from reactive risk management to embedded risk design. Fraud prevention, anomaly detection, and governance mechanisms must be integrated directly into financial infrastructure from inception, not layered on top of it after deployment. In fast-moving systems, the question is no longer whether risks can be eliminated, but whether systems are designed to detect, absorb, and resolve them without undermining confidence. Risk architecture is therefore a founding design requirement, not an operational afterthought.

5. Coordination is a structural requirement, not a voluntary choice

The analysis reveals a persistent and structurally significant coordination failure: institutions operate in shared environments, face shared threats, and depend on shared infrastructure – but respond to those threats individually. The Executive Table polling confirmed that the primary barriers to collaboration are not regulatory or legal, but relational and competitive. Institutional mistrust and competitive incentives to hoard information ranked significantly above legal constraints, regulatory uncertainty, and technological limitations.

Effective defence against fraud, cyber threats, and systemic risks requires coordinated responses across institutions. That coordination cannot depend on voluntary participation, which the evidence shows has been systematically undermined by competitive dynamics. It must be supported by formal mechanisms: shared intelligence platforms with binding participation, neutral convening structures with mandates that span all institution types, and regulatory frameworks that enable and where necessary require collective action. Nigeria's own track record – BVN, NIBSS, GSI, NeFF – demonstrates that this is achievable. Coordination failures are not inevitable, they are design choices that can be recalibrated.

6. Regulatory models must evolve from institutional oversight to system governance

Regulatory frameworks designed to supervise discrete institutions were developed for a financial architecture in which risk was primarily located within individual actors. Platform-led financial systems have changed that architecture fundamentally. Risk now arises from interactions between institutions, from the gaps, interfaces, and coordination failures between actors, rather than from the behaviour of any single one. A regulator monitoring each institution's compliance and soundness in isolation cannot observe, let alone govern, the systemic risks that emerge from how those institutions interact.

Supervisory approaches must therefore evolve from monitoring institutional compliance to shaping system governance. This includes developing frameworks for cross-institutional accountability that assign responsibility when failures span multiple actors; strengthening regulatory capacity in emerging domains such as artificial intelligence, where supervisory understanding has not kept pace with deployment; and creating structured channels for ongoing dialogue between regulators and market participants that are substantive rather than compliance-oriented. The role of regulation shifts from controlling institutional behaviour to governing system dynamics: from asking whether each institution is sound to asking whether the system as a whole can be trusted.

7. Cultural confidence is a policy variable, not a behavioural by-product

The persistence of cash and the relative trust commanded by informal financial providers (despite their offering fewer legal protections

and less sophisticated products) highlight that confidence in financial systems is not determined solely by technical performance or regulatory compliance. It is also shaped by perception, experience, and the relational signals that institutions provide to users. Consumers judge financial systems not only on what they can do, but on how they communicate, how they respond when things go wrong, and whether they feel known and valued as participants rather than processed as customers.

This implies that cultural confidence is a policy variable: one that requires deliberate attention rather than passive expectation. Consumer education, transparency, responsiveness, and the design of user experience all contribute to whether individuals choose to engage with formal financial systems and whether they remain engaged over time. Financial inclusion is therefore a function not only of access, but of active usage and the confidence that sustains it. Systems that neglect the behavioural and perceptual dimensions of trust will continue to struggle to convert access into durable participation – regardless of how technically capable or formally compliant they become.

8. Trust architecture requires a feedback mechanism to function

The Trust Resilience Score of 5.4 produced at the Executive Table was generated by a single closed-door session of thirty senior practitioners. It is a significant data point, precisely because it represents the candid collective assessment of the people closest to the system's performance. But it is not a monitoring system. There is currently no standing, recurring, publicly available instrument that tracks systemic confidence in Nigeria's digital financial ecosystem over time, across consumer segments, geographies, institution types, and financial literacy levels. Governance interventions are therefore made without a reliable feedback mechanism, and course correction currently depends on crisis rather than data.

Trust infrastructure such as shared infrastructure, accountability frameworks, and coordination mechanisms – the substance of the implications above – cannot be assessed for effectiveness without a recurring measure of whether systemic confidence is improving, stagnating, or deteriorating. This places trust measurement benchmarks within the core functions of financial system governance rather than a one-time diagnostic exercise.

This gap has now been recognised at the level of national strategy: the Payments System Vision 2028 commits the CBN to launching a National Payments Trust Index. The value of any such index will depend on whether it measures trust as a system-level, demand-side property or merely aggregates the institutional performance data already collected. The measurement problem this implication identifies is precisely the problem a national index will have to solve.

These eight implications do not list separate problems. They describe one structural problem seen from eight angles: the absence of an architectural approach to confidence in Nigeria's digital financial system. Individually, each implication identifies a specific gap in how the system is currently designed and governed. Together, they define what a system-level approach to trust would require – what the recommendations in Section VI are designed to address.

FROM INSTITUTIONAL SOUNDNESS TO SYSTEMIC CONFIDENCE

The shift these implications demand is not simply a matter of improving individual institutions. It is a shift from institution-centric governance to system-level design: from asking whether each actor is performing well to asking whether the architecture connecting them can sustain the confidence that makes financial participation durable.

BRIDGFORTE

SECTION VI | Recommendations

Building the Confidence Architecture

The following recommendations are addressed to regulators, financial institutions, and development partners. Aligned to the five pillars of the Bridgforte Trust Architecture Framework, they translate the structural implications identified in Section V into targeted institutional actions. They are designed to be actionable, institutionally grounded, and sequenced to prioritise foundational infrastructure and accountability mechanisms before more complex governance and coordination interventions. They reflect not only the analytical framework developed in this report, but also the priorities expressed directly by participants in the post-event survey. Their purpose is not only to reduce system failure, but to build the confidence architecture required for durable financial participation.

For Regulators and Government Agencies

R1 – Mandate Interoperable Identity Infrastructure

The CBN and NIMC should jointly establish a binding interoperability standard for identity verification across financial institutions, beginning with systemically significant institutions and supported by shared infrastructure investment and multi-stakeholder governance.

Progress on BVN-NIN linkage is meaningful, but interoperability remains incomplete. Integration costs and system reliability continue to constrain scaling, while fragmented verification processes weaken fraud prevention, accountability, and consumer recourse.

This would require treating identity infrastructure as a shared public good rather than as a fragmented institutional compliance requirement, with corresponding implications for funding, governance, and privacy design.

R2 – Establish Mandatory Fraud Intelligence Sharing

The CBN should require systemically significant financial institutions to participate in a mandatory fraud intelligence-sharing platform, governed by an independent body with regulatory oversight and supported by privacy-preserving protocols that address competitive sensitivity while creating binding collective defence obligations.

The evidence for coordination is already on the record: under **NeFF**, fraud losses fell 51% to **₦25.85 billion** in 2025, and a Person of Interest Portal now tracks more than 13,400 individuals linked to fraudulent activity. But NeFF remains advisory and voluntary, fraud reporting fell 34% in the last quarter of 2025, and fraudsters continue to move across institutions while reporting remains inconsistent.

This challenge cannot be resolved through voluntary cooperation alone. Effective solutions must align private incentives with collective benefit, making participation in shared defence mechanisms rational for individual institutions as well as mandatory where the system requires it.

R3 – Issue AI Governance Standards for Financial Services

Financial sector regulators should publish binding AI governance standards for financial services, requiring board-level oversight of model deployment, regular bias auditing and performance monitoring, explainability standards for automated decisions in credit, fraud, and customer management, and consumer contestability mechanisms for algorithmic outcomes.

The **CBN sandbox**, the **National AI Strategy** launched in April 2025, and the AI-powered AML guidelines issued in March 2026 provide meaningful foundations, but they address AML compliance specifically rather than the full range of AI applications in financial services. Practitioners located the greater danger not in the technology itself, but in the governance failures surrounding its deployment.

These standards should be developed in consultation with industry and international regulatory peers so they shape practice early, before fragmented deployment creates larger confidence shocks.

R4 – Transition to Outcome-Based Supervisory Frameworks

Financial sector regulators should commit to a phased transition toward outcome-based supervision, beginning with a defined set of digital financial services and accompanied by standing industry-regulator dialogue mechanisms with clear mandates and regular senior-level participation.

Current engagement models remain heavily process-driven and are not always well matched to the system-level risks emerging in platform-led finance. Participants pointed out the need for more substantive dialogue on multi-party accountability, emerging technologies, and systemic interdependence.

This transition should be accompanied by structured engagement mechanisms that support earlier problem-solving, clearer feedback, and more effective coordination across the system.

For Financial Institutions

R5 – Prioritise Dispute Resolution Investment

Financial institutions should treat dispute resolution as strategic infrastructure rather than as a cost centre, extending resolution coverage across all active channels, establishing clear timelines and accountability frameworks, developing consumer-facing tracking tools, and measuring resolution quality as a board-level performance indicator.

The CBN's **Industry Dispute Resolution System (IDRS)** for card channels and its draft 48-hour refund rule are important steps. But consumer complaints surged 143% in the first half of 2025, and the IDRS covers card-based channels only; mobile, USSD, and platform-based transactions still lack equivalent coverage. Resolution speed, not failure prevention alone, emerged as a primary determinant of consumer confidence.

Investment in recourse should therefore be treated not as an operational burden, but as a structural determinant of whether users remain in the system.

R6 – Adopt AI Governance Frameworks Ahead of Regulatory Mandates

Financial institutions should establish board-level AI governance frameworks before regulation compels them to do so, including independent audits of model performance, governance arrangements for bias monitoring and explainability, and clear senior accountability for AI oversight.

Institutions should not wait for regulatory requirements to establish governance discipline. The gap between AI deployment and AI governance already represents a material risk.

Institutions that move early will be better positioned not only to manage risk, but to shape the standards that follow.

R7 – Build Cross-Sector Collaboration Infrastructure

Industry associations and financial institutions should build the neutral intermediary capacity required for collaboration on trust across the ecosystem. This should include a standing governance body that brings together banks, fintechs, mobile money operators, and regulators around shared threats and systemic standards.

This goes beyond fraud intelligence sharing alone. It requires building a cross-cutting coordination mechanism that neither NeFF nor open banking currently provides. Participants identified institutional mistrust as the single greatest barrier to collective action, which means the problem is not only technical design but relationship architecture, extending beyond the reach of regulation to require active industry leadership.

For Development Partners and Research Institutions

R8 – Commission a Longitudinal Trust Barometer

Development partners should support the design and sustained funding of a longitudinal consumer trust survey covering Nigeria's financial system, with comparable methodology across frontier market economies.

The **Edelman Trust Barometer** covers Nigeria only at an economy-wide level, and **IPA**'s consumer protection surveys, while valuable, are not a recurring sector-specific measure. The case for such an instrument is now reinforced by policy: the Central Bank's Payments System Vision 2028 commits to launching a National Payments Trust Index, with a target score of 80 by 2028 and a methodology to be developed in its early phases. That commitment establishes, at the level of national strategy, that trust in the payments system is a variable to be measured rather than assumed. The instrument itself, however, does not yet exist, and its value will depend on how it is built.

A demand-side barometer, designed from the outset to be comparable over time and across markets and to capture confidence as consumers actually experience it, is the instrument this domain requires. Its credibility will rest on design choices made early: measuring what users experience rather than what providers report, independent computation, comparability across markets and over time, and resistance to becoming a target that is managed rather than a condition that is earned.

R9 – Support the Development of Shared AI Training Datasets

International development institutions should fund the development of shared, audited AI training datasets relevant to African financial systems.

No shared federated infrastructure currently exists for AI model training in fraud detection or credit scoring in Nigeria. Institutions develop proprietary models on proprietary datasets, producing inconsistent model quality, duplicating costs across the sector, and weakening collective accountability.

Shared datasets would improve model accuracy, reduce individual institutional cost burdens, and create a mechanism for embedding fairness standards into the training data shaping AI deployment across the ecosystem.

R10 – Facilitate Global Cross-Learning on Trust Governance

Development partners should support mechanisms for cross-country learning that enable frontier market policymakers and practitioners to share evidence and adapt governance innovations across contexts.

Nigeria's removal from the **FATF grey list** in October 2025 and the CBN Fintech Report's proposals for bilateral regulatory passporting with Ghana, Kenya, and Senegal both signal a strengthening of the country's standing within global financial governance frameworks. The structural challenges identified at the Bridgforte Executive Table – around identity, accountability, AI governance, and regulatory design – are not unique to Nigeria.

The opportunity is to translate that standing into intellectual and policy leadership, positioning Nigeria not only as an adopter of global standards, but as an exporter of governance frameworks.

Participant Priorities for Collective Action

The recommendations above align closely with the priorities expressed directly by Executive Table participants in the post-event survey. The highest-ranked areas for collective industry action were **industry-wide fraud intelligence sharing (70%)**, **ethical AI and data governance frameworks (65%)**, **shared consumer protection standards (55%)**, and **structured regulatory dialogue (50%)**. Figure 3 shows how Recommendations **R1–R10** map against those priorities.

Figure 3 – Recommendations R1–R10 and Participant Priorities: Crosswalk

Recommendation	Industry-wide Fraud Intelligence (70%)	Ethical AI & Data Governance (65%)	Shared Consumer Protection (55%)	Structured Regulatory Dialogue (50%)
R1 Mandate Identity Infrastructure			●	
R2 Mandatory Fraud Intelligence Sharing	●			
R3 AI Governance Standards		●		
R4 Outcome-Based Supervision				●
R5 Dispute Resolution Investment			●	
R6 AI Gov. for Institutions		●		
R7 Cross-Sector Collaboration	●			●
R8 Longitudinal Trust Barometer			●	
R9 Shared AI Datasets		●		
R10 Global Cross-Learning				●

● Primary alignment ● Secondary / dual alignment

Source: Bridgforte analysis; participant priorities from post-event survey, February 2026.

Collectively, these recommendations point to a shift in emphasis: from improving individual actors in isolation to strengthening the system they operate within. Their effectiveness will depend on coordination across the financial ecosystem as a whole. **Trust in financial ecosystems is built or lost in the architecture that connects their actors, and that architecture is a choice.**

BRIDGFORTE

SECTION VII | Global Relevance

What Nigeria Reveals for Emerging and Frontier Markets

Nigeria is not the only market confronting the trust implications of digital financial transformation, but it is one of the clearest and most instructive cases through which to examine them. The country has moved further and faster than many peers in building real-time payment infrastructure, expanding digital financial access, and creating the conditions for platform-led finance to scale. Precisely for that reason, the pressures now becoming visible in Nigeria are not best understood as local anomalies. **They are early signals of a broader governance challenge that other frontier and emerging market financial systems are also likely to face.**

Across many such markets, the first generation of digital financial development focused on access: bringing more people into formal finance, widening provider diversity, extending payment rails, and building identity systems that could support scale. That agenda remains unfinished in many places. But a second challenge is now emerging alongside it. As transactions become faster, financial services become more interconnected, and automated systems begin to shape customer outcomes more directly, the policy problem changes. **The question is no longer only whether digital systems can expand inclusion. It is whether they can sustain confidence under conditions of speed, scale, and interdependence.**

The pattern is already visible in the two markets that have built instant payment systems at the greatest scale, and both are now confronting the structural questions this report identifies in Nigeria.

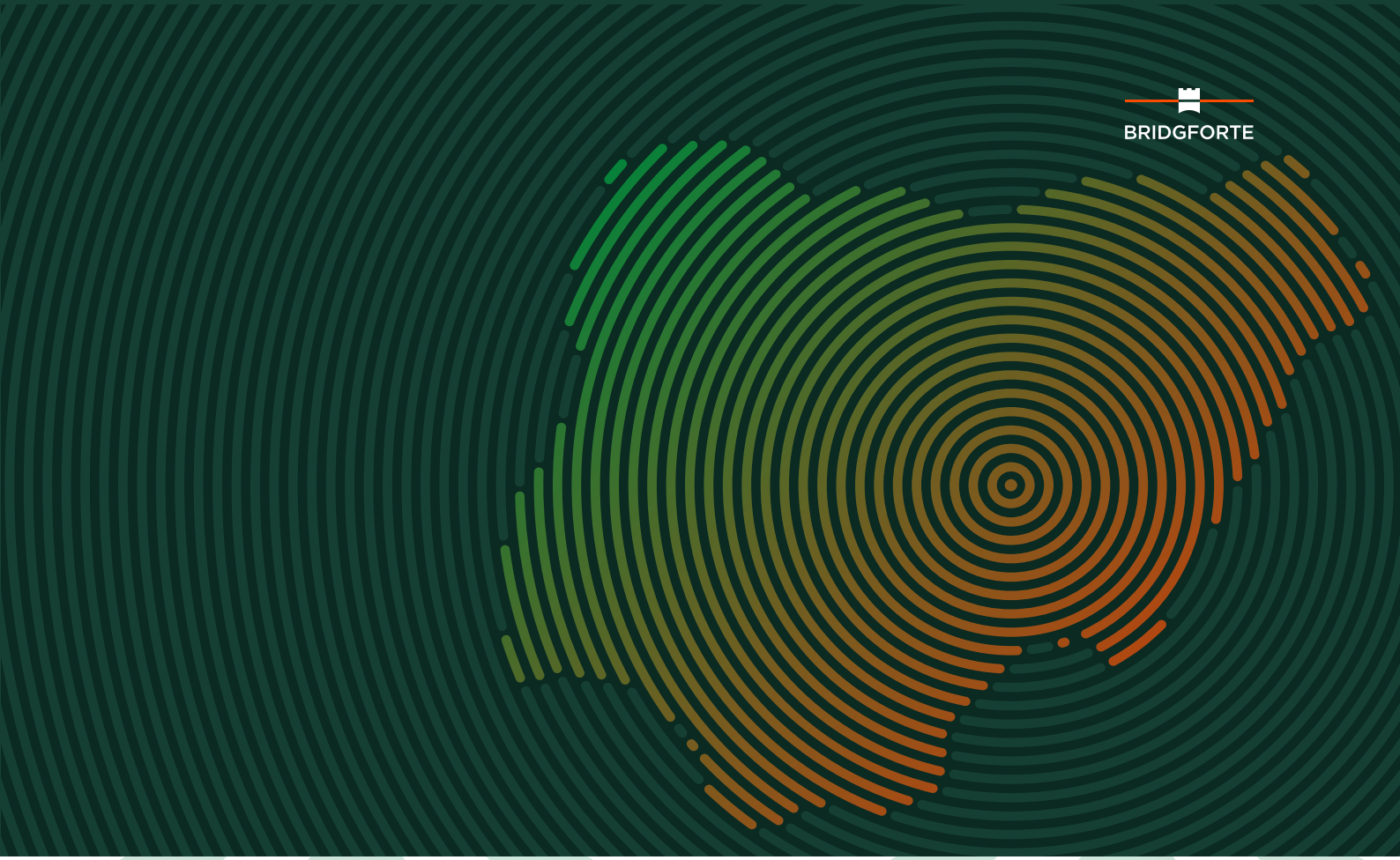
India. The Unified Payments Interface is the largest real-time payment system in the world, processing 228.3 billion transactions in 2025 across more than 500 million users, and by common consent one of the most successful financial inclusion instruments ever built. Yet reported digital payment fraud rose roughly forty-fold in value over five years. The dominant pattern is authorised push payment fraud, in which the customer is manipulated into making the transfer and the money moves beyond recall before anyone can react. In April 2026 the Reserve Bank of India published a discussion paper proposing what would have been unthinkable a decade ago: a one-hour delay on account-to-account transfers above ₹10,000, a customer-controlled kill switch, and additional authentication for vulnerable users, on data showing that transfers above that threshold account for 98.5 per cent of fraud value. India, in other words, is now deliberately reintroducing friction into the system whose defining achievement was its removal. This is the instant payments design tension identified in Section IV, playing out at the largest scale in the world.

Brazil. Pix, launched in 2020, became the country's dominant payment method within four years. It also became its dominant fraud channel, with losses reaching R$6.5 billion in 2025. The more instructive figure is the recovery rate: of funds disputed through Pix's refund mechanism, only 7 per cent were recovered. The reason is structural rather than technical. The original mechanism could block funds only in the first receiving account, and fraudsters move money through several accounts within minutes. Accountability diffused across the chain faster than any single institution could act. Brazil's response, MED 2.0, made mandatory in February 2026, traces and blocks funds across successive accounts with recovery completed within eleven days. It is coordination machinery built after the fact, for a failure mode the original architecture did not anticipate, and it is precisely the accountability diffusion this report identifies along the Consumer to Institution axis.

Neither is a story of institutional failure. Both countries built world-leading infrastructure, supervised by capable central banks and operated by sound institutions. What both are discovering is that individually sound institutions and technically excellent infrastructure do not, by themselves, produce systemic confidence. The gaps opened between institutions, in the arrangements that connect them, and both regulators are now building governance architecture retrospectively to close them.

Nigeria's position within this pattern is instructive. It moved early, and it is meeting these questions early. The advantage available to it, and to markets following the same path, is the opportunity to design the confidence architecture deliberately rather than assemble it after the losses have accumulated.

The specific manifestations differ by context. Fraud patterns, regulatory architectures, identity system designs, and the competitive dynamics between banks and fintechs vary considerably across jurisdictions. **What does not vary is the underlying dynamic:** in platform-led financial systems, trust is no longer primarily a function of individual institutional performance. It is a function of the shared infrastructure, accountability frameworks, and coordination arrangements that connect institutions – and of whether those arrangements were designed with confidence in mind or simply inherited from an earlier, less interconnected era. That is a governance challenge that cuts across national boundaries, and one for which few financial systems – in emerging markets or advanced economies – have yet developed adequate responses. **The Bridgforte Trust Architecture Framework is designed to be applicable across that broader landscape.**



SECTION VIII | Conclusion

Building the Architecture of Confidence

Nigeria's digital financial system has entered a more demanding phase of development. The first phase was defined by expansion: more accounts, faster payments, wider provider diversity, and the infrastructure needed to bring digital finance to scale. That phase produced significant gains. But it also changed where trust sits. In platform-led systems, confidence no longer rests primarily on the standing of individual institutions. **It depends increasingly on the shared infrastructure, accountability frameworks, governance arrangements, and coordination mechanisms that connect them.**

This is the central finding of the report. The most important trust failures now visible in Nigeria's digital financial ecosystem are not isolated malfunctions or simply signs of weak institutional performance. **They are structural failures arising where systems are shared, responsibilities are diffuse, recourse is uneven, and governance has not kept pace with technical capability.** The challenge is no longer only how to build digital financial systems that scale. It **is how to build the confidence architecture required for those systems to remain credible under conditions of speed, interdependence, and stress.**

That shift has direct implications for how financial inclusion must now be understood. Access remains necessary, but it is no longer sufficient. A system can widen participation while still failing to sustain confidence; it can increase transaction volumes while leaving users uncertain about recourse, responsibility, and protection when things go wrong. **The next phase of financial inclusion therefore depends not only on the availability of services, but on whether the systems through which those services are delivered can sustain trust strongly enough to become people's default rather than their fallback.**

What gives this argument particular force is its provenance. The findings in this report did not emerge from desk research alone. They came from a room of thirty senior leaders from competing institutions (banks, fintechs, insurance, and infrastructure providers) who examined their own system with unusual candour. **That candour is also a foundation.**

What must now be built is not only more advanced financial infrastructure, but the governance architecture that makes such infrastructure trustworthy. That task is systemic, not technical. It requires accountability frameworks that operate across institutional boundaries, shared mechanisms that make collective defence possible, coordination structures that align private incentives with public confidence, and feedback tools that show whether trust is strengthening or weakening over time.

Trust in digital finance does not arise automatically from innovation, scale, or institutional soundness alone. It must be designed into the system itself. In Nigeria, that challenge is already visible. Elsewhere, it is likely to follow.

References and Sources

Bridgforte Primary Sources

1. **Bridgforte.** *Executive Table: Trust Architecture in Platform-Led Finance.* Lagos, Nigeria, February 2026. Closed-door convening conducted under Chatham House Rule in partnership with the UNDP Innovation Centre, Lagos. Primary source for participant polling, facilitated discussion insights, and post-event survey findings cited throughout this report.
2. **Bridgforte; Aspen Institute Financial Security Program; ConsumerCentriX.** *Bridgforte Dialogues Roundtable: Financial Inclusion Towards 2035 – Shifting Power, Shaping Systems.* Harvard Club of New York City, New York, 24 September 2025. Foundational context for the Trust Architecture research agenda.

Conceptual and Theoretical Sources

3. **Giddens, Anthony.** *The Consequences of Modernity.* Cambridge: Polity Press, 1990.
4. **Luhmann, Niklas.** *Trust and Power.* Chichester: John Wiley & Sons, 1979.
5. **Luhmann, Niklas.** *Social Systems.* Stanford: Stanford University Press, 1984.
6. **North, Douglass C.** *Institutions, Institutional Change and Economic Performance.* Cambridge: Cambridge University Press, 1990.

Nigeria: Policy, Regulatory, and Market Sources

7. **Alliance for Financial Inclusion (AFI).** *Maya Declaration.* Mexico: AFI Global Policy Forum, 2011.
8. **Central Bank of Nigeria (CBN).** *National Financial Inclusion Strategy.* Abuja: CBN, 2012.
9. **Central Bank of Nigeria (CBN).** *Payments System Vision 2025.* Abuja: CBN.
10. **Central Bank of Nigeria (CBN).** *Payments System Vision 2028. Abuja: CBN, June 2026.*
11. **Central Bank of Nigeria (CBN).** *Shaping the Future of Fintech in Nigeria: Innovation, Inclusion and Integrity.* CBN Fintech Report, Policy Insight Series 2025. Abuja: CBN, February 2026.
12. **Central Bank of Nigeria (CBN) and Nigeria Inter-Bank Settlement System (NIBSS).** *AfriGO Domestic Card Scheme.* Abuja: CBN/NIBSS, January 2023.
13. **Central Bank of Nigeria (CBN).** *National Artificial Intelligence Strategy.* Abuja: CBN, April 2025.
14. **Central Bank of Nigeria (CBN).** *AI-Powered AML Compliance Guidelines.* Abuja: CBN, March 2026.
15. **Central Bank of Nigeria (CBN).** *Consumer Protection Framework: Industry Dispute Resolution System (IDRS).* Abuja: CBN.
16. **Central Bank of Nigeria (CBN).** *Consumer Protection Annual Report 2025.* Abuja: CBN, 2025.
17. **Central Bank of Nigeria (CBN).** *Switching and Processing Licence Granted to Flutterwave Technology Solutions Limited.* Abuja: CBN, September 2022.
18. **Central Bank of Nigeria (CBN).** *Regulatory Framework for Open Banking in Nigeria.* Abuja: CBN, 2021.
19. **Nigeria Inter-Bank Settlement System Plc (NIBSS).** *Corporate Profile.* Lagos: NIBSS.
20. **Nigeria Inter-Bank Settlement System (NIBSS).** *Industry Fraud Report 2024.* Lagos: NIBSS, 2025.
21. **Nigeria Inter-Bank Settlement System (NIBSS).** *Industry Fraud Report 2025.* Lagos: NIBSS, 2026.
22. **Nigeria Electronic Fraud Forum (NeFF).** Established 2011. Lagos: CBN/NeFF.
23. **EFInA (Enhancing Financial Innovation & Access).** *Access to Financial Services in Nigeria Survey (A2F) 2023.* Lagos: EFInA, 2023.

Continental and International Sources

24. **AfricaNenda.** *State of Inclusive Instant Payment Systems in Africa (SIIPS) 2025.* Geneva: AfricaNenda, 2025.
25. **Afreximbank; African Union; AfCFTA Secretariat.** *Pan-African Payment and Settlement System (PAPSS).* Cairo: Afreximbank, launched January 2022.
26. **Alliance for Financial Inclusion (AFI).** *Digital Financial Services Policy and Regulatory Framework.* Kuala Lumpur: AFI.
27. **Edelman.** *Edelman Trust Barometer.* Chicago: Edelman. Published annually.
28. **Financial Action Task Force (FATF).** *Nigeria Removed from the FATF Grey List.* Paris: FATF, October 2025.
29. **Innovations for Poverty Action (IPA).** *Consumer Protection Research, Nigeria.* New Haven: IPA.
30. **Reserve Bank of India (RBI).** *Discussion Paper on Additional Frictions in Digital Payments.* Mumbai: RBI, April 2026.
31. **Reserve Bank of India (RBI).** *Annual Report 2025–26.* Mumbai: RBI, 2026.
32. **National Payments Corporation of India (NPCI).** *UPI Product Statistics 2025.* Mumbai: NPCI, 2025.
33. **Banco Central do Brasil (BCB).** *Resolution BCB No. 493.* Brasília: BCB, August 2025.
34. **Banco Central do Brasil (BCB).** *Resolution BCB No. 546.* Brasília: BCB, January 2026.
35. **Banco Central do Brasil (BCB).** *Mecanismo Especial de Devolução (MED) Recovery Data 2025.* Brasília: BCB, 2025.

Endnotes

[1] Nigeria Inter-Bank Settlement System Plc (NIBSS). Corporate Profile; and related NIBSS operational materials on the BVN system, NIP platform, and GSI architecture.

[2] Central Bank of Nigeria. Payments System Vision 2025. CBN, Abuja.

[3] Central Bank of Nigeria and NIBSS. AfriGO Domestic Card Scheme, launched January 2023.

[4] Afreximbank; African Union; AfCFTA Secretariat. Pan-African Payment and Settlement System (PAPSS), launched January 2022.

BRIDGFORTE

APPENDIX A

Methodology and Convening Design

This appendix sets out the convening design, data sources, and analytical approach underpinning the findings presented in this report. The methodology combines primary evidence from senior industry participants with a system-level analytical framework to generate policy-relevant insights.

Convening Design

The Bridgforte Executive Table is a structured dialogue format designed to elicit candour from senior decision-makers on issues of systemic significance. Deliberately small – thirty participants in this session – the format prioritises depth of engagement over breadth of representation.

The February 2026 convening, held held in partnership with the UNDP Innovation Centre in Lagos, brought together senior decision-makers from across Nigeria's full financial institutional ecosystem for an open conversation under the Chatham House Rule. Participants included chief executives, board directors, and senior institutional leaders from commercial banking, fintech and payments, financial market infrastructure, insurance, pensions, capital markets, and international development finance.

Dialogue was organised around key dimensions of trust in digital financial systems, with particular attention to operational performance, identity infrastructure, fraud and cybersecurity, artificial intelligence, and regulatory engagement. The session was structured around three thematic modules, each preceded by live polling to surface baseline assumptions before open discussion focused on shared risks, structural gaps, and opportunities for coordinated action.

Data Sources

Structured participant polling – capturing real-time prioritisation of trust breakdown points, collaboration barriers, and emerging risks across the session. Six structured polls were conducted during the convening. Polling figures reflect responses from the participants present at each module and are indicative of the room's assessment rather than statistically representative.

Facilitated discussion insights – reflecting practitioner experience and judgment across institutions and sectors, gathered through structured dialogue under Chatham House.

Post-event survey data – providing additional validation of priority areas for collective action, gathered through a follow-up survey completed after the convening.

Together, these sources provide a practitioner-grounded view of system performance. They are complemented by a structured review of Nigeria's digital financial ecosystem drawing on published data from NIBSS, the CBN, AfricaNenda, and relevant academic and policy literature, as well as targeted comparative analysis of digital financial systems in other jurisdictions.

Analytical Approach

The findings presented in this report are the result of constructive synthesis rather than mere transcription of participant views. Insights were analysed thematically and interpreted through the Bridgforte Trust Architecture Framework, introduced in Section III, which provides a system-level lens for understanding how trust is produced and eroded in platform-led financial systems.

The analytical process involved three stages: identifying recurring patterns across participant contributions; triangulating discussion insights with polling data and survey responses; and mapping observed challenges to the structural dimensions of trust set out in the framework. This approach allows practitioner observations to be translated into broader policy insight while preserving the integrity of the underlying evidence.

This report was prepared with the assistance of AI tools to support drafting, editing, and literature synthesis. The analytical framework, interpretation, and all findings and recommendations are the author's own. Bridgforte reviewed and verified the underlying data, sources, and conclusions, and retains full responsibility.

Scope and Limitations

This report draws significantly on the perspectives of senior practitioners operating within Nigeria's financial system, complemented by structured polling, post-event survey data, and targeted research. It is not intended to provide a statistically representative assessment of all stakeholders. The analysis is qualitative and interpretive, designed to surface structural insights rather than quantify outcomes.

The consistency of themes across participants, together with supporting evidence from multiple sources, supports confidence in the relevance of the findings and in the importance of the issues identified.

PARTICIPANT FEEDBACK

Participants gave the session a **9.6 out of 10** overall recommendation score, with **75%** awarding a perfect score. **80%** rated the overall quality of the convening as excellent. **65%** expressed interest in joining the Trust Lab, and **95%** indicated interest in partnering on future sessions. Several participants also noted that the time allocated was insufficient for the weight of the subject matter discussed, itself a signal of the depth of engagement the format generated.

NOTES

BRIDGFORTE

About Bridgforte

The **Bridgforte Centre for Global Impact** is a policy research and convening institution focused on the structural foundations of financial governance, inclusion, and institutional design in Africa. It works at the intersection of practitioner insight, policy analysis, and cross-sector dialogue – convening senior decision-makers, developing analytical frameworks, and advancing the governance conversations needed to translate evidence into institutional reform. Bridgforte's convenings include the Bridgforte Dialogues, which held its inaugural session on the sidelines of the United Nations General Assembly in New York in September 2025.

Bridgforte was founded by **Aishah N. Ahmad, CFA, OFR**, whose experience spans several decades in banking, financial regulation, and public policy. She served as Deputy Governor of the Central Bank of Nigeria from 2018 to 2023, with responsibility for financial system stability and payments policy, and currently chairs the Expert Leaders Group at the Graça Machel Trust, a principals-level body of senior women leaders in African economic governance. Bridgforte's work is informed by this combination of practitioner, policy, and regulatory experience.

About the Executive Table

The **Bridgforte Executive Table** is a closed-door dialogue format designed to enable candid, substantive exchange among senior financial system decision-makers. Sessions are conducted under Chatham House Rule and combine facilitated discussion, structured polling, and post-event survey evidence. The Executive Table series serves as a core evidence base for Bridgforte's **Policy Framework Reports**, complementing the institution's wider research programme by surfacing practitioner insight that informs policy development and supports cross-sector coordination.

The Trust Lab

Bridgforte's **Trust Lab** is a research initiative in development, dedicated to trust as a foundational condition of financial system design. Its work will develop governance frameworks, generate primary research, and support the practitioner dialogue required to translate analytical insight into institutional action – spanning identity infrastructure, AI governance, system-level coordination, and trust measurement. This report is its founding publication.

bridgforte.org | **dialogues@bridgforte.org**

EXECUTIVE TABLE SERIES | No. 1

Trust Architecture in Platform-Led Finance

Structural Governance Imperatives for Nigeria's Digital Financial Ecosystem

Policy Framework Report

July 2026

BRIDGFORTE

In partnership with the UNDP Innovation Centre, Lagos, Nigeria