

BONITA FMI

Redress Is Infrastructure

**Designing Trust Into Africa's Payment Systems Before Investment
Is Committed**

By Andrew Manuel

Published by Bonita FMI

Version 1.1 September 2026

Intended readership

Central banks and regulators

Ministries of finance

Multilateral development banks and development partners

Banks and microfinance institutions

Mobile money providers

Fintechs and payment service providers

Strengthening Financial Market Infrastructure

info@bonitafmi.com bonitafmi.com [linkedin.com/company/bonita fmi](https://linkedin.com/company/bonita-fmi)

About the author

Andrew Manuel is a payment systems and financial market infrastructure specialist with over 18 years of experience across payment switching, transaction routing, cards, digital channels and national payment infrastructure in African markets. His work includes participant readiness, systems integration, testing, certification, operational implementation and coordination across banks, fintechs and mobile money operators. He founded Bonita FMI to support financial authorities, development partners and market participants with upstream diagnostics, programme readiness, delivery assurance and operational resilience.

Contents

Executive Summary..... 3

Methodology and scope..... 3

1. Introduction..... 4

2. Adoption Is Not Trust..... 4

3. Redress as Infrastructure..... 5

4. Redress Precedents in Card Networks..... 6

5. Irrevocability and Instant Payments..... 7

6. The Anatomy of Redress Failure..... 7

7. The Economics of Late Redress..... 8

8. A Redress Readiness Diagnostic..... 9

9. A Lifecycle Framework for Embedding Redress..... 9

10. Measuring Trust..... 10

11. Governance and Cross Provider Coordination..... 12

12. Implications and Recommendations..... 12

13. Applying the Framework in Practice..... 13

14. Limitations and areas for validation..... 14

15. Conclusion..... 14

References..... 15

Appendix A..... 16

Appendix B..... 17

Appendix C..... 18

Publication information

Suggested citation Manuel, A. 2026. Redress Is Infrastructure. Harare, Bonita FMI.

Copyright 2026 Andrew Manuel. This paper presents policy and design analysis. It does not constitute legal advice, regulatory guidance or an assessment of any named payment system.

Abstract. Africa has built payment rails at extraordinary speed, bringing hundreds of millions of people into formal finance through mobile money, instant payment systems and a fast growing fintech sector (Demirguc Kunt et al., 2022, World Bank, 2025, GSMA, 2026). Yet adoption is not the same as trust. This paper argues that consumer redress, the ability to trace a disputed transaction, reverse it within an enforceable timeline, escalate it independently and evidence a fair outcome, is an infrastructural property of a payment system rather than a customer service function added after launch. Treated as a late compliance layer, redress is slow, costly and frequently absent, and the users it fails are disproportionately the first time, low income and women users that inclusion is meant to reach (AfricaNenda Foundation, World Bank and UNECA, 2025, CGAP, 2022). Drawing on the State of Inclusive Instant Payment Systems in Africa report, World Bank consumer protection benchmarking and the CPSS IOSCO Principles for Financial Market Infrastructures, the paper sets out why redress must be designed into scheme rules, blueprints, test scripts and go live criteria. It presents a diagnostic set of upstream questions, a lifecycle framework and a maturity model for embedding redress, and it proposes a trust centred approach to measuring financial inclusion. The argument is directed at central banks, payment system operators and their development partners, and reflects the upstream, diagnose before you invest practice of Bonita FMI.

Keywords, financial market infrastructure, instant payments, consumer protection, redress, dispute resolution, financial inclusion, scheme governance, payments assurance, Africa.

Executive Summary

Africa's payment revolution has proven that people will adopt digital rails at scale. The next phase depends on whether they trust them. This paper makes the case that consumer redress, the ability to trace, reverse, escalate and resolve a disputed transaction and to evidence a fair outcome, is not a customer service add on but an infrastructural property of a payment system, set by its rules, data model and governance. When redress is left as a late compliance layer it becomes slow, costly and often absent, and the users it fails first are the low income, first time and women users that inclusion is meant to reach. The key messages of this paper are as follows.

- Adoption is not trust. Accounts opened measure capacity, not confidence, and an unresolved payment failure can cause a first time user to return to cash and discourage people in the same household or community.
- Redress is infrastructure. Traceability, reversibility, enforceable timelines and independent escalation are design decisions taken in the scheme rules, message standards and go live criteria, not behaviours added afterwards.
- The card networks already prove the point. Chargeback and arbitration frameworks show that redress can be engineered into a scheme's rules, while irrevocable instant payments create a new challenge that the United Kingdom implemented a mandatory reimbursement framework in October 2024 after the Faster Payments system was already operating at scale.
- Design it upstream. The questions that determine whether redress works are cheapest to answer before investment is committed. Answered after go live, each becomes an expensive remediation programme.
- Measure trust, not just reach. Financial inclusion should be judged by whether users believe their money is safe and that recourse exists, using a redress maturity model and a trust centred scorecard.

The paper offers a redress readiness diagnostic, a lifecycle framework for practical implementation, a maturity model, and recommendations for central banks, ministries of finance, development partners, commercial and microfinance banks, mobile money operators and fintechs. Its central recommendation is simple, diagnose before you invest, and build trust into the blueprint rather than into the aftermath.

Methodology and scope

This paper is a policy and design analysis rather than an impact evaluation. It combines a structured review of international standards, payment scheme rules, financial inclusion evidence, consumer protection benchmarking and recent African instant payment system research. It also draws on professional implementation experience in payment switching, participant onboarding, testing, certification and operational readiness. The analysis distinguishes published evidence from the author's interpretation. The diagnostic, lifecycle and maturity model are original frameworks developed by Andrew Manuel intended for adaptation and validation in individual markets. They should not be read as regulatory requirements unless adopted by a competent authority.

The review prioritises sources available by 10 September 2026. Older sources remain where they are foundational or support a specific historical finding. Current editions are used for changing industry data and scheme rules. Numerical claims should be checked again before each new edition because mobile money statistics, network rules and regulatory requirements change frequently.

1. Introduction

Across the African continent, the last decade has produced one of the fastest expansions of payment infrastructure anywhere in the world. Mobile money moved from a Kenyan innovation to a continental utility, and rigorous evidence shows it delivered real welfare gains, lifting an estimated two percent of Kenyan households out of poverty and shifting economic outcomes particularly for women (Suri and Jack, 2016). Account ownership in developing economies rose from 63 to 71 percent between 2017 and 2021, with mobile money an important driver in Sub Saharan Africa (Demirguc Kunt et al., 2022, p. 1). Global Findex 2025 provides the current benchmark and adds evidence on digital connectivity, which should be read alongside account ownership and payment usage (World Bank, 2025). Domestic instant payment systems have proliferated, a new generation of fintechs has layered wallets and acceptance on top of them, and the mobile money industry now processes transaction values measured in the trillions of dollars annually (GSMA, 2026). Measured by accounts opened and systems switched on, financial inclusion has advanced further in ten years than in the preceding fifty. The State of Inclusive Instant Payment Systems in Africa report captures the continuing expansion of instant payment systems across the continent. The 2025 edition combines continental system analysis with consumer research and case studies of IPN in Egypt, EthSwitch in Ethiopia, SIMO in Mozambique and NIBSS in Nigeria. It also shows that inclusion depends on more than system availability. Governance, customer experience, recourse and sustained usage remain material design concerns (AfricaNenda Foundation, World Bank and UNECA, 2025). This paper therefore treats the 2025 report as evidence of both progress and unfinished institutional work. It does not assume that findings reported in earlier editions remain unchanged. This paper takes that qualification as its starting point and develops it into a design argument. The central proposition is that consumer redress is infrastructure. It is not a service quality that can be added to a payment system after the fact through better call centres or clearer terms and conditions. It is a set of capabilities determined by the architecture, rules and governance of the system itself, and if it is not designed in from the beginning it is expensive, slow and often impossible to retrofit convincingly. The paper proceeds as follows. Section 2 distinguishes adoption from trust. Section 3 defines redress as infrastructure and identifies its four constituent capabilities. Section 4 shows that the international card networks already treat redress as designed in infrastructure, and Section 5 examines the new redress challenge created by irrevocable instant payments. Section 6 analyses why redress fails when treated as an afterthought, and Section 7 sets out the economics of late redress. Section 8 presents a diagnostic set of upstream questions, Section 9 a lifecycle framework for practical implementation, and Section 10 a maturity model and trust centred measurement approach. Sections 11 and 12 address governance and offer recommendations for regulators, operators and funders. Section 13 explains practical application, Section 14 states the limitations and Section 15 concludes, and Appendix A provides a redress readiness checklist.

2. Adoption Is Not Trust

2.1 The headline numbers describe capacity, not confidence

The metrics that dominate financial inclusion reporting are adoption metrics. They count accounts, wallets, registered agents, connected institutions and transaction volumes. These are meaningful

measures of capacity, they establish that a rail exists and that people are able, in principle, to use it. They do not establish that people trust the rail. A registered wallet that a user has abandoned after a bad experience still counts as an opened account, indeed, a substantial share of registered mobile money accounts are inactive in any given month (GSMA, 2026). Capacity and confidence are different quantities, and only the first is routinely measured.

2.2 What consumers actually fear

Consumer research across multiple African markets consistently identifies two related anxieties at the top of the list of barriers to digital payment usage, the fear of fraud and scams, and the absence of a reliable way to recover funds when a transaction fails or is disputed (AfricaNenda Foundation, World Bank and UNECA, 2025). These are not abstract concerns. They reflect direct or second hand experience of failed transfers, unauthorised deductions, misdirected payments and scams for which no effective recourse was available. The AfricaNenda consumer research

found that these fears fall hardest on the very groups inclusion is intended to serve, and that women in particular report feeling unsafe using digital payment platforms (AfricaNenda Foundation, World Bank and UNECA, 2025). This matters all the more because the welfare gains of digital finance have been shown to accrue disproportionately to women (Suri and Jack, 2016), and because a gender gap in account ownership persists (Demirguc Kunt et al., 2022). Where recourse is weak, the people with the least capacity to absorb a loss carry the most risk.

2.3 The fraud environment is intensifying

The trust problem is not static. Growing transaction volumes expand the number of opportunities for error, fraud and social engineering. The GSMA reports continued growth in mobile money activity alongside persistent ecosystem risks (GSMA, 2026). CGAP reviews evidence of digital financial service risks that include fraud, inadequate disclosure, data misuse, service failures and ineffective recourse. The importance of each risk differs by market and product, so they should not be treated as a fixed universal classification (CGAP, 2022). Fraud and weak redress can reinforce each other because the events that harm users may also be difficult to trace, evidence and resolve. As exposure grows, the value of designed redress grows with it.

2.4 The asymmetry that makes trust fragile

Trust in a payment system is fragile in a specific way. A user may transact successfully many times, accumulating a diffuse and easily forgotten benefit from each success. A single unresolved failure produces a concentrated and memorable loss. Because the downside of a lost payment is immediate and the upside of each successful one is marginal, the psychology of adoption is asymmetric, one bad experience can outweigh many successful transactions and weaken continued use. This is why systems optimised solely for availability and throughput can still lose users. Reliability reduces how often failures occur, it does nothing about what happens when one does. The gap between those two things is exactly the space that redress occupies.

2.5 The cash fallback and its social cost

When redress is absent, the user has a readily available alternative, cash. Cash requires no dispute process because it fails in visible, immediate ways the user can manage directly. A first time user who loses money through a digital channel and finds no effective help may return to cash and may discourage family or community members from using the same service. The reputational damage of unresolved failures is therefore not contained to the individual user, it propagates through

exactly the social networks that drive adoption in the first place. Trust, once lost at the point of failure, is costly to rebuild and easy to lose again.

3. Redress as Infrastructure

3.1 A definition

By redress we mean the set of capabilities that allow a consumer harmed by a payment, whether through failure, error, unauthorised deduction or fraud, to obtain a fair resolution. Concretely, redress requires that a disputed transaction can be traced end to end, reversed or returned where appropriate within a defined and enforceable timeline, escalated to an independent path when a single provider cannot or will not resolve it, and evidenced as having produced a fair outcome. The claim of this paper is that each of these capabilities is a property of how the system is designed, tested and governed, and not a discretionary behaviour of a customer service function.

3.2 The four capabilities

Traceability is the ability to follow a disputed transaction across every participant that handled it. It is a function of message standards, data models, identifiers and reconciliation design. If the system did not capture and retain the information needed to reconstruct a transaction across participants, that information is simply unavailable when a dispute arises, and no amount of customer service effort can recover it. Traceability is designed in at the level of the message standard, not bolted on afterwards. Reversibility is the ability to reverse or return a transaction where the rules require it. It depends on scheme rules that define reversal and return flows, a settlement model that can accommodate them without creating unmanaged liquidity or credit risk, and participants who have implemented and tested those flows. A real time push payment that has settled cannot be unwound by goodwill, it can only be unwound if the system was built to support a defined return. Timeliness and enforceability mean that resolution occurs within a period the user can rely on, and that the period is actually enforced. A timeline is only credible if it is written into the

rulebook, instrumented so that adherence can be measured, and backed by the scheme's governance. A promise of resolution that cannot be measured cannot be enforced, and a promise that cannot be enforced is not a commitment but an aspiration. Independence is the availability of an escalation path that functions across banks, fintechs and mobile money operators, including where the consumer's own provider is the source of the problem. Internal dispute resolution within a single provider is necessary but not sufficient, because it fails precisely in the cases where the provider has an interest in denying the claim. Independence requires a cross provider path and, at the mature end, a direct channel to an independent body.

3.3 Failure, fraud, reversal and return

Operational failures and fraud require different evidence and liability decisions. A failed payment may involve a timeout, duplicate posting, partial processing or reconciliation break. An unauthorised payment involves a transaction the customer did not approve. An authorised push payment scam involves a customer who approved the instruction after deception. A misdirected payment may be validly authorised but sent to the wrong account. The rulebook should classify these events separately because the appropriate response may be correction, reversal, return, reimbursement, recovery or independent adjudication.

A reversal normally cancels or corrects a transaction that did not complete as intended. A return is a new transaction that sends funds back after the original payment reached final settlement. Settlement finality therefore does not mean that funds can never be returned. It means that the completed settlement cannot be unilaterally revoked outside the governing rules. Redress for an instant payment must preserve finality while providing defined processes for return, reimbursement and recovery.

3.4 Messaging and evidence

ISO 20022 provides a structured financial messaging framework and includes messages that can support payment investigation and exception handling. The standard does not create traceability by itself. End to end tracing also requires persistent identifiers, common implementation guidance, complete data, retention rules, reconciliation controls and participant compliance (International Organization for Standardization, n.d.). Scheme certification should test these elements together.

3.5 The relationship to established standards

Framing redress as infrastructure is consistent with how international standards already treat payment systems. The CPSS IOSCO Principles for Financial Market Infrastructures treat sound governance, clear and enforceable rules, and operational reliability as core properties of a well run system rather than optional extras (CPSS IOSCO, 2012). The extension to redress is direct. A rule that a disputed transaction will be resolved within a defined period is credible only if the system can evidence it, in the same way that a settlement guarantee is credible only if the system can honour it. Redress that cannot be traced, measured and enforced is not a lighter form of consumer protection, it is the appearance of protection

without its substance. Treating redress as an infrastructural property brings it within the same discipline that already governs settlement finality, operational risk and access.

4. Redress Precedents in Card Networks

The claim that redress is infrastructure is not merely theoretical. The international card networks have operated redress as a designed in property for decades, and their dispute frameworks are the clearest existing proof that traceability, reversibility, enforceable timelines and independent adjudication can be engineered into a payment system's rules rather than left to goodwill. Under the Visa and Mastercard schemes, a cardholder who disputes a transaction triggers a structured, rule bound process. Disputes are classified using standardised reason codes, organised by Visa into fraud, authorisation, processing error and consumer dispute categories, with Mastercard using an equivalent four category structure, so that every participant describes the same problem in the same terms (Visa, 2026, Mastercard, 2026). The transaction is traceable end to end because the clearing and message data needed to identify and match it are captured by design. The dispute then moves through defined stages, first chargeback, representment by the merchant, pre arbitration and arbitration, each with explicit deadlines. The network rules define case categories, evidence requirements and time limits for cardholders, issuers, acquirers and merchants. Because these rules change, the current edition must control each operational decision (Visa, 2026, Mastercard, 2026). Where the parties cannot agree, the scheme itself provides an independent adjudication and arbitration mechanism

and rules on the outcome. Every element this paper argues for is present in that design. Reason codes and matched clearing data provide traceability. The chargeback is a defined reversibility mechanism embedded in the settlement model. The staged deadlines are enforceable timelines written into the rulebook and instrumented by the scheme. Arbitration is an independent escalation path that binds participants. None of this is a customer service behaviour, it is a property of the scheme rules, the message standards and the governance, which is exactly the infrastructural treatment this paper recommends for instant payments and other fast rails. The lesson for Africa's newer rails is not to copy card chargebacks wholesale, since they carry costs and complexities of their own, but to recognise that the card networks solved the redress problem by treating it as infrastructure from the outset. The instant payment systems now being built can and should embed an equivalent, fit for purpose redress architecture in their own rulebooks rather than leaving it to each participant's discretion.

5. Irrevocability and the New Redress Challenge in Instant Payments

Instant payment systems introduce a redress challenge that card systems do not face in the same way. Real time retail payments are typically push payments that are irrevocable by design, the payer authorises the transfer and the funds move immediately and with finality. Irrevocability is a feature, delivering certainty to the payee and supporting the speed that makes these systems useful, but it removes the natural reversal mechanism that card pull payments rely on. When a push payment goes wrong there is no chargeback to fall back on, unless the scheme has deliberately built a return or reversal flow. This design choice interacts dangerously with authorised push payment fraud, in which a consumer is deceived into authorising a payment to a fraudster, whether by being misled about who the recipient is or about the purpose of the payment (PSR, 2024). Because the consumer authorised the transaction, it is not obviously the provider's error, and because the payment is irrevocable, the funds are gone by the

time the deception is discovered. Authorised push payment fraud has become one of the most damaging categories of fraud precisely because instant, irrevocable rails give the victim no built in route to recover the money, a risk amplified by the worsening fraud environment described in Section 2 (GSMA, 2026). Jurisdictions that adopted fast payments early are now retrofitting redress at the scheme level to address this gap, which itself illustrates the cost of not designing it in. In the United Kingdom, the Payment Systems Regulator introduced a mandatory reimbursement regime that took effect on 7 October 2024, requiring payment service providers to reimburse in scope victims of authorised push payment scams over the Faster Payments and CHAPS systems, with liability shared equally between the sending and receiving providers and enhanced protection for vulnerable consumers (PSR, 2024). Whatever the specific parameters, the structural point is what matters, the regulator addressed the problem by writing redress and a liability allocation model into the rules of the payment system itself, because individual providers acting alone could not. For African markets building instant payment systems, the implication is direct. Irrevocability and authorised push payment fraud are not edge cases to be handled later by customer service, they are design parameters. The blueprint must decide, before launch, how disputed and fraudulent push payments will be traced, whether and how they can be returned, how liability is allocated between sending and receiving participants, and what independent recourse a deceived consumer has. These are precisely the upstream questions set out in Section 8, and they are far cheaper to answer in the rulebook than to retrofit after a fraud wave has already eroded trust.

6. The Anatomy of Redress Failure

6.1 The compliance layer trap

Consumer protection is still commonly treated as a compliance layer, considered once a system is already operational and framed principally as a matter of disclosure and licensing. This framing is convenient because the parts of consumer protection that can be satisfied by a document, published terms, a stated complaints policy, a licensing condition, can be produced at launch without changing the system. The difficulty is that the parts of redress that actually protect users, traceability, reversibility, enforceable timelines and independent escalation, cannot be produced by a document. They are operational capabilities, and by the time the system is live the design decisions that determine whether they exist have already been made.

6.2 Four structural gaps

The failure of late redress is structural rather than a matter of insufficient goodwill. First, if dispute, reversal and return flows were not written into the scheme rules, providers share no common obligation to honour them, and retrofitting a rulebook across live participants is a slow and contested negotiation. Second, if the message and data

model did not preserve the information needed to trace a transaction across participants, the evidence required to adjudicate a dispute does not exist and cannot be reconstructed after the fact (CGAP, 2022). Third, if resolution timelines were never instrumented, the operator and the regulator cannot see which providers are failing users, and they cannot enforce what they cannot measure. Fourth, if no independent escalation path was designed, a consumer whose provider denies a claim has nowhere to go, and constructing that path after launch means renegotiating responsibilities among institutions that now have every incentive to protect their own positions.

6.3 Evidence from global benchmarking

The World Bank's global benchmarking of financial consumer protection illustrates how wide the gap between intent and practice remains. Its survey gathered responses from financial sector authorities in well over one hundred jurisdictions and assesses consumer protection across five pillars, the legal, regulatory and supervisory framework, disclosure and sales practices, fair treatment and business conduct, data privacy, and dispute resolution (World Bank, 2023). The recurring finding is that dispute resolution is among the weakest pillars. Internal dispute resolution by providers is widely present in principle, but independent external dispute resolution, decisions that bind the provider, and effective mediation are far less consistently in place, only a minority of authorities report following the good practice of issuing decisions binding on the provider (World Bank, 2023). The pattern mirrors the compliance layer trap, the elements that can be met on paper are widely adopted, while the elements that require operational design and enforcement lag. Redress belongs to the second group, which is precisely why it is so often the missing capability.

6.4 Internal versus external dispute resolution

The distinction between internal and external dispute resolution is central to understanding why independence must be designed in. Internal dispute resolution, handled by the provider, resolves the majority of routine complaints and should be the first line. But it cannot be the only line, because the cases that most damage trust are those in which the provider itself is implicated, whether through its own error, its systems or its unwillingness to accept a claim. External dispute resolution, an alternative and independent process outside the provider, exists to catch exactly these cases (World Bank, 2023). For it to function in a multi participant instant payment system, it must operate across provider types, so that a consumer can pursue a claim regardless of whether the counterpart was a bank, a fintech or a mobile money operator. That cross provider reach is an architectural and governance property, not something a single provider can supply.

7. The Economics of Late Redress

7.1 Why retrofitting is expensive

The cost of redress is not fixed, it depends heavily on when the capability is introduced. Designed in at the blueprint stage, the incremental cost of traceability, reversal flows, enforceable timelines and an escalation path is modest, because each is a design input that shapes the system as it is built. Introduced after go live, each becomes a remediation programme in its own right, whether a rulebook renegotiation, a data model change propagated across every participant, a new measurement and reporting capability, or the construction of an independent escalation body and the reallocation of responsibilities among institutions already in production. The same capability that is inexpensive as a design choice becomes expensive as a change request, and some elements, particularly the retention of transaction data that was never captured, cannot be recovered at any price.

7.2 Incentive misalignment among participants

Late redress also runs into an incentive problem. Once a system is live, the allocation of responsibility for disputed transactions has direct commercial consequences for each participant. A rule introduced after launch that assigns liability for certain reversals, or that requires providers to meet measured resolution timelines, will be resisted by those who bear its costs. At the design stage, by contrast, participants negotiate these obligations behind a partial veil of ignorance, before they know exactly how the costs will fall, which makes agreement easier and outcomes fairer. Designing redress upstream is therefore not

only cheaper in engineering terms, it is more achievable in governance terms, because it precedes the entrenchment of positions.

7.3 Redress as an option on trust

There is a further way to understand the value of upstream redress. Building redress into the blueprint is, in effect, purchasing an option on trust. The cost is incurred early and is relatively small. The payoff is realised later and can be large, it is the retention of users at the moment of failure, the point at which trust is most likely to be lost. Systems that decline to purchase this option are exposed to a tail risk that does not show up in adoption metrics until users have already begun to leave. Because the damage propagates through social networks, by the time it is visible in the numbers it is expensive to reverse. Upstream redress converts an unmanaged tail risk into a small, known, early cost.

8. A Redress Readiness Diagnostic

Because the capabilities that make redress possible are set at design time, the highest value intervention is to ask the right questions upstream, before significant investment is committed and while the answers can still change the blueprint. In the diagnostic framework presented here, these questions are organised into four domains. They are design questions to be answered at the outset, not a checklist to be completed at launch.

8.1 Scheme rules and design

- Are dispute, reversal and return flows explicitly defined in the scheme rules, with a clear allocation of responsibility among the sending institution, the receiving institution and the operator?
- Does the message standard and data model preserve sufficient information, end to end, to trace a disputed transaction across every participant that handled it, and for a defined retention period?
- Does the settlement model accommodate reversals and returns without creating unmanaged liquidity or credit risk for participants?

8.2 Timelines and measurement

- Are resolution timelines defined, enforceable and expressed in terms the end user can rely on, rather than left to each provider's discretion?
- Is the system instrumented to measure whether those timelines are met, by participant, so that performance is visible to the operator and the regulator?
- Are there defined consequences, within the scheme's governance, for participants that persistently fail to meet resolution obligations?

8.3 Independence and escalation

- Is there an escalation path that functions across banks, fintechs and mobile money operators when a single provider cannot or will not resolve a claim?
- Can a consumer reach an independent channel, including where their own provider is the source of the problem?
- Are consumers made aware that the recourse channel exists, and is it accessible to users with low literacy, limited connectivity or disabilities?

8.4 Evidence and fairness

- Can the system evidence fair outcomes, not merely uptime, by demonstrating how disputes were resolved and whether affected users were made whole?
- Are the needs of the most vulnerable users, who face the greatest harm from fraud and unresolved loss, explicitly designed for rather than assumed away? Answered at the blueprint stage, these questions cost little and shape the design. Answered after go live, each becomes a remediation programme of the kind described in Section 7. The diagnostic value lies precisely in asking them before the answers are locked in.

9. A Lifecycle Framework for Embedding Redress

Redress readiness is not a single gate but a thread that runs through the whole delivery lifecycle. The framework below maps redress activity to six connected delivery capabilities, from diagnostics and readiness through to operational resilience. It makes explicit that redress can be embedded continuously rather than inspected for at the end.

Delivery capability	Redress focus	Representative deliverable
Diagnostics	Assess current readiness	Gap and readiness assessment

Delivery capability	Redress focus	Representative deliverable
Programme design	Convert gaps into rules, data and governance	Rulebook, data requirements and operating model
Delivery assurance	Track requirements throughout the build	Requirements traceability matrix
Certification	Test tracing, return and escalation	Unhappy path certification
Go live assurance	Gate launch on redress capability	Readiness decision and risk assessment
Operational resilience	Monitor outcomes and recurring causes	Dashboard and remediation plan

9.1 From diagnosis to design

The early stages establish the truth of the current situation and convert it into requirements. Diagnostics and readiness scan the ecosystem to establish where redress obligations sit today, which participants can meet them, and what the legal, regulatory, technical and participant level constraints are, producing an honest picture of the gap between the redress a market promises and the redress it can deliver, and defining the interventions required before money is committed. Strategy and programme design then translate these findings into concrete inputs. These include scheme rule provisions for dispute, reversal and return, data and message requirements that make tracing possible, timeline and escalation obligations, and the governance arrangements that will enforce them.

9.2 From build to assurance

The later stages prove that the designed capability actually exists. Implementation and delivery assurance keep redress requirements visible through the build using a traceability matrix, so that they are not quietly dropped under delivery pressure. Testing and certification treat dispute, reversal and escalation as first class test cases, participant certification includes the ability to originate, receive and resolve disputes correctly and within the defined timelines, so that the capability is proven for every participant rather than assumed, and the unhappy path is tested with the same rigour as the successful payment. Go live assurance makes redress capability an explicit launch criterion, a system is ready not when it can move money, but when it can also resolve a dispute about money that has moved. Finally, operational resilience monitors resolution performance as an ongoing operational metric, with the same seriousness as availability, so that degradation is detected and corrected rather than discovered through user attrition.

9.3 Implementation sequence

The implementation sequence begins with ecosystem diagnosis and legal review. Scheme design then assigns liability, defines case categories and establishes escalation authority. Procurement translates those decisions into requirements for messaging, case management, reporting and integration. Implementation configures workflows and participant interfaces. Certification proves tracing, reversal, return, reimbursement and escalation using realistic cases. Launch approval depends on evidence that every critical path works. Ongoing supervision then monitors outcomes, recurring causes and participant performance.

9.4 Illustrative payment journey

Consider a customer who sends an instant payment and sees a debit, while the intended recipient reports no credit. The customer reports the case to the sending provider using the transaction reference. The sending provider checks its ledger and submits a structured investigation request through the scheme. The operator traces the transaction across the switch and settlement records. The receiving provider confirms whether funds were credited, held or rejected. If the payment failed before completion, the defined reversal process restores the customer balance. If final settlement occurred, the return process is used where the rules permit. If the providers disagree or miss the service deadline, the case moves to scheme escalation and then to an independent body. The customer receives a reasoned outcome and the system retains evidence for supervision.

10. Measuring Trust with a Maturity Model and Scorecard

10.1 A redress maturity model

If redress is infrastructure, its presence can be assessed on a maturity scale in the same way as other infrastructural properties. The model below describes five levels, from the absence of any defined redress to a mature state in which redress is evidenced and trusted. It is deliberately aligned with the logic of the AfricaNenda inclusivity spectrum, on

which consumer recourse is the element that distinguishes the most advanced systems, and on which reaching maturity requires both establishing standards for recourse and, ideally, providing a direct channel for a consumer to dispute a transaction when their provider cannot resolve it (AfricaNenda Foundation, World Bank and UNECA, 2025).

Level	Redress posture	Observable characteristics
0	Absent	No defined redress. Disputes are handled individually and users may bear the loss
1	Nominal	A policy exists but cases are not consistently traceable, timed or enforced
2	Operational	Provider level resolution works but no reliable cross provider path exists
3	Interoperable	Scheme rules define returns and escalation, timelines are measured and an independent path exists
4	Mature	Outcomes are evidenced, direct recourse is accessible and vulnerable users are explicitly considered

The value of the model is diagnostic. A system may describe itself as having consumer protection while remaining at level one or two, a policy exists, and provider level complaints handling functions, but there is no interoperable reversal and escalation capability and no independent, evidenced resolution. The gap between level two and level three is the gap this paper is concerned with, because it is the gap that cannot be closed by a document and must instead be designed into the rules, the data model and the governance.

10.2 A trust centred scorecard

The maturity model is qualitative, it should be complemented by quantitative indicators that make trust visible and manageable. A trust centred scorecard sits alongside adoption figures and reports whether the system delivers fair outcomes. Useful indicators include the share of disputes resolved within the defined timeline, the proportion of users who know that a recourse channel exists and how to reach it, the availability and independence of escalation across provider types, the rate at which users are actually made whole after a valid claim, and, critically, the confidence and resolution outcomes of the most vulnerable users rather than the population average. These indicators are not a compliance report. They are management information that allows operators and regulators to detect erosion of trust before it shows up as user attrition.

10.3 Redefining the inclusion metric

The broader implication is that financial inclusion should not be measured only by accounts opened. An account that its holder does not trust is not inclusion in any meaningful sense, it is a dormant liability on an inclusion dashboard, and the persistence of large inactive account shares suggests this is not a hypothetical concern (GSMA, 2026). A more honest measure combines reach with trust, not only how many people can transact, but whether they believe their money is safe and that redress exists when it is not. On that measure, the most mature systems in the SIIPS inclusivity spectrum establish consumer recourse standards and direct dispute channels (AfricaNenda Foundation, World Bank and UNECA, 2025). Recourse is emerging as the differentiator between a system that is merely live and one that is genuinely inclusive.

10.4 Scoring the Andrew Manuel Redress Maturity Model

Each capability is assessed using documented evidence rather than management assertion. A score of zero indicates that no binding rule or operating process exists. A score of one indicates a policy or provider specific arrangement without consistent operation. A score of two requires functioning provider level workflows and basic reporting. A score of three requires tested cross provider operation, enforceable service levels and accessible independent escalation. A score of four requires outcome based supervision, publication of performance, analysis by customer segment and continuous improvement based on root causes. A market should report both the overall score and the lowest capability score because a strong average can conceal a critical weakness.

10.5 Core redress indicators

The minimum scorecard should report complaints per one hundred thousand transactions, median and upper percentile resolution time, cases resolved within the service level, unresolved cases, reimbursement value and rate,

repeat complaints, escalation rate, independent decisions that overturn provider outcomes, customer awareness of recourse and satisfaction with the fairness of the result. Results should be segmented where lawful and feasible by provider, channel, case type, gender, disability, location and customer vulnerability. Publication should protect personal information and should not create incentives to suppress valid complaints.

11. Governance and Cross Provider Coordination

Redress in a modern payment ecosystem is inherently a cross institutional problem, and its weakest point is usually the boundary between institutions. A dispute that arises within a single provider can, in principle, be resolved by that provider. A dispute that spans a bank, a fintech and a mobile money operator can only be resolved if the scheme's governance defines how responsibility is allocated and how a claim moves across the boundary. This is why redress cannot be delegated wholly to individual participants and must be a property of the scheme (CPSS IOSCO, 2012).

11.1 The three decisive governance elements

Three governance elements are decisive. The first is the rulebook, which must define dispute, reversal and return flows and the allocation of responsibility among participants, so that obligations are common rather than voluntary. The second is measurement and enforcement, which requires the operator to instrument resolution performance and the governance framework to attach consequences to persistent failure, so that timelines are commitments rather than aspirations. The third is the independent path, which requires an external dispute resolution mechanism that operates across provider types (World Bank, 2023). Regulators have a distinctive role in all three, consistent with the G20 High Level Principles for Digital Financial Inclusion, they can require redress capability as a condition of authorisation and interoperability, supervise the operational reality of redress using the data the system is built to produce, and stand behind or host the independent escalation mechanism where the market cannot provide it credibly on its own (GPFI, 2016, 2025).

11.2 An independent recourse mechanism

The independent path is worth treating as a distinct institutional question rather than a by product of the rulebook. In mature consumer protection systems it takes the form of an external dispute resolution

body, an ombudsman or equivalent, that a consumer can approach when their provider has failed to resolve a complaint (World Bank, 2023). For such a body to be effective in a multi participant payments ecosystem it must meet several conditions, it must cover all provider types, so that a consumer is not turned away because the counterpart was a fintech rather than a bank, it must be free or low cost and genuinely accessible, including to users with low literacy or limited connectivity, its decisions must carry weight, ideally binding the provider, and it must feed the data it generates back into supervision, so that patterns of failure inform regulation. Whether the mechanism is industry run under regulatory oversight or hosted by the regulator itself, it must be designed and resourced deliberately, because an escalation path that exists only on paper offers the consumer nothing.

11.3 Redress in cross border and regional payments

As African payments integrate across borders through regional switches and pan continental schemes, redress becomes a cross jurisdictional problem as well as a cross provider one. A disputed transaction may originate in one country and settle in another, under different national rules, currencies and consumer protection regimes. This raises design questions that must be answered by the regional infrastructure itself, which rulebook governs a cross border dispute, how resolution timelines are harmonised across participating systems, how liability is allocated between institutions in different jurisdictions, and how a consumer in one country reaches an independent recourse channel for a transaction that failed in another. These questions are being decided now, as regional payment infrastructure is designed and built, which is precisely the moment to embed cross border redress rather than to discover its absence after the first cross border fraud or failure. The upstream principle applies with even greater force at the regional level, because retrofitting redress across sovereign systems is harder still than retrofitting it within one.

12. Implications and Recommendations

The argument of this paper has implications for every actor in the payments ecosystem. The recommendations below are addressed to each in turn, because redress is a shared property that no single participant can secure alone.

12.1 For central banks and regulators

Set redress expectations as design requirements, not post launch guidance. Require that scheme rules define dispute, reversal and escalation flows, that resolution timelines are enforceable and measured, and that an independent path exists across all participant types. Supervise the operational reality of redress using data the system is built to produce, and make redress capability a condition of licensing new payment systems and of granting interoperability, so that it is designed in from the start rather than negotiated after harm has occurred (World Bank, 2023, GPFI, 2016).

12.2 For ministries of finance and public policymakers

Treat consumer trust as a determinant of the return on national payments and digital public infrastructure investment. Where public funds or sovereign borrowing support a payment system, condition them on redress readiness, and ensure that national payment strategies and financial inclusion targets measure trust and recourse, not only accounts opened. A rail that citizens do not trust will not deliver the inclusion, government payment efficiency or formalisation benefits used to justify the investment.

12.3 For multilateral development banks and development partners

Ask the redress questions before committing capital, and fund the upstream diagnosis and design work that determines whether redress will be built in. Because remediation after go live is more expensive and less effective than getting the blueprint right, the most efficient use of concessional and technical assistance resources is at the diagnostic and design stage. Conditioning support on redress readiness, and financing the work that establishes it, is a high leverage intervention. The cheapest redress mechanism is the one designed into the system from the start.

12.4 For payment system operators and scheme owners

Treat redress as part of the product rather than an obligation to be minimised. Build dispute, reversal and tracing capability into the rulebook, the message standard and the certification regime, make redress performance both a launch criterion and an ongoing operational metric, and compete on trust as well as on cost and speed. In a market where users can revert to cash at any moment, the operator that can resolve failures fairly and demonstrably will retain the users on whom the entire inclusion agenda depends.

12.5 For commercial and microfinance banks

As scheme participants, banks and microfinance institutions are where most disputes are first raised and resolved. Invest in internal dispute resolution that meets the scheme's defined timelines, ensure the data captured at onboarding and in transaction processing supports end to end traceability, and treat participation in cross provider escalation as an obligation rather than a courtesy. Microfinance institutions in particular serve the users most exposed to unresolved loss, and credible redress is central to the trust on which their client relationships depend.

12.6 For mobile network operators and mobile money providers

Mobile money operators carry a large share of first time and vulnerable users, and are often the front line for fraud and failed transactions. Build reversal, tracing and complaint handling capability into the platform and into interoperability arrangements with banks and other providers, resource the customer facing recourse channels adequately, and design proactively for users with low literacy or connectivity. Because these operators frequently sit at the boundary between systems, their participation in a common, cross provider redress framework is decisive for whether it works at all.

12.7 For fintechs and payment service providers

Fintechs compete on user experience, and redress is part of that experience even though it is invisible until something fails. Build dispute and reversal handling into the product from the first release rather than deferring it, integrate with scheme level tracing and escalation rather than constructing closed workarounds, and treat transparent, timely recourse as a differentiator with both users and regulators. A fintech that can demonstrate fair outcomes will earn the trust, and the regulatory confidence, that sustained growth requires.

13. Applying the framework in practice

The framework is intended for use before significant investment decisions and again at each major delivery gate. A diagnostic engagement should establish the current legal, institutional, technical and operational position. The programme can then define required scheme rules, data capabilities, service levels, accountability arrangements and

evidence standards. Delivery assurance should test whether those requirements have been implemented across the operator and every participant type.

The work can be commissioned by a financial authority, payment system operator, development partner or prime implementation contractor. Independence is important where the same organisation is responsible for delivery and for judging readiness. The practical objective is to identify material gaps while design choices remain open, prove the required capabilities before launch and establish the information needed for continuing supervision.

14. Limitations and areas for validation

This paper develops a general design framework. It does not test causal relationships between redress quality and sustained usage, and it does not estimate the cost of remediation for a specific system. The proposition that upstream design is less costly than late remediation is grounded in systems engineering logic and implementation experience, but market level business cases should quantify local costs, risks and benefits before investment decisions.

Card chargeback arrangements demonstrate that rules, reason categories, evidence and escalation can be engineered into a payment scheme. They cannot be copied directly into instant payment systems. Card payments and instant account payments differ in authorisation, settlement, participant roles, fraud patterns and legal treatment. Each market must design arrangements that preserve settlement finality and allocate responsibility fairly.

The African examples in SIIPS 2025 illustrate different institutional and operating contexts rather than a single model. Country assessments should verify the current rules and performance of each scheme directly with its operator and regulator. Further research should test how redress affects continued usage, trust and outcomes for women, first time users, people with disabilities and customers with limited literacy or connectivity.

15. Conclusion

Africa's payment rails are a genuine achievement, and the momentum behind them is real. The next phase of progress will not be won by adding more rails alone. It will be won by making the rails trustworthy, so that the people newly brought into formal finance stay there. That requires treating consumer redress as what it is, infrastructure, designed into the scheme rules, the blueprint, the test scripts and the go live criteria, measured with the same seriousness as availability and throughput, and governed across the boundaries between institutions where it is most likely to fail. Recent African research places recourse within the broader requirements for inclusive instant payment systems (AfricaNenda Foundation, World Bank and UNECA, 2025). Global consumer protection benchmarking also shows material differences between formal frameworks and the operational capabilities available to consumers (World Bank, 2023). The question every market should be asking is not whether it can move money faster. It is whether, when something goes wrong, it can trace, reverse, escalate and resolve, and evidence a fair outcome. How is your market designing redress into its payment systems, rather than adding it later?

References

- AfricaNenda Foundation, World Bank and United Nations Economic Commission for Africa, 2025. The State of Inclusive Instant Payment Systems in Africa, SIIPS 2025. AfricaNenda Foundation. Available at AfricaNenda SIIPS 2025 report page. Accessed 10 September 2026.
- CGAP, 2022. The Evolution of the Nature and Scale of Digital Financial Services Consumer Risks, A Review of Evidence. Washington DC, Consultative Group to Assist the Poor. Available at CGAP consumer protection collection. Accessed 10 September 2026.
- Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, 2012. Principles for Financial Market Infrastructures. CPSS Publications No. 101. Basel, Bank for International Settlements. Available at BIS Principles for Financial Market Infrastructures page. Accessed 10 September 2026.
- Demircuc Kunt, A., Klapper, L., Singer, D. and Ansar, S., 2022. The Global Findex Database 2021, Financial Inclusion, Digital Payments and Resilience in the Age of COVID 19. Washington DC, World Bank.
- Global Partnership for Financial Inclusion, 2016. G20 High Level Principles for Digital Financial Inclusion. Global Partnership for Financial Inclusion. Available at GPFi publication page. Accessed 10 September 2026.
- Global Partnership for Financial Inclusion, 2025. G20 Policy Recommendations for Moving from Financial Access to Usage. Global Partnership for Financial Inclusion. Available at GPFi publication page. Accessed 10 September 2026.
- GSMA, 2026. State of the Industry Report on Mobile Money 2026. London, GSMA. Available at GSMA mobile money report portal. Accessed 10 September 2026.
- International Organization for Standardization, n.d. ISO 20022 Universal Financial Industry Message Scheme. Available at ISO 20022 official website. Accessed 10 September 2026.
- Mastercard, 2026. Mastercard Rules and Compliance Programs. Purchase, New York, Mastercard International. Available at Mastercard rules and compliance page. Accessed 10 September 2026.
- Payment Systems Regulator, 2024. Faster Payments Authorised Push Payment Scams Reimbursement Requirement, Policy Statement. London, Payment Systems Regulator.
- Payment Systems Regulator, 2026. Authorised Push Payment Fraud Reimbursement Protections. London, Payment Systems Regulator. Available at PSR consumer protection page. Accessed 10 September 2026.
- Suri, T. and Jack, W., 2016. The long run poverty and gender impacts of mobile money. Science, 354, 6317, pp. 1288 to 1292. DOI 10.1126 science.aah5309.
- Visa, 2026. Visa Core Rules and Visa Product and Service Rules. San Francisco, Visa Incorporated. Latest edition available through the Visa rules page. Accessed 10 September 2026.
- World Bank, 2023. The Global State of Financial Inclusion and Consumer Protection 2022. Washington DC, World Bank. doi 10.1596/40335. Available at World Bank Open Knowledge Repository. Accessed 10 September 2026.
- World Bank, 2025. The Global Findex Database 2025. Washington DC, World Bank. Available at the Global Findex portal. Accessed 10 September 2026.

Appendix A, Redress Readiness Checklist

The following checklist consolidates the diagnostic questions of Section 8 into a form that programme teams, operators and regulators can apply at the design stage. Each item should be answerable with reference to the scheme rules, the message and data model, or the governance framework, not to a customer service policy. The overall posture can then be located on the maturity model of Section 10.

- Scheme rules define dispute, reversal and return flows, with responsibility allocated among sending institution, receiving institution and operator.
- The message and data model preserves end to end traceability of a disputed transaction for a defined retention period.
- The settlement model accommodates reversals and returns without unmanaged liquidity or credit risk.
- Resolution timelines are defined, enforceable, measured by participant, and expressed in terms the end user can rely on.
- Governance attaches consequences to persistent failure to meet resolution obligations.
- An escalation path functions across banks, fintechs and mobile money operators, including where the consumer's own provider is at fault.
- An independent recourse channel exists and is accessible to users with low literacy, limited connectivity or disabilities, and consumers are made aware of it.
- For instant, irrevocable rails, the treatment of authorised push payment fraud and liability allocation is defined before launch.
- The system can evidence fair outcomes, including whether affected users were made whole, not merely uptime.
- The needs of the most vulnerable users are explicitly designed for rather than assumed away. A system that cannot answer these in the affirmative at the blueprint stage is not ready to commit investment, it is ready for an upstream redress readiness engagement.

Appendix B, Glossary of Key Terms

Authorised push payment (APP) fraud. Fraud in which a consumer is deceived into authorising a payment to a fraudster, whether by being misled about the recipient or the purpose of the payment.

Chargeback. A defined mechanism in the card networks by which a disputed transaction is reversed through the scheme's rules, following standardised reason codes and timelines.

External dispute resolution (EDR). An independent process outside the provider, such as an ombudsman or arbitration body, that resolves complaints the provider has not resolved satisfactorily.

Instant payment system (IPS). A retail payment system that clears and settles transactions in or near real time, typically on a push basis and with immediate finality.

Internal dispute resolution (IDR). The complaints handling process operated by an individual provider as the first line of redress for its own customers.

Interoperability. The ability of customers of different providers, including banks, fintechs and mobile money operators, to transact with one another across a common scheme.

Irrevocability. A design property of many instant payments whereby, once authorised, a transaction settles with finality and cannot be unilaterally reversed.

ISO 20022. An international standard for richer, structured financial messaging that supports end to end traceability of transactions across participants.

PFMI. The CPSS IOSCO Principles for Financial Market Infrastructures, the international standards for the governance, risk management and operation of payment and settlement systems.

Redress. The set of capabilities that allow a consumer harmed by a payment to obtain a fair resolution, tracing, reversal or return, escalation and evidenced outcome.

Reversibility. The ability of a system to reverse or return a transaction where the rules require it, dependent on scheme rules and the settlement model.

Scheme rules (rulebook). The binding rules of a payment scheme that define participation, message standards, settlement, and dispute, reversal and escalation obligations.

Traceability. The ability to follow a disputed transaction end to end across every participant that handled it, a function of message and data design.

Appendix C Minimum redress scorecard

Indicator	Purpose	Suggested reporting
Complaint rate	Shows demand for redress relative to usage	Cases per one hundred thousand transactions
Resolution time	Tests whether users receive timely outcomes	Median and upper percentile days
Service level compliance	Measures enforceability	Percentage completed within the rulebook limit
Reimbursement	Shows whether affected users are made whole	Cases and value reimbursed
Escalation	Shows provider and scheme effectiveness	Percentage escalated and outcomes overturned
Awareness and fairness	Measures trust and accessibility	Survey result by customer segment

Scheme accountability matrix

A credible redress framework assigns responsibility across the transaction chain and provides an independent decision path when participants disagree.

Actor	Primary responsibility
Customer provider	Receive the case, protect the customer, investigate promptly and communicate the outcome
Receiving provider	Trace receipt, preserve funds where lawful, respond to investigation and execute an authorised return
Scheme operator	Maintain rules, case messages, service levels, evidence, escalation and participant performance reporting
Regulator	Set minimum outcomes, supervise implementation, require corrective action and protect vulnerable users
Independent body	Review unresolved complaints and issue a fair decision within its legal authority