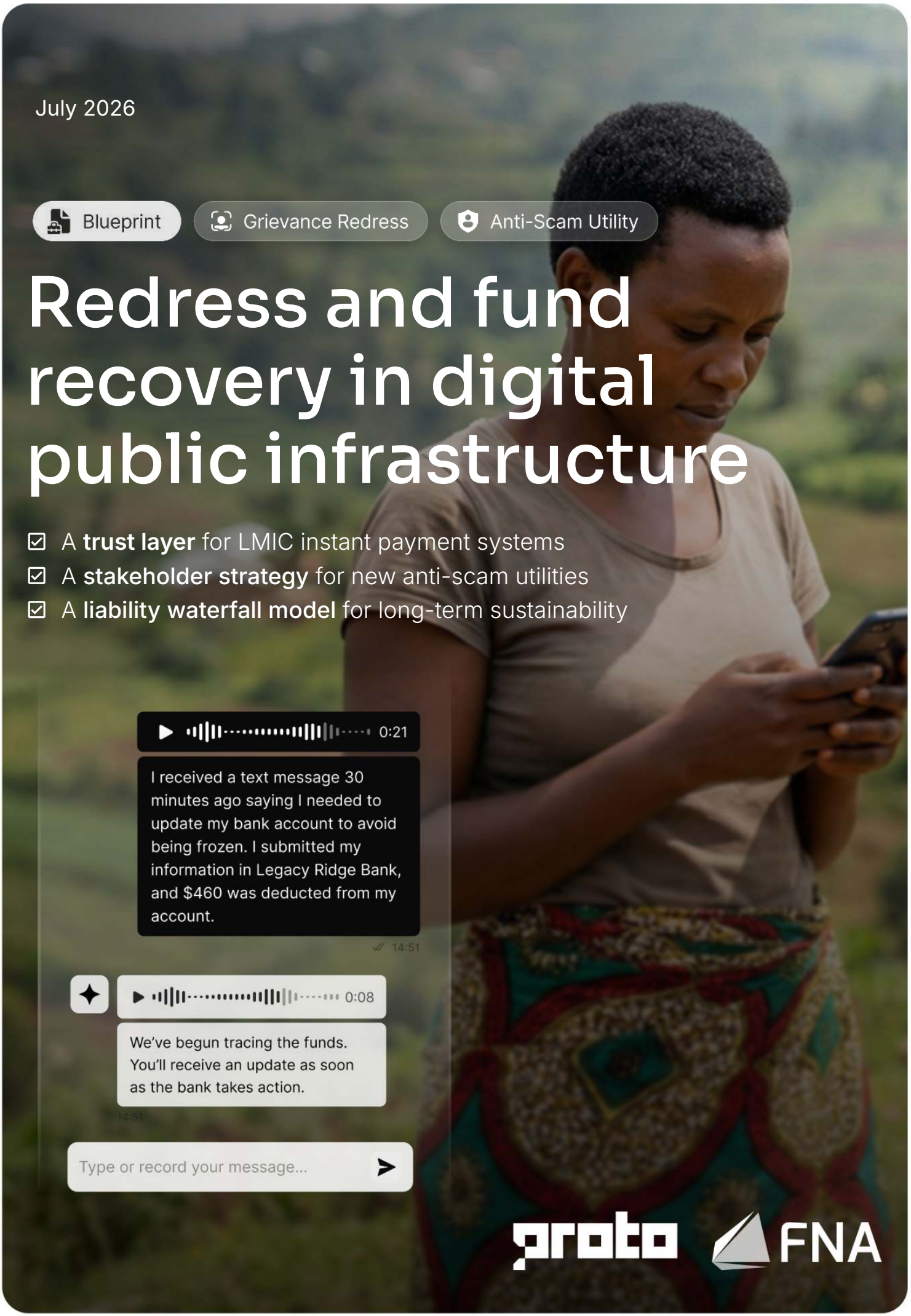
July 2026

Blueprint | Grievance Redress | Anti-Scam Utility

Redress and fund recovery in digital public infrastructure

- ☑ A **trust layer** for LMIC instant payment systems
- ☑ A **stakeholder strategy** for new anti-scam utilities
- ☑ A **liability waterfall model** for long-term sustainability



grata FNA

Authors & Acknowledgements

Curtis Matlock
CEO, Proto, MSc Technology and Public Policy

Curtis is the founder of **Proto**, a social enterprise that deploys inclusive AI redress systems across low- and middle-income countries, such as Rwanda and the Philippines. He served in Canada's armed forces and studied political science at its military college before learning Chinese at the National Taiwan University. His training in public policy from the UN's International Labour Organisation at the University of Turin underpins this blueprint.

Kimmo Soramäki
CEO, FNA, PhD Operations Research

Kimmo is the founder of **FNA**, a financial network analytics innovator that specialises in track-and-trace technology for national fraud portals, such as Malaysia, Indonesia, and the UAE. He has 20+ years of experience as an economist at the Bank of Finland, and visiting researcher at the Bank of England and the US Federal Reserve. He holds scientific degrees in Operations Research and Economics from Aalto University, and led the G20-awarded *Trust at Speed* integrated redress and recovery system.

Noella Dushime
Head of Partnerships, Proto, BSc Computer Science

Noella is a business expansion leader specialised in the application of emerging technology to Africa's public sector. Her career started in the telecommunications industry and led to Irembo, Rwanda's e-gov platform, where she led growth and partnerships. She leads Proto's evolving redress deployments in countries such as Mozambique and Liberia, in coordination with central banks, financial supervisors, and development partners.

Weiying Kok
CTO, Proto, MSc Bioinformatics

Weiying is a natural language processing engineer leading the development of Proto's AI models for redress in low-resource languages, such as Kinyarwanda and Cebuano. Her career started at MIMOS, Malaysia's applied research and development centre for socio-economic growth, following studies in bioinformatics and cognitive science. She leads the engineering of Proto's inclusive AI infrastructure – the technical backbone of the redress layer described in this blueprint.

Gates Foundation

The **INV-073649** and **INV-073693** grants from the Gates Foundation informed this blueprint's recommendations.

RUSI

The Royal United Services Institute's parallel research on authorised payment fraud provided key insights for policy design and governance.

Table of Contents

If it weren't for BOB [the central bank AI agent in the Philippines], I probably wouldn't have gotten my refund. It's a very good way **for consumers like us to have a voice**... you can talk to it like a regular person. You can use English, Tagalog, or Taglish.

Kitty Elicay
Financial Consumer in the Philippines

Read full story →

01 Executive Summary

This blueprint provides a comprehensive answer to a single policy problem: **how to deploy a sustainable trust layer into digital public infrastructure (DPI)?**

During the past decade, bilateral and philanthropic donors have funded DPI technology that expanded access to financial services for over 1.1 billion citizens across low- and middle-income countries (LMICs). In particular, instant payment systems are accelerating financial services – driven by an array of open-source, proprietary, and sovereign frameworks. However, this access and scale has been systematically exploited by transnational criminal networks.

The scale of this threat to the poorest and newest consumers is now clear. Global scam losses were approximately US$579.4 billion in 2025.[1] In Brazil, scams via the Pix instant payment system reached an estimated 28 million cases in the first three quarters of 2025 alone, with R$6.5 billion in confirmed fraud losses and a recovery rate of only 7%.[2] In India, digital fraud totalled US$2.5 billion in 2025, with the Reserve Bank of India now prioritising stakeholder consultations on mule-account monitoring and user-side controls.[3]

In smaller LMICs, 21% of grievances processed by Proto's regulatory AI agents were classified as scam reports – none of which resulted in successful fund recovery as the appropriate form of redress.[4] There is no lack of research or international guidance: RUSI, FATF, INTERPOL, UNDP, OECD, and the World Bank have converged on the same principles for constraining authorised payment fraud.[5]

Rather, the persistent gap across LMICs is operational: the absence of a replicable model that helps establish redress and recovery systems as core DPI, sustain these without recurring donor capital or stakeholder resistance, and protect low-income consumers from bearing the cost of their trust in everyday digital services.

> **"The challenge right now is, whose baby is this?"**
> Rajesh Bansal, former CEO, Reserve Bank of India Innovation Hub on anti-scam system ownership between regulators, police, and financial institutions.

[1] Nasdaq Verafin (2026). 2025 Global Financial Crime Report.
[2] Banco Central do Brasil (2026). MED 2.0 announcement and Pix fraud disclosure; TI Inside Online (2025).
[3] BBC News (2026). Digital fraud costs Indians $2.5bn in 2025; Reserve Bank of India (2026). Discussion paper on measures to curb digital fraud.
[4] Proto (2026). FY2025 data across deployments in the Philippines, Rwanda, Mozambique and Namibia.
[5] Royal United Services Institute, Centre for Finance and Security (2026). Authorised Payment Fraud: Approaches to Policy Design and Governance. London: RUSI.

The Trust Layer

This blueprint covers three technical functions governed by a central bank mandate:

- **Redress** delivers zero-cost grievance intake through messaging app, SMS, and voice channels in local languages with AI-mediated resolution and auto-escalation for scam reports.
- **Recovery** executes real-time cross-institution tracking and tracing with time-limited fund freezing capability delegated to an anti-scam utility with KYC-verified victim fund return.[6]
- **IPS integration** federates fraud signals under a hybrid data sovereignty model, while preserving data in financial institutions and allowing redress and recovery workflows.

The Stakeholder Strategy

This blueprint sequences stakeholder engagement in three phases per the influence-interest mapping exercise to support successful redress and recovery implementations in LMICs[7]:

- **Establish (months 0–6).** Move fast with the smallest coalition to organise and issue authority.
- **Scale (months 6–18).** Widen the coalition as performance KPIs become defensible publicly.
- **Sustain (month 18+).** Transition from an initial project to permanent governance and funding.

The Liability Waterfall Model

This blueprint outlines how LMICs can launch with donor capital support and transition to a 17-category liability waterfall that assigns first, second, and third payment responsibility across case types (see Instrument 4). The model has two non-negotiable properties:

- **Scheme protection pool.** Low-income consumers and social-protection beneficiaries must not pay for the Trust Layer. When no institutional payer is liable, a scheme protection pool is pre-funded through instant payment system levies to cover this cost.
- **No structural veto.** The Trust Layer's responsibilities are diffused across the central bank, IPS operator, financial institutions, and insurers. With the liability waterfall, no single participant can reasonably slow-walk implementation by virtue of bearing the entire eventual cost.

The liability waterfall model does not yet exist in LMICs for redress and recovery, and represents this blueprint's novel instrument. The model is based on three developed economy frameworks:

- The UK's Payment Systems Regulator introduced mandatory authorised push payment fraud reimbursement in October 2024, splitting costs 50/50 between sending and receiving institutions. In its first year, 88% of money lost to in-scope scams – £173 million – was reimbursed to victims, up from a 65% voluntary rate in 2024.[8]

[6] FNA (2025). A Blueprint for Building National Anti-Scam Utilities. London: FNA.
[7] Mendelow, A. (1991). Stakeholder Mapping. Proceedings of the 2nd International Conference on Information Systems, Cambridge, MA; Howlett, M., & Rayner, J. (2007). Design Principles for Policy Mixes. *Policy and Society* 26(4); RUSI CFS (2026). Authorised Payment Fraud, op. cit., Consideration 5.
[8] Payment Systems Regulator (2026). *APP Scams Reimbursement Dashboard for Q3 2025.* London: PSR.

- Singapore's Shared Responsibility Framework, which took effect in December 2024, was the first regulatory instrument to use the term "waterfall" explicitly – cascading liability from financial institutions to telcos to consumers depending on which party failed its duties.
- Australia's Scams Prevention Framework Act (February 2025) extended the logic furthest, empowering the Australian Financial Complaints Authority to allocate liability across multiple institutions on a multilateral basis; consumer losses in Australia fell 33.1% to AUD 318.8 million in 2024 as banks implemented controls ahead of full operationalisation.[9]

☑ **A self-sustaining trust layer**

A large-scale LMIC example of a redress and recovery system with no perpetual donor dependence – or risky funding reliance on a single stakeholder – could be seen in Pakistan. The Liability Waterfall Model would transition from a $3M donor sponsored project over 24 months to a prospective 5% success fee on Pakistan's estimated US$186 million fee-bearing fund recovery base. This would generate approximately US$9.3 million per year, sufficient to cover operating costs, generate revenue for regulators, and fund over 5,000 Benazir Income Support Programme (BISP) recipient grievance cases for every US$1 million of commercial recovery. Importantly, the waterfall is designed to ensure that the cost of the Trust Layer is not passed onto low-income consumers.

Instruments

Finally, this blueprint will provide policymakers and implementers with six ready-to-adapt instruments for their national Trust Layer projects:

1. **Policy Brief.** A template for policy professionals to secure initial approval for the redress and recovery implementation initiative.
2. **Central Bank Directive.** A template for the central directive and indemnity letter to be distributed across financial institutions and instant payment participants.
3. **Project Charter.** A template for project managers to align stakeholders within donor-funded redress and recovery implementations, and transition to long-term sustainability.
4. **Liability Waterfall Matrix.** A matrix to ensure the long-term sustainability of the redress and recovery systems by defining first, second, and third-pay responsibility across 17 categories.
5. **Instant Payment APIs.** Technical specifications required to embed the Trust Layer into the instant payment system, including API specifications for transaction enrichment, case event handover, performance SLAs for trace and freeze workflows, and audit logging requirements.
6. **Theory of Change.** A framework explaining *how* and *why* the Trust Layer's implementation will achieve its long-term consumer protection objectives.

[9] Department of the Treasury, Australia (2025). *Scams Prevention Framework: Protecting Australians from Scams.* Canberra: Commonwealth of Australia.

Two country cases – Pakistan and Namibia

Pakistan and Namibia are selected as this blueprint's national examples to bracket the institutional complexity and instant payment maturity ranges across LMICs in Asia and Africa. Both have yet to establish an agentic Trust Layer at scale and have the opportunity of donor-backed technology partnerships. Pakistan represents the federally-complex example where there are dual instant payment systems (one already used for G2P payment). Namibia represents the simpler, pre-instant payment case where the Trust Layer can be implemented as a core component rather than as a post-harm afterthought.

	Pakistan	Namibia
Population & exposure	240M citizens; ~US$9.3B annual scam losses (2.5% of GDP)[10]; 9M BISP beneficiaries on Raast.	3M citizens; 63% of adults targeted by scams; 11% confirm money losses.[11]
Payment & protection infrastructure	Two competing IPSs (Raast operated by SBP and 1LINK switch); G2P at population scale already live.	Pre-IPS – launching in 2026; *ConsumerConnect* redress system piloted for BoN, NAMFISA and CRAN.
Institutional configuration	Federally complex; strong central authority at SBP; Raast integration options available.	Federally simpler with under 10 major participating financial institutions; bankers' association chairs the fraud working group.
Languages for AI processing	Urdu, Punjabi, Sindhi, Balochi, Pashto	Afrikaans, English, German, Oshiwambo
Sustainability transition	Direct entry into the liability waterfall after $3M donor-funded trust layer implementation over 24 months; market complexity is addressed by integration with Raast instant payment (built by CMA).	Evolution from $200K donor-funded *ConsumerConnect* redress pilot into the liability waterfall as instant payment (built on Indian's UPI) launches. Stakeholder alignment ongoing.
Strategic role for replication to other LMICs	Stress-test for the liability waterfall in a high-complexity, multi-switch market with a politically salient protected consumer tier (BISP recipients).	Cleanest reference case for an LMIC instant payment deployment that embedded the Trust Layer as a fundamental component rather than a post-harm afterthought.

[10] Profit Pakistan Today (2025, October). Pakistan loses over $9 billion to financial scams annually.
[11] TransUnion Namibia (2024). Consumer Fraud Exposure Study.

02 LMIC Problem Snapshot

This blueprint provides a full-spectrum redress system, including, for example, mediated disputes between consumers and financial institutions. However, the most urgent grievance category is fraud and scams. INTERPOL's 2026 Global Financial Fraud Threat Assessment recorded a 54% increase in fraud-related notices and diffusions since 2024 and warned that almost half of the world's population is now targeted by scammers each week.[12] In LMICs, where formal safety nets are thin, each fraud represents a material financial inclusion setback: a social-protection payment intercepted, a mobile wallet drained, a microenterprise account compromised.

$579.4B	54%	<24h	59%
Global annual scam losses (Nasdaq Verafin 2026)	Rise in INTERPOL fraud notices since 2024	Window to trace and freeze funds	Female share of complainants[13]

The pattern is now well documented. GASA data show that consumers in developing countries are more likely to lose money to scams, and that these nations see a larger share of GDP lost; Nigeria, for example, lost an estimated 11.3% of GDP to scams in 2025.[14] The UNDP's Anti-Scam Handbook catalogues why developing countries are exposed: widespread digital platforms, high levels of economic informality, low institutional capacity, and the presence of pre-existing organised criminal groups.[15] FATF's 2026 update on cyber-enabled fraud confirms that scams are now “polycriminal” combining human trafficking, cybercrime, and terrorist financing.[16] A wave of national strategies has emerged in developed economies. The FATF, INTERPOL, and ASEAN have issued complementary guidance.[17] This guidance – recently synthesised in RUSI's Centre for Finance and Security report – recommends the qualities of an effective intervention: distributed legal obligations, cross-sectoral collaboration, and disciplined incentive design.[18] But, as RUSI argues, the gap in LMICs is the challenge of operationalising these international principles within the institutional realities of local jurisdictions. This blueprint exists in that gap.

[12] INTERPOL (2026). Global Financial Fraud Threat Assessment, Second Edition. INTERPOL.
[13] Proto (2025). Operational data from central bank grievance redressal AI agents in LMICs.
[14] GASA & Feedzai, Global State of Scams 2025, op. cit., p. 17.
[15] UNDP Global Centre for Technology, Innovation and Sustainable Development (2025). Anti-Scam Handbook v2.0: Collective response and tools to safeguard development.
[16] FATF (2026). Cyber-enabled fraud: Digitalisation and money laundering, terrorist financing and proliferation financing risks. FATF.
[17] FATF, Egmont Group & INTERPOL (2023). Illicit Financial Flows from Cyber-Enabled Fraud; ASEAN (2026). ASEAN Guide on Anti-Scam Policies and Best Practices.
[18] Royal United Services Institute, Centre for Finance and Security (2026). Authorised Payment Fraud: Approaches to Policy Design and Governance. RUSI.

03 The Trust Layer

DPI investments have transformed how governments deliver services at scale. National digital identity platforms, instant payment systems, and shared data lakes now underpin public service delivery in many LMICs. These systems handle financial entitlements and transactions with unprecedented efficiency for previously-excluded populations. However, the expansion of DPI has also revealed a structural imbalance: these systems have been designed primarily for throughput and inclusion, but not for redress or recovery when problems arise. As DPI becomes fundamental to economic life, this imbalance is a material risk to trust in digital public systems.[19]

In the context of financial consumer grievances, in particular fraud and scams, this trust is systematically eroded as manual, siloed reporting channels and human-triage processes cannot match the speed of criminal operations. This means that the most urgent scam reports face too many referral loops and manual steps to satisfy the <24 hours recovery window.

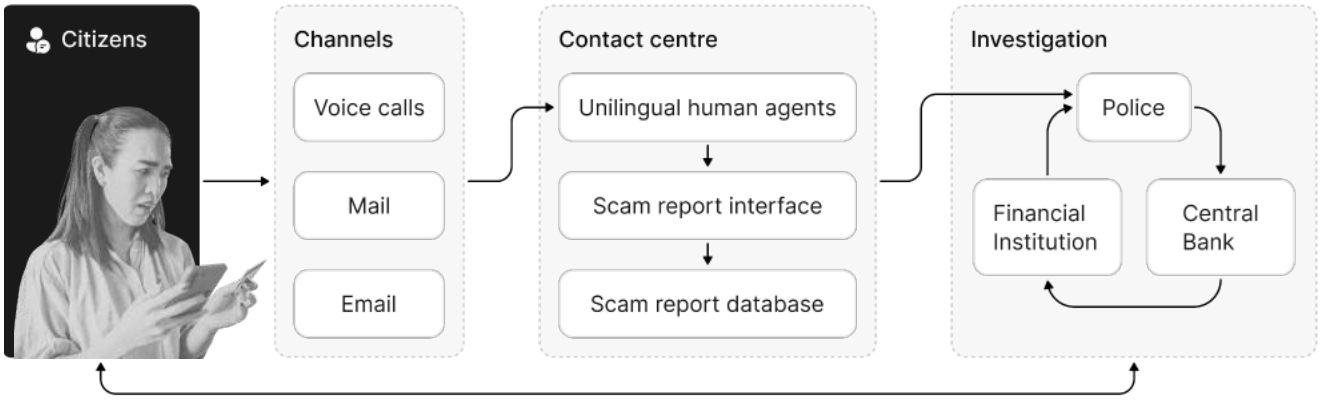


Figure 1 – An illustration of the manual workflows and trust gaps in siloed scam reporting.

Redress – beyond grievance referral

The Trust Layer is the operational expression of three integrated functions – redress, recovery, and IPS integration – that together enable a national system to receive and resolve grievances, or otherwise route, trace, freeze and recover consumer funds within the 24-hour window in which recovery remains feasible. Rapid and scalable redress relies on AI agents that understand citizen narratives in local languages and take coordinated action across institutions without requiring a human case officer to be available at every step. This is not automation as substitution for institutional accountability – it is automation as the precondition for matching problem complexity.

[19] Digital Impact Alliance, "Online Dispute Resolution and Digital Public Infrastructure – What's the Connection?", Expert Comment, 9 Oct 2024, Digital Impact Alliance.

3.1 Online dispute resolution

This starting point for redress is traditionally understood as “online dispute resolution” (ODR). ODR is increasingly recognised as a missing layer of digital public infrastructure rather than a peripheral application.[20] Research from UNCTAD and OECD precedent established that the trust deficit in DPI cannot be closed by identity, payment, and data exchange alone: without an accessible mechanism for citizens to seek redress, the benefits of digital inclusion are systematically eroded. The Digital Impact Alliance reinforced the same position in its 2024 expert comment on ODR and DPI.[21]

3.2 Accessible channels – deployment into financial institutions

The grievance intake system should be channel-agnostic and zero-cost to the consumer through WhatsApp, Telegram, Viber, LINE, Messenger, SMS, webchat, and voice call (IVR). The system should produce a structured case record – a standardised JSON object containing the extracted parameters of the grievance – regardless of intake channel, and ensuring case continuity from first contact through resolution. The redress agents should be integrated directly into the digital channels of regulated financial institutions (i.e. via an AI agent network) so that consumer-facing grievance interactions within bank apps or wallets automatically generate a case in the centralised system. This design shifts the burden of “knowing where to go” from the citizen to the public infrastructure. The National Bank of Rwanda’s *Intumwa* AI agent has been deployed across over 600 regulated entities, with direct website hosting and API integration for the 50 largest financial institutions.[22] This immediately accessible architecture resulted in 78% of grievances cases being generated directly from the financial institutions rather than the central bank’s own channels.

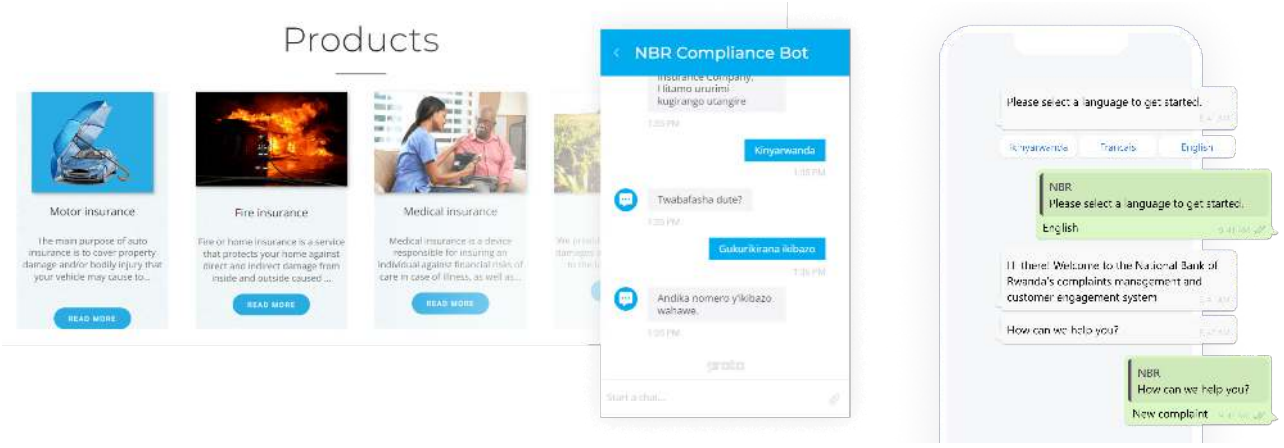


Figure 2 – A financial institution website hosting *Intumwa* and the central bank’s own WhatsApp channel.

[20] Tech Policy Press (2025). No Digital Public Infrastructure Without Redress.

[21] Digital Impact Alliance (2024, October). Online Dispute Resolution and Digital Public Infrastructure. Expert Comment.

[22] Proto. 2025. National Bank of Rwanda Automates Consumer Protection Across 600 Financial Institutions. Case Study.

3.3 Local languages – voice AI for higher female usage

In high-exclusion environments – characterised by low literacy, shared device usage, limited smartphone access and emotionally stressed speech from recent scam victims – text-based and form-driven redress systems are structurally exclusionary. This is compounded by a growing divide in large language model performance between developed economies and LMICs, where local languages accuracy lags behind due to a lack of AI compute and training data.[23] Bidirectional voice AI (automatic speech recognition and text-to-speech) should be trained on target-language data at a minimum of 50 hours per language, enabling handling of dialectal variation, informal phrasing, code-switching, and the specific linguistic patterns of distressed complainants. For example, Canada's ScaleAI programme funded a Proto-led consortium to train on 200 hours of Tagalog, Cebuano, Kinyarwanda and Oshiwambo, establishing the model architecture and training pipeline for redressal deployments.[24]

Baseline word error rates in comparable low-resource language deployments should aim for 10–15% under clean conditions and 15–30% in noisy environments prior to fine-tuning. Following fine-tuning on domain-specific grievance data, error rates should reduce substantially and the system's ability to extract key case parameters – transaction reference, amount, institution, date, and scam typology – should reach production-level accuracy. Where feasible, voice intake should be treated as the most effective lever for female complainant participation in the redress system.

3.4 Auto-routing to FSPs and monitored resolution

Once a citizen narrative is captured, the AI agent applies routing logic to identify the responsible institution. In a multi-agency environment – where a single scam may involve a sending bank, a receiving mobile money operator, a payment switch, a financial regulator and a police financial-intelligence unit – static routing rules are insufficient. The routing logic should therefore be AI-driven, trained on regulatory mandates, case typologies, and institutional SLA agreements. Resolution is then monitored continuously: response times are logged and escalation thresholds and SLAs are enforced.

The Philippines deployment of the *BSP Online Buddy (BOB)* AI agent with an 89% automation rate demonstrated that complaints escalated through the central bank AI agent resolve within days rather than months, with documented cases of refunds secured within one week following months of failure through financial institution channels.[25]

3.5 AI-based mediation suggestions

Where a case cannot be resolved through automated referral – typically where an institution disputes liability, the consumer's account of events conflicts with transaction records, or partial

[23] Hussen, K. Y., Sewunetie, W. T., Ayele, A. A., et al. (2025, June). The State of Large Language Models for African Languages: Progress and Challenges. arXiv.
[24] Proto. 2025. Proto Delivers Voice AI for Underserved Languages with Canada's ScaleAI Funding.
[25] Proto. 2025. 89% Automation of Financial Consumer Protection Interactions in the Philippines. Case Study.

recovery has occurred – the redress system should provide a three-party mediation involving the consumer, the institution and a regulator-supervised AI mediator. The AI mediation tools should review the case record, surface relevant regulatory obligations and precedent decisions, and propose a mediation outcome within a defined response-time SLA. This mediation can also be a revenue-generating service for central banks and payment switches where appropriate.

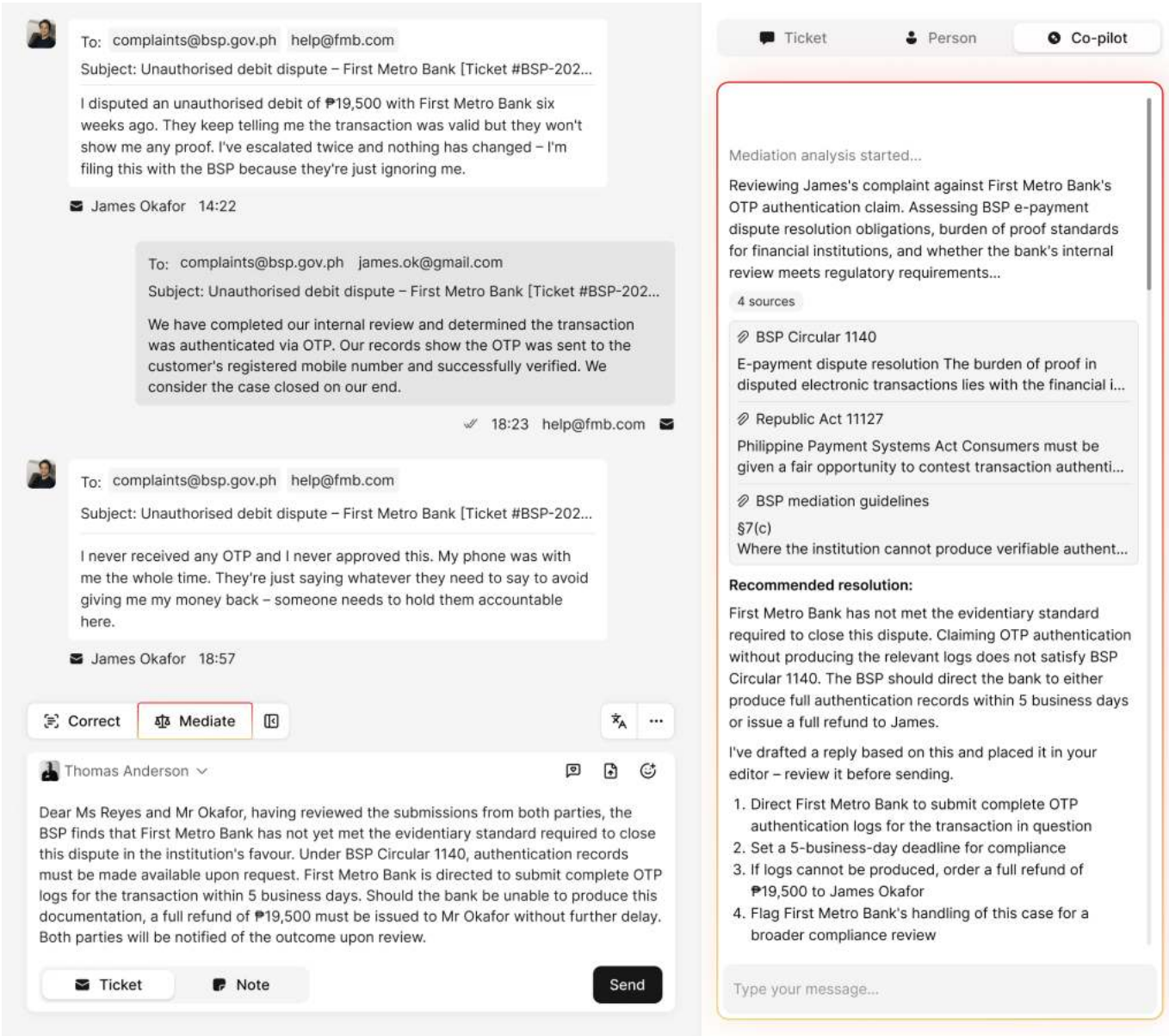


Figure 3 – An AI-mediation suggestion within the Proto *Inbox* interface for supervisors, trained on case law.

3.6 Escalation of scam reports to track-and-trace

Scam reports should be tagged at intake and routed automatically to the Trust Layer's track-and-trace system. This handover is the bridge between the redress and recovery functions: the case record produced by the AI agent at intake contains the originating transaction reference, the reported amount, the institution and the typology classification – the inputs required to begin

cross-institution fund reconstruction. The handover is governed by a delegated administrative authority that allows a national anti-scam utility to initiate the fund freezing workflow without waiting for individual judicial confirmation.

Recovery – targeting >20% fund return

Fund recovery in instant payment fraud is a time-critical operation. Evidence from leading anti-scam utilities in Singapore and Malaysia indicates that the probability of successful recovery drops precipitously after 24 hours. The Trust Layer is designed to compress the institutional response from the norm – measured in days or weeks – to under two hours.

3.7 Real-time, cross-institution tracing

FNA's *Money Trails* is the core reconstruction engine in the recovery system. Upon receipt of an escalated scam report, the engine automatically reconstructs the full payment chain across all participating institutions and payment rails using network graph analysis to identify mule accounts that received funds derived from the reported transaction. The system then updates the money trails in near real-time as new transactions occur and scores each account and transaction node using mule detection models trained on historical fraud patterns, behavioural metadata, and peer network signals. These models operate across institutions simultaneously – an essential capability in markets where scam proceeds routinely traverse four to seven institutions before reaching a withdrawal point. The output is a scored intervention list: accounts where funds remain recoverable, ordered by urgency and institutional jurisdiction, with automatically-calculated maximum freeze amounts and supporting documentation for financial institutions.

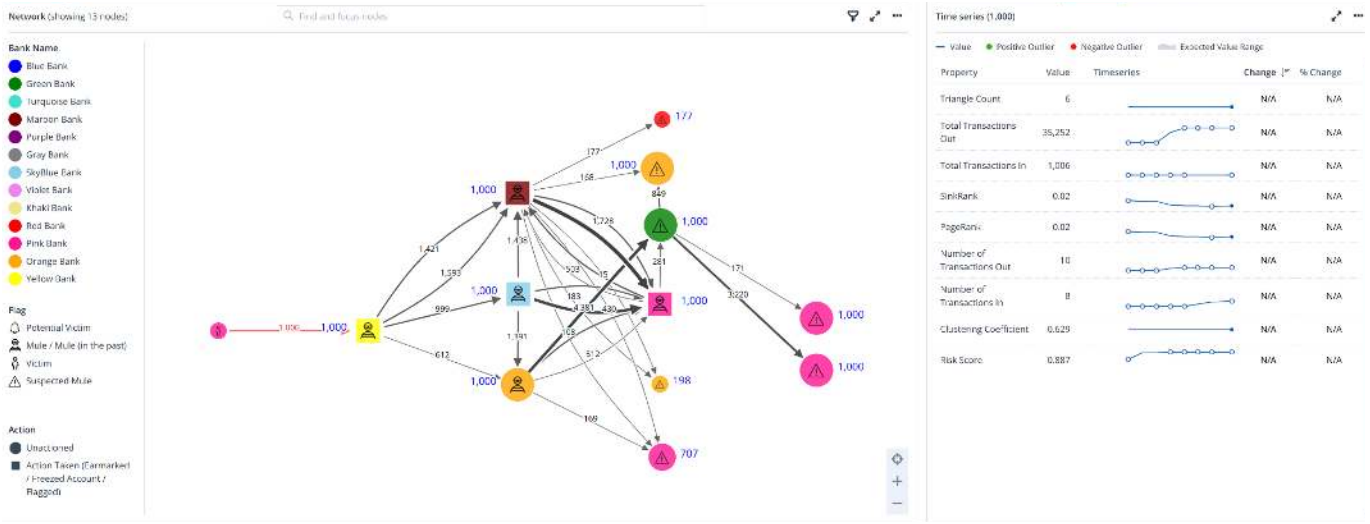


Figure 5 – The FNA *Money Trails* interface showing real-time movement of fraudulent funds.

3.8 Mule account freezing

Freeze authority varies substantially across jurisdictions. The optimal model – exemplified by Malaysia's National Scam Response Centre – delegates a time-limited administrative freeze authority (typically 24–72 hours) directly to the anti-scam utility, allowing accounts to be suspended while judicial confirmation is sought in parallel. This blueprint recommends a 30-day initial freeze limit to allow quality investigation, reducing to 14 days after one year of operational workflow automation. Where delegated freeze authority does not exist, the recovery system generates pre-formatted legal documentation – police holding notices, regulatory directives or institution-specific internal freeze protocols – that reduce the time from case identification to freeze initiation. For each LMIC jurisdiction, this blueprint recommends a central bank directive authorising freeze actions within the anti-scam utility framework, pending enabling legislation, and drawing on the model used by the Nigerian Central Bank's 2025 draft APP guidelines.[26]

3.9 Victim fund return and KYC verification

The final stage in the recovery system is the return of recovered funds to verified victims. KYC verification of claimants is performed through integration with national credit bureaux and identity verification platforms – for example, TransUnion in a potential Namibia deployment[27] – ensuring that funds are returned to the documented victim rather than to a second-stage scammer presenting a fraudulent claim. The system generates an indemnity letter template and escrow instruction for the returning institution, closing the case record with a recovery confirmation and the amount returned.

3.10 Recovery performance targets

The operational effectiveness of the anti-scam utility is evaluated through six headline key performance indicators (KPIs) designed to ensure transparency, accountability, and the prioritisation of vulnerable segments within the digital public infrastructure. These metrics provide a real-time assessment of the trust layer's ability to match the velocity of criminal networks while maintaining low barriers to entry for citizens.

- **Reporting Rate.** This metric tracks the number of cases per 10,000 adult population per month. To identify structural exclusion, data is disaggregated by income tier, gender, geography, and language, ensuring that the redress system is accessible to low-literacy and non-English speaking populations.
- **Automated Resolution Rate.** This measures the share of grievances resolved through AI-mediated intake and auto-routing without requiring human case officer intervention, aiming for high efficiency in high-volume, low-complexity disputes.

[26] Central Bank of Nigeria (2025). Exposure Draft of the Guidelines for Handling Authorised Push Payment Fraud.

[27] TransUnion Namibia (2024). Consumer Fraud Exposure Study, op. cit.

- **Response Time.** Defined as the median time elapsed from a victim's initial report to the execution of the first trace and freeze action. Compressing this window is critical to successful fund recovery before funds are withdrawn by criminal actors.
- **Twenty-Four (24) Hour Recovery Rate.** This KPI monitors the percentage of fraudulent funds successfully intercepted and frozen within the first day of reporting, providing a direct measure of the recovery system's technical performance.
- **Female Complainant Share.** By monitoring the proportion of women accessing the system, the Centre can evaluate the success of voice-first AI and zero-rated channels in overcoming gender-based barriers to redress.
- **Unit Cost Per Resolved Case.** This ensures long-term sustainability by tracking total operating costs against resolutions, supporting the transition to the liability waterfall model.

Instant payment integration

The instant payment system is the third component of the Trust Layer. Unlike the redress and recovery systems, which operate at the case level, the instant payment system operates at the transaction level – providing real-time enrichment to the other layers and maintaining the liability waterfall that determines which institution bears recovery costs in each case category.

3.11 Role of the IPS in the Trust Layer

IPS integration enables two distinct enrichment functions. First, real-time transaction metadata – sender and receiver identifiers, amounts, timestamps, and routing paths – is made available to the recovery system, providing the data substrate for fund tracing without requiring individual banks to build bespoke APIs. Second, fraud scores generated by transaction-scoring models are federated back into the payment switch's risk engine, enabling pre-emptive intervention – holds or delayed settlement – on high-risk payments before they are executed.

3.12 Hybrid data sovereignty

The primary implementation challenge for IPS integrations is not technical but organisational: persuading multiple financial institutions, each with its own compliance and legal teams, to share transaction data with a centralised system in real time. The blueprint's recommended architecture addresses this through a hybrid operating model in which each institution retains data sovereignty, contributing only normalised fraud signals and case-specific metadata rather than raw transaction data.[28] This federated approach allows the recovery system to construct accurate fund traces without exposing individual customer records to the central platform, and is the operationally and politically resilient configuration for LMIC contexts where centralisation concerns are acute.

[28] FNA (2025). A Blueprint for Building National Anti-Scam Utilities. FNA. Confidential.

04 Stakeholder Strategy

This blueprint determines that successful Trust Layer implementation relies on a coherent combination of complementary substantive and procedural instruments.[29] The involvement of stakeholders through these instruments should be sequenced over time, and tailored to the political realities of each LMIC jurisdiction. Research on the interaction between policy innovation and instruments provides the theoretical grammar for this stakeholder engagement plan.[30]

Phased stakeholder engagement

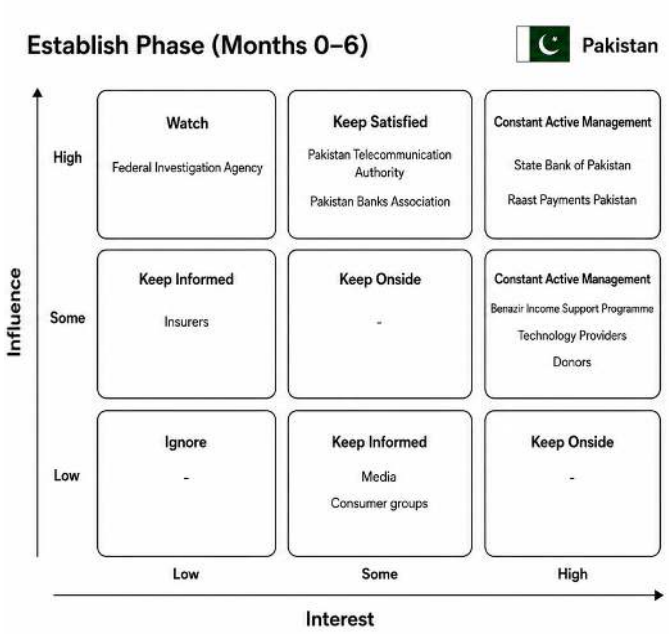
- **Establish (months 0–6).** Move fast with the smallest coalition to organise and issue authority.
  - **Include** the IPS operator, the implementing technology partners & donors, and the social-protection programme (if G2P is relevant).
  - **Consult** the bankers' association (framing the liability waterfall as shared cost reduction, not a new obligation), telco regulator, and the financial supervisor.
  - **Defer** law enforcement, telcos, insurers, civil society, and consumer groups.
- **Scale (months 6–18).** Widen the coalition as performance KPIs become defensible publicly.
  - **Bring in** the telco regulator (for zero-rated IVR and SMS access), the telcos themselves for scam-vector reporting obligations, the bankers' association (to pre-fund the scheme protection pool), and civil society and media (to align on public awareness campaigns).
  - **Activate** the public performance dashboard to create a reputational incentive for sustained financial institution participation, and surface disaggregated KPIs by income and gender.
  - **Continue to defer** law enforcement, primary legislation (the central bank directive is sufficient through month 18), and bankers' association proposals that dilute central bank authority.
- **Sustain (month 18+).** Transition from a sponsored project to permanent governance.
  - **Bring in** standing advisory roles for the bankers' association, insurers, civil society and law enforcement, with no operational veto over freeze, routing or refund decisions.
  - **Promote to permanent governance** the central bank (chair), IPS operator(s), financial supervisor, telco regulator, and social-protection programme.
  - **Codify** primary legislation replacing the central bank directive, the liability waterfall matrix in the IPS participation agreements, and the scheme protection pool levy.

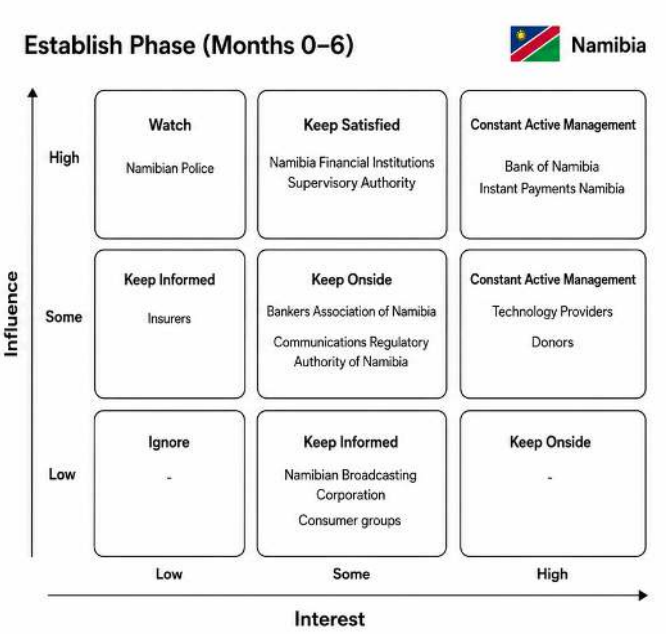
[29] Howlett, M., & Rayner, J. (2007). Design Principles for Policy Mixes: Cohesion and Coherence in 'New Governance Arrangements'. Policy and Society, 26(4), 1–18.

[30] Howlett, M., Mukherjee, I., & Rayner, J. (2018). The Innovation Policy Mix and Instrument Interaction: A Review. Innovation Policy Studies, OECD/Cambridge.

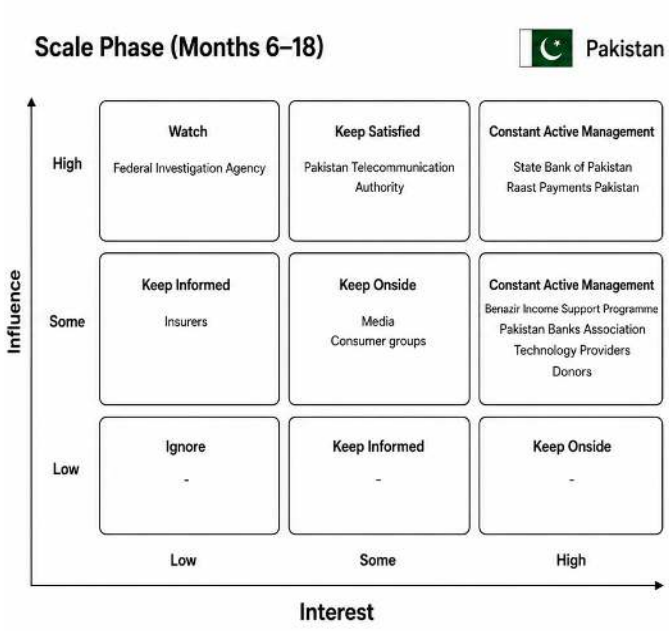
This sequencing and stakeholder positioning can be explained generally in the country cases for Pakistan and Namibia. The following influence-interest maps are intended to be read in parallel: Pakistan demonstrates the complex environment in which the central bank's authority must be exercised through the Raast instant payment system and BISP social-protection programme; Namibia demonstrates the simpler environment with a to-be-launched instant payment system.

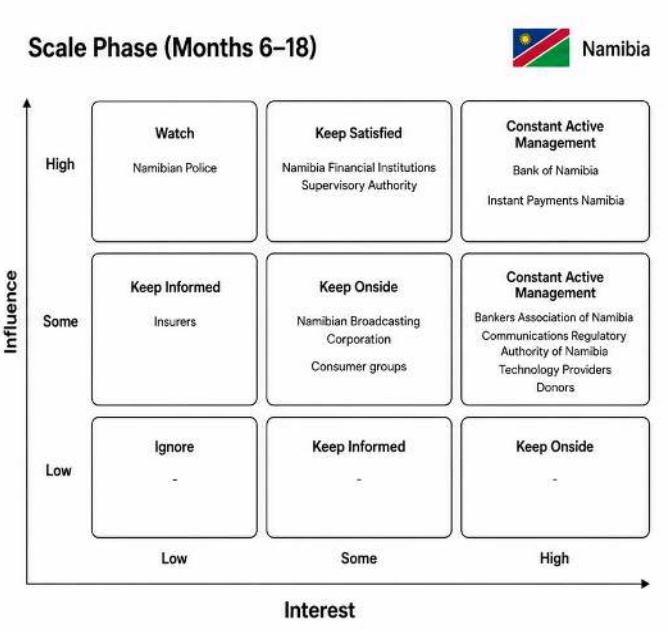
4.1 Establish (months 0-6)



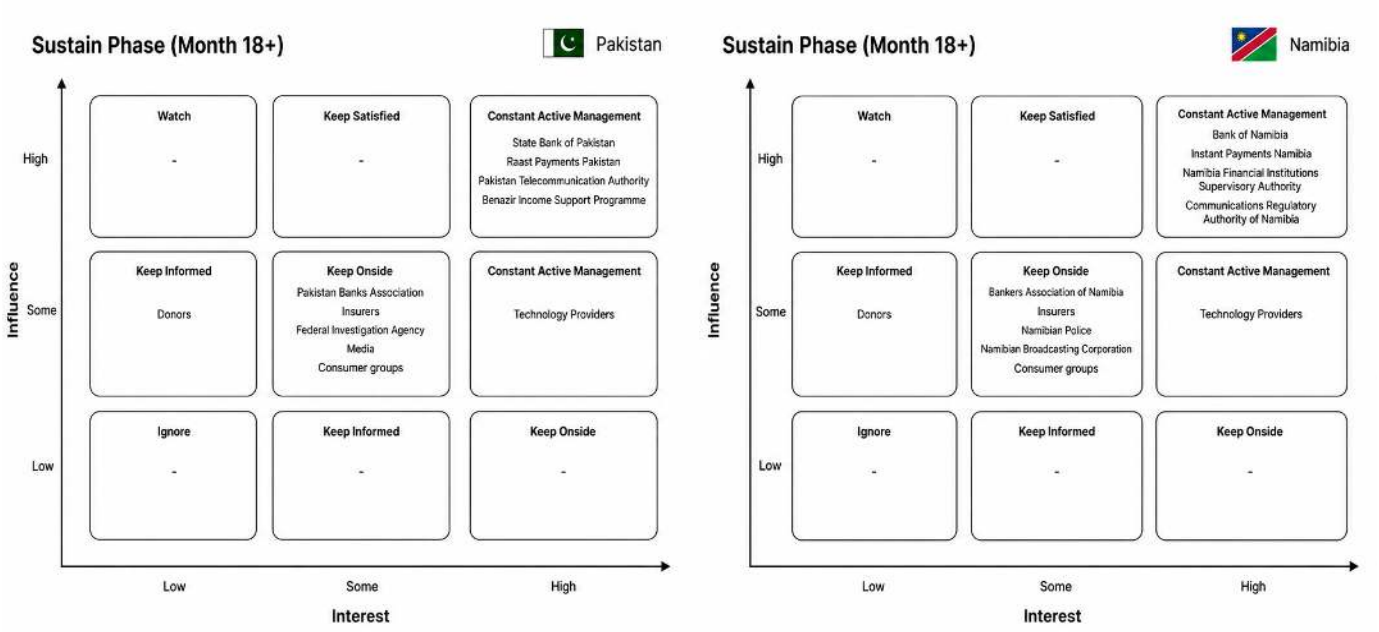


4.2 Scale (months 6-18)





4.3 Sustain (month 18+)



Patterns to avoid and embrace

Two policy models recur in LMIC anti-scam utility establishment discussions and should be explicitly avoided. Both reinvent the wheel in ways that compromise the recovery curve and the consumer protection prioritisation within long-term sustainability.

Anti-pattern 1 – Police-centric architectures

Anti-scam utilities located organisationally within law-enforcement agencies – common in Latin America and parts of Asia – tend to inherit the operational tempo and political-economy constraints of the host institution. Where law-enforcement freeze authority is gated by judicial confirmation that takes more than 24 hours to obtain, the recovery curve is structurally limited; where corruption is perceived, victim reporting drops; where prosecutorial mandates dominate, the consumer-redress function is systematically deprioritised.

RUSI's analysis notes this political-economy risk explicitly[31] and CGAP's research on consumer protection failures in digital finance underscore this risk.[32] This blueprint's recommendation is that law enforcement receive structured case logs for investigation rather than holding structural veto power in the Trusty Layer's implementation. The central bank directive and indemnity letter should delegate authority for fund freezing to the anti-scam utility (see Instrument Two).

[31] RUSI CFS (2026), Authorised Payment Fraud, op. cit., Enabler 1.2 (Anti-Corruption).
[32] CGAP (2023). Survey on the Risks Associated with the Use of Digital Financial Services.

Anti-pattern 2 – Abdication of design to the bankers' association

Several LMIC contexts have, in the absence of clear central bank ownership, defaulted to bankers' association-led models in which the industry designs and/or collectively operates the redress and/or recovery function. These models systematically under-protect non-bank consumers (mobile money and EMI users), generate adversarial compliance dynamics for long-term sustainability planning, and offer no precedent mechanism for subsidising the social-protection tier of consumers. This pattern also rarely survives leadership change at the host association. This blueprint instead anchors authority with the central bank and relies on the bankers' association for consultation, not design and establishment.

The recommended pattern for LMICs – IPS operation and donor-backed technology

A highly-effective pattern in LMIC contexts is a coalition of the following stakeholders to quickly establish, scale, and sustain the Trust Layer:

- **Central bank leadership.** Strong central bank control of redress and fund recovery system design, and issuance of a directive (see Instrument Two) to establish anti-scam utility authority without waiting for primary legislation as consumer trust erodes.
- **Instant payment system operation.** Integration of the redress and recovery systems with the instant payment operator through APIs (see Instrument Five) under a hybrid data sovereignty model. The IPS operator may also house the scheme protection pool.
- **Technology partners & donors.** Leverage redress and recovery technology partners operating in LMICs, who can facilitate time-bound donor support for implementations to avoid *reinvention of the wheel* and initial budget blockers. Such projects should be structured in a project charter with a steering committee of the key stakeholders (see Instrument Three).

☑ **Strategic use of sponsorship**

LMICs with instant payment ecosystems and verifiable and/or urgent consumer harms may be eligible for consumer protection funding from various philanthropic and bilateral donors focused on protecting advancements in financial inclusion. This funding can be facilitated by validated redress and recovery technology partners in LMICs to derisk local stakeholder alignment and anti-scam utility establishment. However, follow-through on performance reporting, public awareness campaigns, and transition to a sustainability model – such as the liability waterfall – are essential commitments. The project charter provides a template for coordinating and managing such sponsorship projects (see Instrument Three).

10 stakeholder action items

These ten action items are drawn from RUSI's authorised payment fraud research, FNA's pioneering anti-scam utility designs, and Proto's operational experience. Each item is beyond recommendation: it specifies an output, an owner, a deadline, and an instrument (or reference) for implementation.

1	**Issue a central bank directive establishing anti-scam utility authority** ● Output: The directive should establish operational authority for case routing, administrative freeze (initial 30-day, reducing to 14-day after one year), data-sharing under the hybrid operating model, and SLA enforcement against participating financial institutions. ● Owner: Central bank ● Deadline: within 90 days of project charter sign-off ● Instrument: Central Bank Directive (Instrument Two)
2	**Sign a multi-stakeholder project charter aligning the anti-scam utility coalition** ● Output: Signed charter by the central bank, instant payment system, financial supervisor, telecommunications regulator, and donor-backed technology partners. Charter specifies governance structure, dispute-resolution mechanism, data-sharing principles, performance KPIs, and liability waterfall transition. ● Owner: Central bank, with a secretariat held by the grantee for the sponsorship. ● Deadline: within 60 days of project sponsorship ● Instrument: Project Charter (Instrument Three)
3	**Formalise the liability waterfall matrix as a regulatory annex to the IPS participation agreement** ● Output: Specification for each case category: first-pay, second-pay, scheme protection pool contribution rule, consumer protection rule, and dispute resolution sequence. The matrix is published as a regulatory annex and updated based on observed recovery outcomes. ● Owner: Central bank, with the IPS Operator ● Deadline: within 180 days of project charter sign-off ● Instrument: Project Charter (Instrument Three)
4	**Adopt a clear indemnity policy for victim-fund return** ● Output: Indemnity letter used to authorise returning institutions to release frozen funds to verified claimants, the KYC verification standard (national ID + credit bureau cross-check), the dispute-resolution sequence in the event of contested claims, and the regulator's indemnification of returning institutions. ● Owner: Central bank, with financial supervisor as required ● Deadline: within 90 days of project charter sign-off ● Instrument: Central Bank Directive (Instrument Two)

5	**Publish a cross-stakeholder public awareness campaign plan** ● Output: Coordinated public awareness campaign across central bank, telco regulator, social-protection programme, financial institutions, and media. ● Owner: Central bank communications office ● Deadline: within 180 days of project charter sign-off. ● Reference: *United Thailand Against Scammers* campaign.
6	**Adopt an IPS integration checklist for redress and recovery modules** ● Output: APIs required to embed the Trust Layer into the instant payment system, including: transaction enrichment, trace and freeze workflows, and audit logging. ● Owner: IPS Operator, with technology implementers ● Deadline: within 90 days of project charter sign-off ● Instrument: Instant payment APIs (Instrument Five)
7	**Stand up a public quarterly performance dashboard** ● Output: Data disaggregated by income tier, gender, geography and language with the six headline KPIs (reporting rate, automated resolution rate, response time, 24-hour recovery rate, female complainant share, unit cost per resolved case). ● Owner: Central bank ● Deadline: within 12 months of project charter sign-off ● Reference: Rwanda's *Mbaza* public complaints resolution dashboard
8	**Pre-negotiate zero-rated IVR and SMS access with all major telco operators** ● Output: Required to remove cost for low-income consumers to use the system. ● Owner: Telco regulator ● Deadline: within 6 months of project charter sign-off ● Reference: Australia SPF's *telco-obligation* logic
9	**Activate the scheme protection pool through IPS ecosystem levies** ● Output: Pre-funded scheme protection pool that reimburses low-income consumers; funded with a levy on financial institutions, calibrated to volumes. ● Owner: IPS Operator, with central bank authority ● Deadline: within 12 months of project charter sign-off ● Reference: Liability Waterfall Matrix (Instrument Four)
10	**Activate the donor-graduation milestone with a formal handover review** ● Output: The handover review confirms that the Trust Layer is sustainably funded through the liability waterfall model and the scheme protection pool is solvent. ● Owner: Grantee, with central bank participation ● Deadline: within 24 months of project charter sign-off ● Reference: Project Charter (Instrument Three)

05 Liability Waterfall Model

The most persistent failure mode in donor-backed digital financial infrastructure is the absence of a credible transition plan. Systems are launched with philanthropic capital and collapse when that capital expires, leaving governments with a decommissioned service and no institutional memory of how to operate an intervention sustainably. The liability waterfall matrix is the answer to this failure mode for the Trust Layer (see Instrument Four). It defines who pays for redress and recovery in each case category – ensuring that the cost never falls on low-income consumers, while generating sufficient revenue to sustain operations after the sponsorship period ends.

Principles and architecture

1.1 Four foundational principles

The waterfall is constructed on four principles derived from international consumer protection frameworks, the OECD's consumer redress guidelines, and the operational data from anti-scam utility deployments. Each principle constrains the design of every category in the matrix.

1. **Consumer protection first.** Low-income consumers, social-protection beneficiaries, and digitally excluded users never pay for redress or recovery services. Where no institutional payer exists, a pre-funded scheme protection pool absorbs the cost.
2. **Fault-based attribution.** Where an institutional failure contributed to the loss – weak fraud controls, delayed freeze, insufficient KYC at the receiving end – the responsible financial institution bears the recovery cost through invoiced case fees or SLA penalties. This creates a financial incentive for prevention rather than for ex-post remediation.
3. **Donor capital as catalyst.** Philanthropic funding covers the initial twelve to twenty-four months of implementation and operation. Its purpose is to establish operational capacity and demonstrate recovery outcomes, not to create a permanent subsidy. The sustainability model is activated in parallel with the sponsorship period, not after it.
4. **Revenue proportional to success.** Revenue is generated primarily from successful recoveries and mediated refunds, not from access fees or case-lodgement charges. This aligns the financial model with consumer outcomes and avoids the perverse incentive of charging victims for reporting fraud.

1.2 The seventeen-category architecture

The four principles are operationalised through a matrix of seventeen case categories. Each category specifies, in order of seniority, the first-pay institution, the second-pay institution, any further fallback payer, whether a consumer fee can ever apply, and the collection mechanism. Cases are classified on intake by the redress layer and routed through the matrix automatically;

the categorisation is the trigger for the waterfall, not an output of it. Three structural features of the matrix carry most of the design work:

- **Ordering by political sensitivity.** The categories are numbered from the most politically critical (social-protection beneficiary scams at category 1) to the least (corporate cybercrime at category 17). This ordering is a deliberate communication device: the categories that would be most damaging to the financial-inclusion narrative if a consumer were charged sit at the top of the matrix and are the most explicitly protected.
- **Cross-subsidy by design.** Categories that generate fee revenue (15 to 17) are not separate products; they are line items within the same matrix. Revenue from successful recovery of a higher-income consumer scam, an SME invoice fraud, or a corporate business-email compromise directly underwrites the cost of processing protected-category cases. A single five per cent success fee on a one-million-unit recovery in category 15 generates enough revenue to fund the full cost of processing approximately five thousand vulnerable-consumer fraud cases at zero cost to the victim.
- **A scheme protection pool as a backstop.** Where no institutional payer exists for a protected-category case, the scheme protection pool pays. The pool is pre-funded through a small ecosystem levy on participants in the instant payment system, calibrated to transaction volume. The pool is not a charity reserve; it is a capitalised mechanism with an annual solvency review and a defined contribution formula.

Liability tiers and fee collection

2.1 Protected, hybrid, and commercial tiers

In operation, the seventeen categories cluster into three tiers. The tier a case falls into determines not only who pays, but also the language used in public communication, the consent workflow at intake, and the dashboard segmentation used in supervisory reporting.

Tier	Categories	Case types	Operational logic
Protected	**1–4**	Social-protection beneficiary scams; vulnerable consumer scams; government payment disputes; systemic scam campaigns.	No consumer fee ever applies. The scheme protection pool, the originating government agency, or the responsible financial institution carries the cost. Recovery outcomes are publicised to drive reporting rates.
Hybrid	**5–14**	FI operational failures; mule-account exposures; wallet, EMI, and PSP disputes; agent-assisted fraud; failed transfers; mistaken payment; non-delivery; refund refusal; insurance-covered fraud; APP scams with no clear FI fault.	Cost falls on the institution at fault – the originating FI, the receiving FI, the merchant, the insurer, or the agent network operator. Consumer fees apply only in narrow residual cases and only with explicit, documented consent.

Tier	Categories	Case types	Operational logic
Commercial	**15–17**	Higher-income consumer scam recovery; SME invoice and supplier fraud; corporate cybercrime and business-email compromise.	Success fees on recovered funds are the standard collection mechanism. This tier is the principal revenue source that cross-subsidises the protected tier. Pricing can be tiered or default (i.e. 5% of recovered value).

Two design rules govern the boundaries between the tiers. First, eligibility for the protected tier is determined by objective criteria – receipt of social-protection payment, qualification as a vulnerable user, demographic and income indicators – not by self-declaration at intake. Second, movement from the commercial tier to the protected tier is always permitted (a case initially classified as a higher-income recovery that on review turns out to involve a vulnerable claimant is reclassified upward); movement in the opposite direction is not. This asymmetry is intentional and is the operational expression of the consumer protection principle.

2.2 Funding sources and the transition pathway

The liability waterfall model is funded from four distinct streams whose relative contribution shifts deliberately over time. At the conclusion of a sponsored project, success fees are deducted from the social-protection pool or invoiced to at-fault financial institutions and merchants. The accounting and collection function for the fees should be administered by the central bank or the IPS operator. Technology partner licenses can be paid via direct commercial license agreements or as a share on the success fees.

Funding stream	Role in the model	Introduction timing
Donor capital	• Catalyses the launch. • Covers project management, technology partner licences, training, and initial Trust Layer operation. • Designed to retire on a defined schedule.	**Months 1–24**
Scheme protection pool	• Annual levy from each instant payment system participant, calibrated to transaction volume. • Pre-funds the pool and underwrites protected-tier cases where no institutional payer exists. • Success fee is deducted from the pool, where applicable.	**Month 12 onwards**
Fault-based invoices	• Case fees, SLA penalties, and refund recoveries invoiced to the institution at fault in hybrid-tier cases. • Operates as a compliance and remediation mechanism, not as a consumer charge.	**Month 12 onwards**
Commercial success fees	• Percentage success fees on recovered funds in commercial-tier cases. • The principal cross-subsidy that sustains the protected tier once donor capital has been retired.	**Month 18 onwards**

Instrument One | Policy Brief

☑ **Ready to adapt**

Policy professionals may edit this template for executive briefings to secure approval for their redress and recovery implementation projects.

Executive statement

Authorised push payment fraud has become the dominant consumer protection failure mode in instant payment economies, with global losses approaching US$579.4 billion annually and [Country] loses an estimated US$[X.X] billion – [X.X]% of GDP – per year. Existing consumer redress channels are primarily manual and cannot match criminal velocity within the 24-hour window in which fund recovery remains feasible. This policy brief recommends that the [Central Bank and/or Payment Switch] establish a national anti-scam utility as a critical **trust layer** – embedding redress, recovery and instant payment integration under central bank mandate, funded initially through donor-backed technology innovators, and transitioning to a liability waterfall model that never passes cost onto low-income consumers. Three actions can be initiated immediately: an interim central bank policy directive within 90 days, a multi-stakeholder project charter, and deployment of the trust layer into the instant payment ecosystem.

Introduction

Instant payment systems have delivered transformational financial inclusion. [Country] has [X.X] million new financial consumers over the previous decade, and instant payments promise to accelerate government-to-person (G2P) and everyday commerce. But the same rails that accelerate inclusion have become the primary attack surface for transnational scam operators. INTERPOL reports a 54% increase in global fraud-related notices since 2024, and concerningly, criminals are targeting vulnerable consumers in low- and middle-income countries (LMICs).

The policy problem is not the absence of evidence or research, but rather the operational gap between international progress and domestic implementation. In implementing its trust layer, [Country] must not fall into the pattern of reinventing its approach. A generalised blueprint already exists, suitable to LMICs both with active, dual-switch, or early instant payment systems. The financial inclusion gains in [Country] are not irreversible. If current trends continue, consumer trust will be eroded unless a protective system is deployed alongside the payment rails – with a clear central bank mandate, and a **liability waterfall model** that quickly aligns stakeholders and does not pass cost onto the very consumers that the system is designed to protect.

Methodology and results

This brief synthesises evidence from active national deployments, including redress and recovery systems in the Philippines, Rwanda, Namibia, Malaysia, Indonesia, and the UAE. Key results include 89% grievance intake automation in the Philippines, accessible reporting channels through direct integration with 600+ financial institutions in Rwanda, and a 20% fraudulent fund recovery rate in Malaysia. This brief also incorporates policy guidance from RUSI, FATF, OECD, UNDP, and the Aspen Institute, alongside United Nations policy-design theory.

The Trust Layer combines three integrated functions operating under a single central bank mandate:

- **Redress** delivers zero-cost intake through messaging apps, SMS, voice and in-person channels in local languages, with AI-mediated resolution and auto-routing for disputes, and rapid escalation for fraud cases.
- **Recovery** executes real-time cross-institution fund tracking and tracing on payment rails, with fund freeze authority delegated to the anti-scam utility for KYC-verified victim fund return.
- **IPS integration** federates fraud signals under a hybrid data-sovereignty model that preserves data inside each financial institution while enabling redress and recovery workflows.

[Country] may be eligible for initial sponsorship and support through social enterprises and open-source instant payment frameworks, such as FNA, Mojaloop, Proto and Tazama. This 12-24 sponsorship period would allow for design, deployment, monitoring, and sustainability.

The Liability Waterfall Model ensures long-term system operation after sponsorship. The model relies on a 17-category liability determination framework with two non-negotiable properties: (a) low-income and other vulnerable consumers never pay, and (b) no single stakeholder bears a sufficient share of cost so that it may obstruct implementation.

At a 5% success fee on the US$[X] million fee-bearing base, [Country] would generate US$[X] million per year – sufficient to cover full operating costs at steady state, and to fund processing of approximately 5,000 low-income consumer cases for every US$1 million of recovery at zero cost to the victim.

Three patterns to avoid are evidenced by survey across LMIC redress and recovery deployments:

- Police-centric architectures that hit judicial, ethical and institutional bottlenecks, and then fail to meet the 24 hour recovery window;
- Abdication of system design to bankers' associations, which can lead to under-protection of non-bank consumers and an adversarial compliance dynamic for system sustainability; and
- Postponement of redress investment until *after* instant payment are perceived to have scaled, despite the loss curve being steepest in the first 24 months of IPS operation.

Recommendations

The three priority actions for immediate decision are:

1. **Issue a central bank directive within 90 days to establish anti-scam utility authority.** The directive should establish operational authority for money-loss case routing, indemnity for administrative freezes (initial 30-day window, reducing to 14-day after one year of operational maturity), data-sharing under the hybrid operating model, and SLA enforcement against participating financial institutions. This pre-empts the multi-year legislation timeline and creates the institutional foundation on which all subsequent action depends.

   Owner: *Governor's office in coordination with the payment and supervision departments.*

2. **Sign a multi-stakeholder project charter convening the implementing coalition.** Signatories should include the central bank, IPS operator, financial supervisor (if separate from the central bank), telecommunications regulator, social-protection programme agency (if G2P is on instant payment), and the donor-backed technology implementers. The charter binds parties to the implementation's schedule and governance structure, dispute resolution and fraud escalation architecture, data-sharing principles, monitoring KPIs, and sustainability.

   Owner: *Central bank with secretariat held by grantee during the sponsorship period.*

3. **Embed the Trust Layer into IPS participation agreements.** Update or amend, as necessary, the IPS agreement framework to include mandatory payment of defined annual allotments into the scheme protection pool, in addition to terms and conditions governing participants' dispute mediation and recovery success fee obligations under the liability waterfall model.

   Owner: *IPS operator with central bank approval.*

References

1. FATF. 2023. Illicit Financial Flows from Cyber-Enabled Fraud. Paris: FATF.
2. OECD. 2024. Recommendation of the Council on High-Level Principles on Financial Consumer Protection. Paris: OECD.
3. UNDP Global Centre for Technology, Innovation and Sustainable Development. 2025. Anti-Scam Handbook v2.0: Collective Response and Tools to Safeguard Development. Singapore: UNDP.
4. Royal United Services Institute, Centre for Finance and Security. 2026. Authorised Payment Fraud: Approaches to Policy Design and Governance. London: RUSI.
5. Bank Negara Malaysia. 2024. Guidelines on Authorised Push Payment Fraud and the National Fraud Portal. Kuala Lumpur: BNM.

Instrument Two | Central Bank Directive

☑ **Ready to adapt**

Central bank executives may edit this template for the central directive and indemnity letter to be distributed across financial institutions and instant payment participants.

[CENTRAL BANK]

Office of the Governor

DIRECTIVE No. [ ] of [YYYY]

Issued under the [Banking Act / Payment Systems Act / Consumer Protection Mandate]

Establishment and Operation of the

National anti-scam utility

Operational Authority, Administrative Freeze, Data-Sharing, and Service-Level Enforcement

Issued by	The Governor of the [Central Bank]
Effective date	[DD Month YYYY]
Status	Interim policy directive pending enabling legislation
Review date	Twenty-four (24) months from the effective date
Reference	[Central Bank Directive No. /YYYY]
Enclosure	Schedule A – Standard Indemnity Letter for the Return of Recovered Funds

Preamble

WHEREAS the [Central Bank] (hereinafter the "Central Bank") is the public authority responsible for the safety, soundness, and integrity of the national payment system and for the protection of consumers of regulated financial services;

WHEREAS the proliferation of authorised push payment fraud and scam activity over instant payment rails has produced a measurable and material loss of consumer funds, a disproportionate impact on low-income consumers, women, and social-protection beneficiaries, and a corresponding erosion of public trust in digital financial services;

WHEREAS empirical evidence from comparable jurisdictions establishes that the probability of successful fund recovery falls precipitously after twenty-four (24) hours from the originating fraudulent transaction, and that an administrative freeze authority delegated to a national anti-scam utility is the only intervention capable of operating within that window;

WHEREAS the absence of a coordinated national mechanism for citizen redress, cross-institution fund tracing, account freezing, and victim fund return materially impedes the Central Bank in the discharge of its consumer-protection mandate;

WHEREAS the [Financial Supervisor], the [IPS Operator], and the [Telco Regulator] have, by signed Project Charter dated [DD Month YYYY], confirmed their participation in a coordinated multi-stakeholder framework;

NOW THEREFORE, the Central Bank, in exercise of the powers conferred upon it by [the Banking Act / the Payment Systems Act / the Consumer Protection Mandate] and acting in the public interest, hereby issues this Directive.

Article 1 – Definitions and scope

1. In this Directive, unless the context otherwise requires:

(a) **"anti-scam utility"** means the National anti-scam utility established under Article 2 of this Directive, operating as the integrated Agentic Trust Layer comprising a redress system, the recovery system, and the instant payment system integration.

(b) **"Administrative freeze"** means the time-limited suspension of all debit operations on an identified account, issued by the anti-scam utility on behalf of the Central Bank, pending the resolution of a Case.

(c) **"Case"** means a complaint of authorised push payment fraud, scam, mistaken payment, or related conduct received by the anti-scam utility through the redress system.

(d) **"Hybrid operating model"** means the data-sharing arrangement under which each Participant retains sovereignty over its raw customer data and contributes only normalised fraud signals and case-specific metadata to the centralised system.

(e) **"Indemnity Letter"** means the document set out in Schedule A to this Directive, by which the Central Bank indemnifies a Returning Institution against loss arising from the release of frozen funds to a Verified Claimant in accordance with this Directive.

(f) **"Participant"** means any bank, electronic money institution, payment service provider, agent network operator, or other financial institution regulated by the Central Bank or by the [Financial Supervisor] and required to participate in the anti-scam utility under Article 3.

(g) **"Returning Institution"** means the Participant holding the account into which fraudulent funds were received and from which the funds are to be released to the Verified Claimant in accordance with the Indemnity Letter.

(h) **"Verified Claimant"** means a natural or legal person whose identity has been verified in accordance with Article 6 and who has been determined by the anti-scam utility to be the lawful recipient of the recovered funds.

2. This Directive applies to:

(a) All Participants;

(b) The [IPS Operator] and any successor operator of the national instant payment system;

(c) Any agent of a Participant providing services to consumers under the Participant's authority; and

(d) Any technology service provider contracted by the Central Bank to operate any component of the anti-scam utility.

Article 2 – Establishment of the anti-scam utility

1. The Central Bank hereby establishes the National anti-scam utility as a shared national infrastructure for the receipt, routing, tracing, freezing, and resolution of Cases.

2. The anti-scam utility shall comprise three integrated components:

(a) **Redress system** – a multilingual AI agent providing voice and text intake, automated case classification, jurisdiction-aware routing, and online dispute resolution, operated by the Central Bank in coordination with the [Financial Supervisor];

(b) **Recovery system** – a cross-institution fund-tracing, mule-detection, and freeze-workflow engine, operated under the technical operating responsibility of the [IPS Operator]; and

(c) **Instant payment system integration** – the application programming interfaces, transaction-enrichment functions, and audit-logging functions through which the anti-scam utility interoperates with the national instant payment system.

3. The operational ownership and public mandate of the anti-scam utility vest in the Central Bank. The day-to-day operation of each component may be delegated to a contracted technology operator in accordance with the Project Charter referred to in the Preamble.

4. The anti-scam utility shall operate on a twenty-four (24) hour basis, seven (7) days per week, with no scheduled downtime exceeding two (2) consecutive hours during off-peak periods.

Article 3 – Mandatory participation

1. Every Participant is required to connect to the anti-scam utility within sixty (60) days of the effective date of this Directive, or, in the case of an institution licensed after that date, within sixty (60) days of the date of its licence.

2. Each Participant shall designate, in writing to the Central Bank and within thirty (30) days of the effective date:

(a) A senior officer accountable for the institution's compliance with this Directive;

(b) A twenty-four (24) hour operational contact point for the receipt and execution of freeze instructions; and

(c) A technical contact for the integration of institution systems with the anti-scam utility.

3. Failure by a Participant to connect within the period specified in clause 1, or to designate the contacts required under clause 2, constitutes a breach of this Directive and shall be subject to the enforcement provisions of Article 9.

Article 4 – Administrative freeze authority

1. The anti-scam utility is hereby authorised, on behalf of the Central Bank, to issue an administrative freeze in respect of any account identified by the recovery system as having received funds derived from a reported Case.

Initial freeze limit

2. The initial administrative freeze shall be valid for thirty (30) calendar days from the moment of issuance.

3. Twelve (12) months after the effective date of this Directive, the initial freeze limit shall be reduced to fourteen (14) calendar days, on the basis of accumulated operational experience and reduced investigation lead times.

Execution by Participants

4. On receipt of a freeze instruction issued by the anti-scam utility, a Participant shall:

   (a) Effect the freeze in its core banking system within sixty (60) minutes of receipt;

   (b) Confirm execution to the anti-scam utility through the instant payment system integration; and

   (c) Refrain from notifying the account holder of the freeze or of the underlying investigation, unless instructed otherwise by the anti-scam utility.

Extension, lifting, and judicial confirmation

5. The anti-scam utility may extend an administrative freeze by a single further period not exceeding thirty (30) calendar days where:
    (a) The investigation remains active;
    (b) The recovery system continues to identify the account as a credible holding point for recoverable funds; and
    (c) A senior officer of the anti-scam utility certifies the extension in the case record.
6. Where a freeze is required beyond the period authorised under this Article, the anti-scam utility shall refer the matter to the competent judicial authority for confirmation. Pending such confirmation, the freeze shall remain in force.
7. The anti-scam utility shall lift any administrative freeze immediately upon a determination that the account did not receive funds derived from the reported Case, or that the funds have been fully recovered.

Account-holder rights

8. An account holder subject to an administrative freeze under this Article shall have the right to:
    (a) Be informed of the existence of the freeze upon the expiry of the initial period or upon judicial confirmation, whichever is earlier;
    (b) Submit a written representation to the anti-scam utility contesting the freeze, which shall be considered within five (5) business days of receipt; and
    (c) Access the dispute-resolution sequence set out in Article 7.

Article 5 – Data-sharing under the hybrid operating model

1. Each Participant shall share with the anti-scam utility, in real time and through the instant payment system integration:
    (a) Normalised fraud signals and risk scores generated by the Participant's internal fraud-detection systems;
    (b) Case-specific metadata necessary for the conduct of a fund trace, including originating account, receiving account, amount, timestamp, and transaction reference;
    (c) Confirmation of execution of freeze instructions issued under Article 4; and
    (d) Case-resolution outcomes, including the amount and date of any funds returned under the Indemnity Letter.

2. Each Participant retains sovereignty over its raw customer data. Nothing in this Directive requires a Participant to transmit raw customer records to the anti-scam utility except where:
    (a) The Participant is the originating institution and the customer is the Verified Claimant; or
    (b) Disclosure is specifically required by a judicial order or by the [Data Protection Authority].
3. All data shared under this Article is processed by the anti-scam utility solely for the purposes of this Directive and in accordance with the [National Data Protection Law]. Banking secrecy obligations under [the Banking Act] are hereby varied to the extent necessary to give effect to the data-sharing provisions of this Directive.
4. The anti-scam utility shall maintain an audit log of every access to, transmission of, and modification of data under this Article. The audit log shall be retained for a period of seven (7) years and shall be available for inspection by the Central Bank, the [Financial Supervisor], and the [Data Protection Authority].

Article 6 – Victim fund return and KYC verification

1. Frozen funds shall be released to a Verified Claimant only upon completion of the verification procedure set out in this Article and the issuance of the Indemnity Letter in Schedule A.

Verification procedure

2. The anti-scam utility shall verify the identity of every claimant by:
    (a) Confirming the national identity number against the records of the [National Identity Authority];
    (b) Cross-checking the claimant's profile against the records of the [Credit Bureau or equivalent];
    (c) Matching the claimant's account or wallet identifier against the originating transaction recorded in the recovery system; and
    (d) Where the claim is made on behalf of a deceased or incapacitated person, requiring documentary proof of legal authority.

Indemnity and release

3. Once a claimant has been verified under clause 2, the Central Bank shall issue the Indemnity Letter set out in Schedule A to the Returning Institution.

4. On receipt of the duly executed Indemnity Letter, the Returning Institution shall release the recovered funds to the Verified Claimant within two (2) business days, by credit to a nominated account in the Verified Claimant's name.
5. The Returning Institution shall not be required to obtain the consent of the account holder of the frozen account before releasing the funds to the Verified Claimant in accordance with the Indemnity Letter.
6. Where partial recovery has occurred, the Returning Institution shall release the recovered portion in accordance with the procedure in this Article. The unrecovered portion shall be treated in accordance with the liability waterfall set out in the regulatory annex to the instant payment system participation agreement.

Article 7 – Dispute-resolution sequence

1. A dispute arising under this Directive shall be resolved in the following sequence:
   (a) **First stage – anti-scam utility review.** A senior case officer of the anti-scam utility, not previously involved in the Case, shall review the matter within five (5) business days.
   (b) **Second stage – Internal escalation.** Unresolved disputes are escalated to the Head of the anti-scam utility, who shall determine the matter within ten (10) business days.
   (c) **Third stage – Central Bank determination.** Where the dispute concerns the conduct of a Participant or the lawfulness of a freeze or release, the matter is referred to the Consumer Protection Office of the Central Bank, which shall issue a determination within twenty (20) business days.
   (d) **Fourth stage – Judicial review.** A party aggrieved by a determination under stage three may seek judicial review in accordance with the [Administrative Justice Act / equivalent] within the time limits prescribed by that law.
2. Where the dispute concerns the identification of the Verified Claimant or the apportionment of recovered funds between competing claimants, the recovered funds shall remain in the escrow position of the Returning Institution until the dispute is resolved.
3. Where the dispute concerns the conduct of a Participant in respect of a non-bank consumer matter, the dispute shall be referred to the [Financial Supervisor] under the existing market-conduct framework, with the anti-scam utility acting as the case-of-record holder.

Article 8 – Service-level enforcement

1. Each Participant shall comply with the following service-level commitments:

Service event	SLA	Measurement
Acknowledgement of freeze instruction	**Within 15 minutes**	Time from instruction issuance to acknowledgement in the case record
Execution of freeze in core banking system	**Within 60 minutes**	Time from acknowledgement to system confirmation
Sharing of normalised fraud signals	**Real time**	Continuous via the IPS integration
Release of funds following Indemnity Letter	**Within 2 business days**	Time from receipt of Indemnity Letter to credit to claimant account
Response to dispute escalation	**Within 5 business days**	Time from dispute notice to first written response
Quarterly KPI submission	**Within 10 business days of quarter end**	Submission against the six headline KPIs

2. Compliance with the service-level commitments set out in this Article shall be measured by the anti-scam utility on a monthly basis and reported to the Central Bank.
3. The six headline key performance indicators against which the operation of the anti-scam utility shall be measured and publicly reported are:
    (a) Reporting rate (cases per 10,000 adult population per month), disaggregated by income tier, gender, geography, and language;
    (b) Automated resolution rate;
    (c) Response time (median time from victim report to initial trace and freeze action);
    (d) Twenty-four (24) hour recovery rate;
    (e) Female complainant share; and
    (f) Unit cost per resolved case.

Article 9 – Enforcement and penalties

1. A breach of this Directive by a Participant shall be addressed in the following sequence:
    (a) **Written notice.** The Central Bank shall issue a written notice of breach, specifying the conduct and the remediation required.
    (b) **Remediation period.** The Participant shall have twenty (20) business days to remediate the breach and to confirm remediation to the Central Bank in writing.

(c) **Administrative penalty.** Where the breach is not remediated within the period specified, the Central Bank may impose an administrative penalty calibrated to the gravity of the breach and to the size of the Participant, in accordance with the existing penalty regime under [the Banking Act / the Payment Systems Act].

(d) **Licence action.** Repeated or wilful breach may give rise to suspension or revocation of the Participant's licence under the existing supervisory framework.

2. Nothing in this Article limits any other power of the Central Bank or of the [Financial Supervisor] under the existing legal framework.

Commencement, review, and citation

This Directive shall come into force on [DD Month YYYY] and shall be reviewed by the Central Bank no later than twelve (12) months from that date. The review shall consider, at a minimum, the reduction of the initial administrative freeze limit from thirty (30) to fourteen (14) days under Article 4, clause 3. This Directive may be cited as the "[anti-scam utility Directive YYYY]".

Issued under my hand at [City], on this day of [YYYY].

_____

[Full name]
Governor
[Central Bank]

SCHEDULE A

Standard Indemnity Letter for the Return of Recovered Funds

Issued pursuant to Article 6 of the anti-scam utility Directive [YYYY]

[Central Bank]

Office of the Governor

[Street address, City]

[Telephone] | [Email] | [Website]

Our reference: [ASC/IL/YYYY/NNNNNN]
Case reference: [CASE-YYYY-NNNNNN]
Date: [DD Month YYYY]

To: The [Chief Executive Officer / Country Head]

[Name of Returning Institution]

[Street address, City]

For the urgent attention of: The Designated Operational Contact for the anti-scam utility

Subject: Indemnity for the release of frozen funds under Case [CASE-YYYY-NNNNNN]

Dear [Sir / Madam],

This letter is issued by the [Central Bank] (the "Central Bank") under Article 6 of the [anti-scam utility Directive YYYY] (the "Directive") and constitutes the formal indemnity required for the release of recovered funds to the Verified Claimant identified below.

1. Case particulars

Case reference	[CASE-YYYY-NNNNNN]
Date of originating transaction	[DD Month YYYY]
Originating institution	[Name of Originating Participant]
Originating account / wallet	[Masked identifier, last four digits]
Returning Institution	[Name of Returning Institution]
Receiving account / wallet	[Masked identifier, last four digits]
Amount frozen	[Currency and amount in words and figures]
Amount to be released	[Currency and amount in words and figures]

Date of administrative freeze	[DD Month YYYY]
Scam typology	[As classified by the anti-scam utility]

2. Verified Claimant

The anti-scam utility has verified the identity of the claimant in accordance with Article 6, clause 2 of the Directive. The verification record is held in the case file and is summarised as follows:

Full legal name of Verified Claimant	[Full name]
National identity number	[Verified against National Identity Authority records]
Credit bureau cross-check	[Performed on DD Month YYYY – result: confirmed]
Transaction-record match	[Confirmed against the originating transaction]
Authority to claim (if applicable)	[Self-claimant / legal representative documentation reference]
Nominated account for release	[Bank name, account number in the claimant's name]

3. Indemnity

The Central Bank, acting under the authority of Article 6 of the Directive, hereby:

1. **Confirms** that the Verified Claimant identified in paragraph 2 has been verified in accordance with the procedure prescribed in the Directive and is the lawful recipient of the funds described in paragraph 1.
2. **Authorises** the Returning Institution to release the amount described in paragraph 1 to the Verified Claimant's nominated account, within two (2) business days of receipt of this letter.
3. **Indemnifies** the Returning Institution against any direct loss, claim, demand, action, or judgment, together with all reasonable legal costs and expenses, arising out of or in connection with the release of the funds in accordance with this letter. The indemnity covers, in particular, any claim by the account holder of the frozen account contesting the release of the funds.
4. **Confirms** that the Returning Institution is not required to obtain the consent of the account holder of the frozen account before effecting the release contemplated by this letter.
5. **Confirms** that the release of funds under this letter does not constitute, and shall not be treated as, a breach by the Returning Institution of (a) any contractual duty owed to the account holder of the frozen account; (b) any banking secrecy obligation under the [Banking Act]; or (c) any duty of care under the [National Consumer Protection Law], the variation of those duties having been affected by Article 5 and Article 6 of the Directive.

4. Scope and limits of the indemnity

The indemnity granted under paragraph 3 is subject to the following:

- **Compliance with this letter.** The indemnity applies only to a release executed strictly in accordance with the particulars set out in paragraphs 1 and 2 of this letter. Any release in excess of the amount specified, or to any account other than the nominated account, falls outside the indemnity.
- **Good faith.** The indemnity applies only where the Returning Institution acts in good faith and without notice of any fact that would render the release manifestly improper.
- **No fraud by the Returning Institution.** The indemnity does not extend to any loss arising from fraud, wilful default, or gross negligence of the Returning Institution or its employees.
- **Cap.** The aggregate liability of the Central Bank under this indemnity shall not exceed the amount released to the Verified Claimant under paragraph 3 plus reasonable legal expenses.
- **Notice.** The Returning Institution shall notify the anti-scam utility in writing within ten (10) business days of becoming aware of any claim or demand to which this indemnity may relate, and shall co-operate with the Central Bank in the conduct of any such matter.

5. Acknowledgement and execution by the Returning Institution

Please indicate the Returning Institution's acknowledgement and acceptance of this letter by signing in the space provided below and returning a scanned copy to the anti-scam utility at the address shown above. The release of the funds shall be effected within two (2) business days of the date of acknowledgement.

Issued for and on behalf of the Central Bank

Signature: _____ Date: _____

Name: _____ Title: Governor, [Central Bank]

Acknowledged and accepted by the Returning Institution

Signature: _____ Date: _____

Name: _____ Title: _____

Institution: _____ Stamp / Seal: _____

Instrument Three | Project Charter

☑ **Ready to adapt**
Project managers may edit this charter template to align stakeholders within donor-funded redress and fund recovery implementations, and ensure long-term sustainability.

PROJECT CHARTER

Agentic Trust Layer

Redress and fund recovery for digital financial services in [Country]

Lead agency	[Central Bank]
Implementing partners	[Redress Provider] (redress system), [Recovery Provider] (recovery system), [IPS Operator] (IPS integration)
Document version	1.0
Date	[Date]

Purpose of this charter

This Project Charter documents the deployment of the Agentic Trust Layer – an integrated AI agent system for citizen redress and fund recovery in [Country]'s digital public infrastructure and financial services. This charter is signed by the lead agency and implementing partners and replaces any interim understanding governing earlier work. This charter sets out:

- The problem and the case for the Agentic Trust Layer
- The scope, boundaries, governance, and main deliverables
- The implementation roadmap structured around ten stakeholder action items
- The transition pathway from sponsorship to a self-sustaining model

Part I – Project overview

1. Problem statement

Instant payment systems have transformed financial inclusion but have also become the primary attack surface for a global scam industry estimated at USD$579.4 billion in 2025 according to Nasdaq Verafin. Once funds move through a real-time rail, the recovery window closes within twenty-four hours – yet most national redress mechanisms still rely on manual call centres, paper-based complaint routing, and multi-day legal procedures to authorise a freeze. The asymmetry between criminal speed and institutional response is the core vulnerability the Agentic Trust Layer is designed to close. The harm falls disproportionately on the newly banked: low-income consumers, women, social-protection beneficiaries, and digitally excluded users. The Trust Layer addresses this by treating citizen redress and fund recovery as core digital public infrastructure rather than peripheral add-ons activated after trust has already eroded.

2. Baseline

Digital financial services and instant payment

[Country] has deployed an instant payment system and continues to expand digital wallet, mobile money, and government-to-person payment programmes. Adoption is concentrated in working-age and low-income segments, with particular risk to social-protection schemes.

Current redress and recovery posture

Existing complaints management is fragmented across regulators and individual financial institutions. Complaints are predominantly received through manual channels with limited real-time visibility into payment flows, no centralised case routing, and no administrative authority to freeze funds across institutions inside the twenty-four-hour recovery window. There is no shared schema for scam typologies and no public performance dashboard.

3. Justification for the project

Business needs

[Central Bank]'s consumer protection mandate requires a unified system to:

- Receive citizen reports in local languages across voice, SMS, web, and messaging channels at zero cost to the consumer.
- Route cases to the correct regulator and institution automatically and maintain an auditable case trail across organisations throughout dispute resolution.
- For urgent scam cases, escalate, trace, freeze, and return funds within the twenty-four-hour window in which recovery is realistically possible.
- Generate structured intelligence to support supervisory action, prosecution, and policy development.

Expected impact

- Citizen reporting rate increases as voice-first, local-language, zero-cost intake reaches populations excluded by text-based and form-driven systems.
- Median time from victim report to initial trace and freeze action falls from days to minutes.
- Recovery rate – the share of reported funds successfully returned to victims – increases materially in the first year of operation.
- Per-case unit cost falls as the AI agent automates routing and resolution, freeing human case officers for high-complexity matters.
- Supervisory reporting against consumer-protection KPIs is automated through the public performance dashboard.

Strategic alignment

The Agentic Trust Layer aligns with [Country]'s consumer protection and market-conduct objectives, and is consistent with the OECD Good Practice Principles for Public Service Design and Delivery in the Digital Age and with the Financial Action Task Force and INTERPOL guidance on anti-scam operations.

4. Scope of the project

Objectives

- Deploy the redress system – an AI agent for multilingual voice and text intake, automated case classification, jurisdiction-aware routing, and online dispute resolution – under the lead agency's public mandate.
- Deploy the recovery system – cross-institution fund tracing, mule-account detection, and administrative freeze workflow – integrated with the IPS.
- Integrate both systems with the IPS to enable case enrichment and audit logging.
- Activate the liability waterfall and the scheme protection pool, transitioning from donor capital to a self-sustaining funding model within twenty-four months.

Main deliverables

- This signed project charter and a central bank directive establishing operational authority.
- A production-grade Trust Layer comprising the redress system ([Redress Provider]), the recovery system ([Recovery Provider]), and the systems' integration with [IPS Operator].
- Standard operating procedures, training materials, and certification records for case officers across participating institutions.
- A public quarterly performance dashboard reporting on six headline KPIs.
- A solvent scheme protection pool and an approved donor-graduation handover review.

Boundaries

In scope: deployment of the three Trust Layer components (redress, recovery, IPS integration); SOPs and training for participating institutions; the public performance dashboard; and the liability waterfall and scheme protection pool.

Part II – Technical proposal

5. The Agentic Trust Layer

The Agentic Trust Layer is a modular, sovereign-deployable architecture that integrates with existing digital public infrastructure rather than requiring new systems. The three components run in parallel with bidirectional data flows: the redress system feeds case events to the recovery system; the recovery system returns trace and freeze confirmations to the redress system for victim communication; and the IPS integration provides real-time transaction enrichment to both while receiving fraud intelligence for risk scoring.

Component	Technology	Function	Operator
Redress system	Voice AI agent, NLP, online dispute resolution	Citizen reporting, complaint routing, dispute mediation, victim communication	[Redress Provider]
Recovery system	Money Trails, graph AI, mule detection	Cross-institution fund tracing, account freezing, victim fund return	[Recovery Provider]
IPS integration	APIs over the national instant payment rails	Real-time transaction enrichment, federated fraud scoring, waterfall liability tracking	[IPS Operator]

Redress system – design principles

The redress system is the citizen-facing entry point to the Agentic Trust Layer. It is governed by five non-negotiable requirements: intake across channels and local languages; jurisdiction-aware routing to the appropriate regulator and institution; case continuity with auditable trails across organisations; dispute resolution and fund recovery capability linked to the recovery system; and structured data generation that supports institutional learning. The agent's voice AI models should be trained on a minimum of 50 hours of speech per supported language and be designed to operate on feature phones and shared devices at zero cost to the consumer.

Recovery system – design principles

The recovery system ingests validated case records from the redress system and traces the originating transaction across institutions to identify accounts that received fraud proceeds, including through multiple forwarding hops. Each node is scored using mule-detection models trained on historical case data. Administrative freezes are issued under the central bank directive with an initial limit of thirty days, reducing to fourteen days after one year of operational data has been collected. Recovered funds are returned to verified claimants under the indemnity policy described in action item four.

IPS integration – design principles

The IPS integration uses a federated approach in which each financial institution retains sovereignty over its raw customer data, contributing only normalised fraud signals and case-specific metadata to the centralised system. This allows accurate fund tracing without exposing individual customer records to the central platform. Federated fraud scores are returned to the IPS switch to enable pre-emptive intervention – adaptive holds, warning overlays, or delayed settlement – on high-risk payment before they are executed.

Key performance indicators

Six headline KPIs are reported publicly each quarter and form the basis of the donor-graduation review:

- Reporting rate – number of cases received per ten thousand adult population per month, disaggregated by income tier, gender, geography, and language.
- Automated resolution rate – share of cases resolved without human case-officer intervention.
- Response time – median time from victim report to initial trace and freeze action.
- Twenty-four-hour recovery rate – share of reported funds frozen within the recovery window.
- Female complainant share – share of complainants who are women, tracked against gender-disaggregated targeting evidence.
- Unit cost per resolved case – total operating cost divided by resolved cases, segmented by category.

Part III – Implementation plan

6. The ten action items

Implementation is structured around ten action items, each with a defined output, an accountable owner, a deadline expressed in days or months from project charter sign-off, and an associated policy instrument or reference precedent. The action items are sequenced to maintain institutional momentum: the directive, the charter, and the waterfall annex are issued first to establish authority; technical integration and operational onboarding follow; the public dashboard, the scheme protection pool, and the donor-graduation review close the implementation cycle.

#	Action and output	Detail	Owner and deadline
1	**Issue a central bank directive establishing anti-scam utility authority** *Instrument: Central Bank Directive*	The directive establishes operational authority for case routing, administrative freeze (initial 30 days, reducing to 14 days after one year), data-sharing under the hybrid operating model, and SLA enforcement against participating financial institutions.	[Central Bank] **[Date]**

#	Action and output	Detail	Owner and deadline
2	**Sign a multi-stakeholder project charter aligning the anti-scam utility coalition** *Instrument: Project Charter*	Signed charter by the central bank, the instant payment system operator, the financial supervisor, the telecommunications regulator, and the donor-backed technology partners. The charter specifies governance structure, dispute-resolution mechanism, data-sharing principles, performance KPIs, and the liability waterfall transition pathway.	[Central Bank], with the secretariat held by [Redress / Recovery Provider] grantee for the sponsorship period **[Date]**
3	**Formalise the liability waterfall matrix as a regulatory annex to the IPS participation agreement** *Instrument: Liability Waterfall Matrix*	The waterfall matrix specifies, for each of the seventeen case categories: first-pay institution, second-pay institution, scheme protection pool contribution rule, consumer-protection rule, and dispute-resolution sequence. The matrix is published as a regulatory annex and updated annually based on observed recovery outcomes.	[Central Bank], with the [IPS Operator] **[Date]**
4	**Adopt a clear indemnity policy for victim-fund return** *Instrument: Central Bank Directive*	Indemnity letter used to authorise returning institutions to release frozen funds to verified claimants, the KYC verification standard (national ID plus credit bureau cross-check), the dispute-resolution sequence in the event of contested claims, and the regulator's indemnification of returning institutions.	[Central Bank], with the financial supervisor where required **[Date]**
5	**Publish a cross-stakeholder public awareness plan with a quarterly campaign calendar** *Instrument: Communications Plan*	Coordinated messaging across the central bank, the telecommunications regulator, the social-protection programme, financial institutions, and media to promote reporting-rate growth as the primary measurable KPI. Reference precedent: the United Thailand Against Scammers campaign.	[Central Bank] communications office **[Date]**

#	Action and output	Detail	Owner and deadline
6	**Adopt an IPS integration checklist for redress and recovery modules** *Instrument: Instant payment APIs*	Technical integration tasks required to embed the Agentic Trust Layer into the instant payment system, including API specifications for transaction enrichment and case event handover, trace and freeze workflows, and audit logging requirements.	[IPS Operator], with the [Redress / Recovery Provider(s)] **[Date]**
7	**Stand up a public quarterly performance dashboard** *Instrument: Performance dashboard*	Data disaggregated by income tier, gender, geography, and language, with the six headline KPIs: reporting rate, automated resolution rate, response time, 24-hour recovery rate, female complainant share, and unit cost per resolved case. Reference precedent: Rwanda's Mbaza public complaints resolution dashboard.	[Central Bank] **[Date]**
8	**Pre-negotiate zero-rated IVR and SMS access with all major telco operators** *Instrument: Telco zero-rating agreements*	Removes the cost barrier to low-income consumer use of the redress system. All major mobile network operators commit to zero-rating inbound voice and SMS to the Agentic Trust Layer short code or shared number. Reference precedent: Australia SPF telco-obligation logic.	[Telco Regulator] **[Date]**
9	**Activate the scheme protection pool through IPS ecosystem levies** *Instrument: Liability Waterfall Matrix*	Pre-funded scheme protection pool that pays category-one cases where no institutional payer exists; funded through a small ecosystem levy on participating financial institutions, calibrated to transaction volume.	[IPS Operator], with [Central Bank] authority **[Date]**
10	**Activate the donor graduation milestone with a formal handover review** *Instrument: Project Charter*	The handover review confirms that the Agentic Trust Layer is sustainably funded through the liability waterfall model and that the scheme protection pool is solvent. Donor capital is formally retired and the lead agency assumes full operational ownership.	Grantee, with [Central Bank] participation **[Date]**

7. Mapping of action items to implementation work streams

Each action item supports one or more of the ten implementation work streams that structure the deployment timeline. The mapping ensures that no work stream is left unfunded or unowned.

Work stream	Scope in this project	Linked actions
Funding and sustainability	Donor capital catalyses the first 24 months. The liability waterfall, the scheme protection pool, and the IPS ecosystem levy carry costs from month 18 onwards. Donor graduation is reviewed at month 24.	**2, 3, 9, 10**
Legal and regulatory framework	The central bank directive establishes operational authority without waiting for enabling legislation. The indemnity policy authorises returning institutions to release frozen funds.	**1, 4**
Governance and institutional ownership	The lead agency owns the public mandate. The Steering Committee holds strategic and financial decision authority. The waterfall matrix is published as a regulatory annex.	**2, 3**
Stakeholder engagement and buy-in	Phased engagement from anchor (central bank, supervisor) through operationalise (IPS, vendors), broaden (banks, EMIs, PSPs), integrate (telco, law enforcement, foreign regulators), to sustain (all parties).	**2, 5, 8**
Standard operating procedures	Case triage, trace request, freeze authorisation, fund return, and dispute resolution SOPs documented and signed off by each participating institution.	**1, 4, 6**
Technology deployment and configuration	Deployment of the redress system ([Redress Provider]), the recovery system ([Recovery Provider]); data schemas, audit logging, and dashboards configured.	**6, 7**
Launch	Controlled launch with a priority cohort of financial institutions, followed by phased onboarding under the central bank directive.	**1, 2, 5, 6**
AI agent integration	Voice AI agent in supported local languages; AI-powered case classification, jurisdiction-aware routing, mule detection, and federated fraud scoring fed back to the IPS switch.	**6, 7**

Work stream	Scope in this project	Linked actions
Human capability and training	Role-based training for case officers, supervisors, law enforcement liaisons, and regulator dashboard users. Initial simulation-based onboarding, refresher training, and certification.	**1, 6**
Measurement and continuous improvement	Six headline KPIs published quarterly. Typology library, scoring models, and SOPs updated based on confirmed case outcomes and operational reviews.	**5, 7, 10**

8. Indicative timeline

The timeline below is expressed in months from project charter sign-off and is consistent with the deadlines specified in the action items. Quarterly Steering Committee reviews track progress and authorise corrective action where deadlines are at risk.

Period	Milestone	Linked actions
[Date]	Charter sign-off; central bank directive issued (action 1); secretariat constituted	**Actions 1, 2**
[Date]	IPS integration checklist agreed; indemnity policy adopted; vendor mobilisation	**Actions 4, 6**
[Date]	Telco zero-rating secured; communications plan published; first cohort of FIs onboarded	**Actions 5, 8**
[Date]	Liability waterfall regulatory annex published; SOPs signed off across participating institutions	**Action 3**
[Date]	Public performance dashboard live; scheme protection pool activated and pre-funded	**Actions 7, 9**
[Date]	Steady-state operation; commercial cases (categories 15–17) generate cross-subsidy revenue; quarterly KPI publication	**All**
[Date]	Donor graduation review; full operational ownership transitioned to the lead agency	**Action 10**

9. Project team and responsibilities

Organisation names are inserted on signature. The role definitions below are binding regardless of the named individual.

Role	Organisation	Responsibilities
Lead Agency	[Central Bank]	Owns the public mandate; chairs the Steering Committee; issues the central bank directive; authorises the indemnity policy; receives operational ownership at donor graduation.
Counterpart Authority	[Financial Supervisor]	Co-owns non-bank market-conduct matters; contributes sector-specific typologies; participates in dispute-resolution escalation.
Technical Operator	[IPS Operator]	Operates the IPS integration; executes administrative freezes; collects and remits the ecosystem levy to the scheme protection pool.
Counterpart Authority	[Telco Regulator]	Negotiates and enforces zero-rated IVR and SMS access for the Trust Layer short code or shared number.
Project Owner & Steering Committee Member	[Redress Provider]	Implements the redress system; provides the project secretariat during the donor-funded period; coordinates training; reports on KPIs.
Project Owner & Steering Committee Member	[Recovery Provider]	Implements the recovery system; operates the fund-tracing and mule-detection engines; supports federated fraud scoring.
Steering Committee Chair	[Central Bank]	Chairs quarterly Steering Committee meetings; ratifies strategic and financial decisions; signs off the donor-graduation review.
Steering Committee Member	[Donor]	Authorises grant tranches; reviews KPI performance; signs off the donor-graduation handover.

10. Governance

Information use and sharing

Information acquired through the project is treated confidentially. The Steering Committee may produce knowledge products, presentations, and case studies; the lead agency reviews these

before public circulation and may exclude information that should not be disclosed. Sharing of personal or financial data is governed by the applicable national data-protection law and by the data-sharing principles in the liability waterfall matrix.

Applicable laws and regulations

The project operates within national consumer-protection, financial-services, payment-system, electronic-communications, and data-protection legal frameworks. Where the existing legal framework does not yet authorise administrative freezes or cross-institution data sharing, the central bank directive provides interim authority pending enabling legislation.

Steering Committee

The Steering Committee is composed of the central bank (chair), the donor representative, and the project owners. The Steering Committee meets quarterly, ratifies strategic and financial decisions, and signs off each action item against the deadlines in section 6.

11. Dependencies and risks

Lead agency contributions

- Issuance of the central bank directive and the indemnity policy.
- Designation of a named project lead with authority to convene participating institutions.
- Coordination with the financial supervisor and the IPS operator on the regulatory annex.

Technical operator contributions

- API and data schema availability for transaction enrichment and case event handover.
- Collection and remittance of the ecosystem levy to the scheme protection pool.
- Operational execution of administrative freezes within the SLA defined in the directive.

Project owner contributions

- Production-grade deployment of the redress and recovery layers in supported local languages.
- Training and certification of case officers across participating institutions.
- Quarterly KPI reporting to the Steering Committee and to the public dashboard.

Key risks and mitigations

Risk	Likelihood and impact	Mitigation
Delay in central bank directive	Medium likelihood, high impact – blocks freeze authority and SLA enforcement	Charter signature triggers a 90-day directive deadline; Steering Committee tracks progress monthly during the first quarter.
Adversarial compliance by	Medium likelihood, medium impact – slows onboarding	Consultation through the bankers' association; secondment opportunities for

Risk	Likelihood and impact	Mitigation
financial institutions		FI technical staff; framing of participation as shared cost reduction.
Insolvent scheme protection pool	Low likelihood, high impact – protected categories lose coverage	Ecosystem levy calibrated to transaction volume; pool top-up by donor capital during the first 12 months; annual solvency review.
Telco zero-rating not secured	Medium likelihood, medium impact – reduces low-income reporting rate	Telecommunications regulator engaged in the first 60 days
Donor exit before sustainability is achieved	Low likelihood, high impact – system collapses post-donor period	Donor-graduation review embedded as action item 10; sustainability model activated in parallel with the donor period, not after it.

Part IV – Sustainability and donor graduation

12. The liability waterfall

The liability waterfall is the financial architecture that transitions the Trust Layer from donor capital to a self-sustaining model. It is constructed on four principles:

- **Consumer protection first.** Low-income consumers, social-protection beneficiaries, and digitally excluded users never pay for redress or recovery services.
- **Fault-based attribution.** Where institutional failure contributed to the loss, the responsible financial institution bears the recovery cost through invoiced success fees or SLA penalties.
- **Donor capital as catalyst.** Philanthropic funding covers the initial 12 to 24 months; the sustainability model is activated in parallel with the donor period.
- **Revenue proportional to success.** Revenue is generated primarily from successful recoveries and mediated refunds, not from access fees or case lodgement charges.

13. Transition pathway

The transition is structured in three phases, mirrored in the action item deadlines:

Phase	Duration	Mechanism	Key condition
Sponsorship	Months 1–24	Grant funding covers [Redress Provider] implementation, the [Recovery Provider] recovery licence, and zero-cost IVR and SMS access for low-income consumers.	Demonstrable recovery outcomes; cross-agency case routing live; central bank directive in force.

Phase	Duration	Mechanism	Key condition
Hybrid transition	Months 18–36	Participating institutions contribute through an ecosystem levy calibrated to transaction volume; the scheme protection pool is pre-funded; commercial success fees accumulate.	Regulatory annex published; circular mandating FI participation; KPI dashboard live.
Self sustaining	Month 36 onwards	Success fees, ecosystem levies, and commercial recovery cases (categories 15–17) cover operating costs. Donor funding is fully retired.	Social-protection pool solvent on its own revenues; donor-graduation review signed off.

Part V – Charter approval

14. Charter as a working document

This Project Charter is a working document. Refinements may be proposed by the Project Owners and the Steering Committee. Substantial or strategic changes – including modifications to the action item deadlines, the liability waterfall categories, or the donor-graduation criteria – require Steering Committee ratification and re-signature by the lead agency.

15. Signatures

The undersigned acknowledge that they have reviewed this Project Charter and authorise their organisation to participate in the activities described herein.

Lead Agency – [Central Bank]

Signature: _____ Date: _____

Print name: _____ Title: _____

Technical Operator – [IPS Operator]

Signature: _____ Date: _____

Print name: _____ Title: _____

Project Owner – [Redress Provider]

Signature: _____ Date: _____

Print name: _____ Title: _____

Project Owner – [Recovery Provider]

Signature: _____ Date: _____

Print name: _____ Title: _____

Instrument Four | Liability Waterfall Matrix

☑ **Ready to adapt**

Central bank and instant payment system executives may edit this liability waterfall to ensure long-term sustainability of the redress and fund recovery systems across participants.

	Case Type	Who Pays First	Who Pays Second	Who Pays Third	Consumer Pays?	Collection Mechanism	Fee Base
1	Social protection beneficiary scams	Scheme protection pool	Origin FI (if controls failed)	N/A	No	Success fee on recovered funds deducted from scheme protection pool or invoiced to Origin FI	Recovered funds
2	Other vulnerable consumer scams	Scheme protection pool	Origin FI (if fault exists)	N/A	No	Success fee on recovered funds deducted from scheme protection pool or invoiced to Origin FI	Recovered funds
3	Gov't payment dispute	Gov't agency	Scheme protection pool	N/A	No	Success fee on refund invoiced to government agency or deducted from scheme protection pool	Disputed funds
4	Systemic scam campaign	Scheme protection pool	Origin FI (if fault exists)	N/A	No	Success fee on recovered funds deducted from scheme protection pool, or invoiced to Origin FI	Recovered funds
5	Clear FI operational failure	Origin FI	Receiving FI	Scheme protection pool	No	Success fee on recovered funds invoiced to Receiving / Origin FI or deducted from scheme protection pool	Recovered funds

	Case Type	Who Pays First	Who Pays Second	Who Pays Third	Consumer Pays?	Collection Mechanism	Fee Base
6	Mule account / Receiving FI exposure	Receiving FI	Origin FI	Scheme protection pool	No	Success fee on recovered funds invoiced to Receiving / Origin FI or deducted from scheme protection pool	Recovered funds
7	Wallet / EMI / PSP dispute	Origin FI	Sponsor bank, if applicable	Scheme protection pool	No	Participant invoice to EMI/PSP; if sponsored, billing can flow through sponsoring bank	Disputed funds
8	Agent assisted fraud	Origin FI	Agent network operator	Scheme protection pool	No	Success fee on recovered funds, invoiced to Origin FI or agent network operator, or deducted from scheme protection pool	Recovered funds
9	Failed IPS transfer / duplicate debit	Origin FI	Scheme protection pool	N/A	No	Success fee on refund, invoiced to Origin FI or deducted from scheme protection pool	Disputed funds
10	Wrong transfer / mistaken payment	Origin FI	Receiving FI	Consumer only if non vulnerable	Usually no	Success fee on refund, invoiced to origin or receiving FI	Disputed funds
11	Non delivery dispute	Merchant	Receiving FI	Consumer only if voluntary mediation	Usually no	Success fee on refund, invoiced to merchants or receiving FI	Disputed funds
12	Defective service / refund refusal	Merchant	Receiving FI	N/A	Usually no	Success fee on refund, invoiced to merchant or receiving FI	Disputed funds
13	Insurance-covered fraud	Insurer	Origin FI (if controls failed)	Consumer/ business deductible	Usually no	N/A	N/A
14	Authorised push payment scam with no clear FI fault	Scheme protection pool if vulnerable consumer	Success fee for non vulnerable consumes	N/A	Possibly	Success fee from scheme protection pool if vulnerable consumer; success fee from recovered funds with consent if non vulnerable consumer	Recovered funds

	Case Type	Who Pays First	Who Pays Second	Who Pays Third	Consumer Pays?	Collection Mechanism	Fee Base
15	Higher income consumer scam recovery	High income consumer	Scheme protection pool	N/A	Yes, residual only	Success fee from recovered funds	Recovered funds
16	SME invoice / supplier fraud	Business victim	Insurer	Origin FI (if control failure exists)	No	Success fee from recovered funds	Recovered funds
17	Corporate cybercrime	Corporate victim	Insurer	Origin FI (if control failure exists)	No	Success fee from recovered funds	Recover funds

Instrument Five | Instant Payment APIs

#	Endpoint	Method	Purpose	Latency	Rate Limit	Key Fields
Redress system						
1.1	`/v1/cases/intake`	POST	Receive complaint from voice AI/SMS/web; validate & generate case ID	<2s (p99)	1,000/min	case_id, citizen_id_hash, scam_type, transaction_reference, amount, receiving_account_hint, confidence_metadata
1.2	`/v1/cases/{case_id}`	GET	Retrieve case status, recovery trace results, freeze timeline	<500ms	Unlimited (owner); 100/min (analyst)	case_id, status, recovery_trace_summary, freeze_status_timeline, next_milestone
1.3	`/v1/cases/{case_id}/route`	POST	Route case to analyst queue, institution, or recovery engine based on priority	<1s	–	case_id, routing_logic, target_institution_codes, assigned_analyst_id, internal_notes
1.4	`/v1/cases/{case_id}/odr`	POST	Initiate online dispute resolution between citizen & receiving institution	<2s intake; 2-hour institutional SLA	–	case_id, institution_code, dispute_amount, settlement_authority, dispute_timeline_hours
1.5	`/v1/cases/{case_id}/classify`	POST	Submit final case classification (scam type, recovery outcome,	<5s	–	case_id, final_scam_type, recovery_outcome, recovery_amount, primary_institution_code,

#	Endpoint	Method	Purpose	Latency	Rate Limit	Key Fields
			control failures)			institutional_control_failure[], repeat_victim, case_duration_hours
1.6	`/v1/cases/{case_id}/notify`	POST	Send case status update to citizen (SMS/voice callback/email, multi-lingual)	<3s; SMS <30s; voice callback <5min	100k/min	case_id, notification_type, delivery_channels[], message_variables{}
Recovery system						
2.1	`/v1/recovery/trace`	POST	Initiate Money Trails graph analysis; request full cross-institutional transaction trace	<30s (p95)	10,000/min	case_id, originating_transaction_id, originating_amount, sender_institution_code, initial_receiver_account_hash, trace_depth, mule_detection_sensitivity
2.2	`/v1/recovery/trace/{trace_id}`	GET	Retrieve detailed trace results (account chain, risk scores, intervention recommendations ranked by priority & recovery potential)	<500ms	Unlimited	trace_id, status, account_chain[{account_hash, institution_code, balance, risk_score, risk_factors, withdrawal_method}], intervention_recommendations[{rank, account_hash, funds_present, recommended_action, time_to_recovery_risk}]
2.3	`/v1/recovery/freeze`	POST	Initiate account freeze (time-limited administrative hold or legal	<30s order; institution ack <5min	1,000/min	case_id, trace_id, account_hash, institution_code, freeze_amount, freeze_type,

#	Endpoint	Method	Purpose	Latency	Rate Limit	Key Fields
			order) at receiving institution			freeze_duration_hours, legal_justification, freeze_authorization_token
2.4a	/v1/recovery/freeze/{freeze_id}	GET	Retrieve freeze status, remaining duration, institution compliance	<500ms	Unlimited	freeze_id, freeze_status, freeze_expiry_timestamp, hours_remaining, funds_frozen_amount, institution_compliance{}, legal_order_status
2.4b	/v1/recovery/freeze/{freeze_id}/extend	POST	Extend freeze duration (requires legal order or renewed authority)	<5s	–	freeze_id, extension_hours, extension_justification, legal_order_reference
2.5a	/v1/recovery/freeze/{freeze_id}/release	POST	Release freeze (expiry, court order, non-fraud determination)	<10s for release order	–	freeze_id, release_reason, release_authority, release_authorization_token
2.5b	/v1/recovery/fund-return	POST	Initiate fund return to victim (from frozen account or victim fund pool)	<30min initiation; delivery <24h	–	case_id, freeze_id, victim_account_identifier, victim_institution_code, return_amount, return_method, return_narrative
2.6	/v1/recovery/mule-score	POST	Generate composite mule detection risk score for account (used by Money Trails; can be called separately)	<2s (p99)	100k/min	account_hash, institution_code, include_peer_network, peer_network_depth

#	Endpoint	Method	Purpose	Latency	Rate Limit	Key Fields
2.7	`/v1/recovery/legal-document`	POST	Generate standardized legal documentation (freeze order, police hold, regulatory directive, reimbursement warrant) ready for signature	<3s	–	case_id, document_type, jurisdiction, account_hash, institution_code, freeze_amount, freeze_duration_days, template_language
Instant payment system						
3.1	`/v1/ips/transaction-metadata`	POST	IPS operator submits transaction metadata in real-time for enrichment, risk scoring, pre-emptive intervention	<500ms; must not block settlement	No limit (fire & forget)	transaction_id, transaction_timestamp, amount, sender_institution_code, receiver_institution_code, high_value_flag, geographic_anomaly_detected, time_of_day_anomaly_detected, transaction_narrative
3.2	`/v1/ips/fraud-risk-score`	POST	anti-scam utility returns fraud risk scores to IPS for integration into IPS's risk engine (enables pre-settlement overlays, delayed settlement, additional verification)	<5s post-transaction	No limit	transaction_id, fraud_risk_score, fraud_risk_category, scoring_timestamp, score_reason, recommended_ips_action, overlay_message_template_id

#	Endpoint	Method	Purpose	Latency	Rate Limit	Key Fields
3.3	`/v1/ips/verify-account`	GET	Verify account existence & holder name in centralized IPS directory (CoP); supports pre-payment or post-complaint verification	<1s (p99)	1M/min	receiver_account_identifier, receiver_institution_code, receiver_account_holder_name_candidate, query_context
3.4	`/v1/ips/transaction-status`	GET	Query real-time settlement status of transaction within IPS; determine if reversal is still possible	<500ms (p99)	Unlimited	transaction_id → status, status_timestamp, clearing_timestamp, hours_until_irreversible, sender_received_credit, receiver_received_credit
3.5	`/v1/ips/participant-register`	POST	Onboard financial institution to Trust Layer; exchange credentials, establish mutual TLS certs, configure API access	<10s (typically during setup meeting)	–	institution_code, institution_name, contact_email, certificate_signing_request, apis_to_enable[], data_retention_days
3.6	`/v1/ips/incident-report`	POST	Report operational incidents affecting Trust Layer (outage, fraud spike)	<2s acknowledgement	–	incident_type, severity, affected_institutions[], estimated_impact_percentage, description, estimated_resolution_time_minutes

Instrument Six | Theory of Change

☑ **Ready to share**

Policy professionals may share this theory of change framework to align stakeholders and secure approval for their redress and recovery implementation projects.

Stakeholder group

Primary group: Citizens of LMICs harmed by scams over instant payment rails — low-income consumers, social-protection beneficiaries, and women.
Custodians: Central bank, financial supervisor, IPS operator, telco regulator, FIs, donors.

Stakeholder needs

- Free, voice-first, local-language redress at zero cost to the consumer.
- Fund tracing, freeze, and return within the 24-hour recovery window.
- Cross-institution case routing; indemnity for verified-victim fund return.
- Liability allocation that never charges protected consumers.

... will be met because ...

Impact

Long-term change sought:
Financial-inclusion dividend preserved at scale.
Citizen trust in digital financial services sustained, not eroded by scam losses.
Redress and recovery recognised as core digital public infrastructure.

Outcomes

Short-term changes:
- Reporting rate rises with parity by gender, income, geography.
- Median response time falls from days to minutes.
- 24-hour recovery rate rises materially in year one.
- Protected consumers never pay; commercial fees cross-subsidise.
- Self-funding by month 36.

Outputs

Deliverables:
- Operational Trust Layer: redress, recovery, IPS integration.
- Central bank directive.
- Signed multi-stakeholder charter.
- Liability waterfall (17 categories) as regulatory annex.
- Indemnity policy and KYC standard.
- Public KPI dashboard.
- Scheme-protection pool.

Activities

The ten action items:
1. Issue central bank directive.
2. Sign multi-stakeholder charter.
3. Formalise liability waterfall.
4. Adopt indemnity policy.
5. Publish awareness plan.
6. Adopt IPS integration checklist.
7. Stand up KPI dashboard.
8. Secure telco zero-rating.
9. Activate scheme-protection pool.
10. Donor-graduation review.

Inputs

Resources required:
- Donor capital (months 1–24).
- Redress and recovery technology stacks.
- Central bank mandate and convening authority.
- IPS operator infrastructure and APIs.
- Telco zero-rating commitments.
- FI fraud operations staff.
- National ID and credit bureau integration.

... will happen because ...

Preconditions

What must be in place before impact can be achieved:
• Live instant payment system at national scale. • Data-protection law admitting federated fraud-purpose data-sharing. • Functional national ID and credit-bureau infrastructure. • Central bank willing to assert administrative authority pending enabling legislation. • Donor aligned with a defined transition out of philanthropic dependency.

References

Multilateral and international guidance

1. ASEAN. 2026. ASEAN Guide on Anti-Scam Policies and Best Practices. Jakarta: Association of Southeast Asian Nations. https://asean.org/wp-content/uploads/2026/01/ASEAN-Guide-on-Anti-Scam-Policies-and-Best-Practices-090126.pdf
2. Basel Institute on Governance. 2025. Collective Action in Practice: A Game-Changer for Business Integrity. Basel: Basel Institute on Governance. https://baselgovernance.org/publications/collective-action-practice-game-changer-business-integrity
3. Bank for International Settlements. 2024. Cross-Border payment and Fraud: A BIS Innovation Hub Perspective. Basel: BIS. https://www.bis.org/about/bisih/topics/fmis.htm
4. Egmont Group of Financial Intelligence Units. 2024. Operational Guidance on Authorised Payment Fraud. Toronto: Egmont Group.
5. FATF. 2023. Illicit Financial Flows from Cyber-Enabled Fraud. Paris: Financial Action Task Force. https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html
6. FATF. 2026. Cyber-Enabled Fraud: Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks. Paris: FATF. https://www.fatf-gafi.org/en/publications/Methodsandtrends/cyber-enabled-fraud-digitalisation-ml-tf-pf-risks.html
7. FATF, Egmont Group, and INTERPOL. 2023. Illicit Financial Flows from Cyber-Enabled Fraud. Paris: FATF.
8. Financial Stability Board. 2025. Financial Stability Implications of Authorised Payment Fraud. Basel: FSB.
9. Global Anti-Scam Alliance and Feedzai. 2025. Global State of Scams 2025 Report. Amsterdam: GASA. https://www.gasa.org/post/global-scams-on-the-rise-over-half-of-adults-worldwide-report-scam-encounters
10. Global Anti-Scam Alliance. 2026. GASA Knowledge Hub: Regional Scam Briefings. https://gasa.org/knowledge-base
11. INTERPOL. 2026. Global Financial Fraud Threat Assessment, Second Edition. Lyon: INTERPOL. https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat
12. International Monetary Fund and World Bank. 2024. Financial Sector Assessment Program: Consumer Protection Supervision Module. Washington, DC: IMF and World Bank.
13. International Telecommunication Union. 2025. Measuring Digital Development: Facts and Figures 2025. Geneva: ITU. https://www.itu.int/en/ITU-D/Statistics/pages/facts/default.aspx

14. OECD. 2022. Good Practice Principles for Public Service Design and Delivery in the Digital Age. OECD Public Governance Policy Papers No. 23. Paris: OECD Publishing.
15. OECD. 2024. Recommendation of the Council on High-Level Principles on Financial Consumer Protection. Paris: OECD. https://www.oecd.org/finance/financial-education/high-level-principles-on-financial-consumer-protection.htm
16. UNCTAD. 2021. Consumer Trust in the Digital Economy: The Case for Online Dispute Resolution. Geneva: UNCTAD.
17. UNCTAD. 2024. Manual on Consumer Protection in Digital Finance. Geneva: United Nations Conference on Trade and Development.
18. UNDP Global Centre for Technology, Innovation and Sustainable Development. 2025. Anti-Scam Handbook v2.0: Collective Response and Tools to Safeguard Development. Singapore: UNDP. https://www.undp.org/sites/g/files/zskgke326/files/2025-05/undp_anti-scam_handbook_v2.0.pdf
19. UNODC. 2009. Manual on Victimisation Surveys. Vienna: United Nations Office on Drugs and Crime. https://www.unodc.org/documents/data-and-analysis/Crime-statistics/Manual_on_Victimization_surveys_2009_web.pdf
20. UNODC. 2021. Organised Crime Strategy Toolkit for Developing High-Impact Strategies. Vienna: UNODC. https://www.unodc.org/cld/uploads/pdf/Strategies/OC_Strategy_Toolkit_Ebook.pdf
21. UNODC. 2024. Organized Fraud: Issue Paper. Vienna: UNODC. https://www.unodc.org/documents/organized-crime/Publications/IssuePaperFraud-eBook.pdf
22. World Bank. 2024. Financial Consumer Protection and Inclusion: A G20/OECD Toolkit. Washington, DC: World Bank Group.
23. World Bank. 2024. Digital Public Infrastructure: A Framework for Public Goods in the Digital Era. Washington, DC: World Bank Group.
24. World Bank Survey Solutions. n.d. Survey Solutions. https://mysurvey.solutions/en/
25. G20. 2023. High-Level Principles for Digital Financial Inclusion. Cape Town: G20 Global Partnership for Financial Inclusion.
26. G20. 2024. Roadmap for Enhancing Cross-Border Payment. Basel: Financial Stability Board.

National strategies, regulations and frameworks

27. Department of the Treasury, Australia. 2025. Scams Prevention Framework: Protecting Australians from Scams. Commonwealth of Australia. https://treasury.gov.au/publication/p2025-623966
28. Australian Government Attorney-General's Department. 2025. Commonwealth Fraud Prevention Centre: Annual Report. Canberra: Commonwealth of Australia.
29. Bank of England. 2024. Payment Systems Regulator Discussion Paper: Authorised Push Payment Reimbursement. London: Bank of England.

30. Bank of Namibia. 2025. Consumer Protection Framework. Windhoek: Bank of Namibia. https://www.bon.com.na/
31. Bank Negara Malaysia. 2024. Guidelines on Authorised Push Payment Fraud and the National Fraud Portal. Kuala Lumpur: BNM.
32. Central Bank of Nigeria. 2025. Exposure Draft of the Guidelines for Handling Authorised Push Payment Fraud. Abuja: CBN. https://www.cbn.gov.ng/Out/2025/CCD/Exposure%20draft%20of%20the%20Guidelines%20for%20Handling%20Authorised%20Push%20Payment%20Fraud.pdf
33. European Banking Authority. 2024. Guidelines on Fraud Reporting under the Payment Services Directive. Paris: EBA.
34. European Commission. 2026. Payment Services Directive 3 Implementing Standards. Brussels: European Commission.
35. Home Office, United Kingdom. 2026. Fraud Strategy 2026–2029. London: HM Government. https://www.gov.uk/government/publications/fraud-strategy-2026-to-2029
36. Home Office, United Kingdom. 2026. New Disruption Unit Launched in Crackdown on Fraud. London: HM Government. https://www.gov.uk/government/news/new-disruption-unit-launched-in-crackdown-on-fraud
37. Home Office, United Kingdom. 2026. Global Taskforce Launched to Hunt Down Overseas Scammers. https://www.gov.uk/government/news/global-taskforce-launched-to-hunt-down-overseas-scammers
38. Monetary Authority of Singapore. 2024. Guidelines on Shared Responsibility Framework. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework
39. Ministry of Home Affairs, Singapore. 2022. Written Reply to Parliamentary Question on the Anti-Scam Command. https://www.mha.gov.sg/media-room/newsroom/written-reply-to-pq-on-the-agencies-and-organisations-that-have-partnered-the-anti-scam-command-to-raise-awareness-on-scams-and-protect-singaporeans/
40. Reserve Bank of India. 2024. Master Direction on Customer Protection: Limiting Liability of Customers in Unauthorised Electronic Banking Transactions. Mumbai: RBI.
41. Reserve Bank of Australia. 2024. Conformance with payment System (Regulation) Act 1998 – Scam Considerations. Sydney: RBA.
42. Royal Thai Embassy, Taipei. n.d. United Thailand Against Scammers: A National War on Scams. https://thaibiztaiwan.thaiembassy.org/th/content/united-thailand-against-scammers-a-national-war-on
43. Singapore Police Force. 2021. The anti-scam utility: A Collaborative Approach Against Scams. https://www.police.gov.sg/media-hub/police-life/2021/11/the-anti-scam-centre---a-collaborative-approach-against-scams
44. State Bank of Pakistan. 2024. Raast Annual Report 2023–24. Karachi: State Bank of Pakistan. https://www.sbp.org.pk/raast/

45. State Bank of Pakistan. 2025. Consumer Grievance Handling Mechanism Framework. Karachi: SBP.

Policy design, instruments and policy mixes

46. Acciai, Claudia. 2024. Procedural Policy Tools in Theory and Practice. London: Routledge.
47. Bagg, Samuel Ely. 2024. The Dispersion of Power: A Critical Realist Theory of Democracy. Oxford: Oxford University Press.
48. Béland, Daniel, and Michael Howlett. 2016. "How Solutions Chase Problems: Instrument Constituencies in the Policy Process." Governance 29 (3): 393–409.
49. Capano, Giliberto, and Michael Howlett. 2021. "Causal Logics and Mechanisms in Policy Design: How and Why Adopting a Mechanistic Perspective Can Improve Policy Design." Public Policy and Administration 36 (2): 141–162.
50. Cohen, Lawrence E., and Marcus Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." American Sociological Review 44 (4): 588–608.
51. European Union Agency for Law Enforcement Cooperation (OLAF). 2016. Guidelines on National Anti-Fraud Strategies. Brussels: European Commission. https://sfc.ec.europa.eu/sites/default/files/EN-ORI-General%20Guidelines%20on%20National%20Anti-Fraud%20Strategies%20ARES%282016%296943965.pdf
52. Howlett, Michael. 2019. Designing Public Policies: Principles and Instruments, 2nd ed. London: Routledge.
53. Howlett, Michael, and Jeremy Rayner. 2007. "Design Principles for Policy Mixes: Cohesion and Coherence in 'New Governance Arrangements'." Policy and Society 26 (4): 1–18.
54. Howlett, Michael, Ishani Mukherjee, and Jeremy Rayner. 2018. The Innovation Policy Mix and Instrument Interaction: A Review. Innovation Policy Studies. Cambridge: Cambridge University Press.
55. Hood, Christopher. 1983. The Tools of Government. London: Macmillan.
56. Hood, Christopher, and Helen Margetts. 2007. The Tools of Government in the Digital Age. London: Palgrave Macmillan.
57. Linder, Stephen H., and B. Guy Peters. 1989. "Instruments of Government: Perceptions and Contexts." Journal of Public Policy 9 (1): 35–58.
58. Mendelow, Aubrey L. 1991. "Stakeholder Mapping." Proceedings of the 2nd International Conference on Information Systems, Cambridge, MA.
59. Salamon, Lester M. 2002. The Tools of Government: A Guide to the New Governance. Oxford: Oxford University Press.
60. Schneider, Anne, and Helen Ingram. 1993. "Social Construction of Target Populations: Implications for Politics and Policy." American Political Science Review 87 (2): 334–347.
61. Schneider, Anne, and Helen Ingram. 2019. "Social Constructions, Anticipatory Feedback Strategies, and Deceptive Public Policy." Policy Studies Journal 47 (2): 206–236.
62. Tools, Policy and Process (TPP) Methodology Brief. 2026. Identifying Target Populations. Version 2.
63. Tools, Policy and Process (TPP) Methodology Brief. 2026. Screening Possible Instruments. April.

64. Tools, Policy and Process (TPP) Methodology Brief. 2025. Identify and Frame the Policy Issue.
65. Vedung, Evert. 1998. "Policy Instruments: Typologies and Theories." In Carrots, Sticks and Sermons: Policy Instruments and Their Evaluation, edited by Bemelmans-Videc, Rist, and Vedung. New Brunswick, NJ: Transaction Publishers.

Policy research and think-tank reports

66. Aspen Institute Fraud Task Force. 2025. United We Stand: A National Strategy to Prevent Scams. Washington, DC: Aspen Institute. https://static1.squarespace.com/static/671a80aa4a84f2359ce4d360/t/690e1fe9c5c80642162575a5/1762533353206/FraudTFReport_Digital_Final.pdf
67. Button, Mark, et al. 2024. Scoping Study on Fraud Centres: Ghana, India, Nigeria. London: London School of Economics. https://researchonline.lse.ac.uk/id/eprint/126338/1/Fraud-Scoping-Study-for-publication-2024.pdf
68. Carnegie Endowment for International Peace. 2024. Cybercrime, Scams and the Erosion of Trust in Digital Finance. Washington, DC: Carnegie Endowment.
69. CGAP. 2023. Survey on the Risks Associated with the Use of Digital Financial Services, Designed for Financial Authorities. Washington, DC: CGAP. https://www.cgap.org/sites/default/files/2023-09/Survey-Questionnaire-on-DFS-Consumer-Risks.pdf
70. CGAP. 2024. Responsible Digital Finance Ecosystem (RDFE): A Conceptual Framework. Washington, DC: CGAP. https://www.cgap.org/research/publication/responsible-digital-finance-ecosystem-rdfe-conceptual-framework
71. Consumers International. 2025. Building Consumer Resilience in Digital Finance. Research Report. London: Consumers International.
72. Devex. 2025. USAID Restructuring and the Future of Donor-Funded Financial Inclusion. https://www.devex.com/
73. Digital Impact Alliance. 2024. Online Dispute Resolution and Digital Public Infrastructure. Expert Comment. Washington, DC: DIAL.
74. Khidr, Mostafa. 2026. "From Detection to Disruption: Building a Central-Bank-Led National Framework to Combat Fraud and Financial Crime." Speech, UNODC Global Fraud Summit 2026, Vienna.
75. Nortal. 2024. Research: Trust Lacking in Digital Public Services. Industry Research Brief.
76. Royal United Services Institute, Centre for Finance and Security. 2026. Authorised Payment Fraud: Approaches to Policy Design and Governance. London: RUSI. Draft.
77. Wood, Helen, Tom Keatinge, Kayla Ditcham, and Aleksandar Janjeva. 2021. The Silent Threat: The Impact of Fraud on UK National Security. RUSI Occasional Paper. London: RUSI. https://www.rusi.org/explore-our-research/publications/occasional-papers/silent-threat-impact-fraud-uk-national-security

78. Westmore, Kelvin, and Alex Owen. 2025. Following the Fraud: The Role of Money Mules. RUSI Emerging Insights. London: RUSI. https://www.rusi.org/explore-our-research/publications/emerging-insights/following-fraud-role-money-mules

Proto, FNA and joint deployments

79. FNA. 2025. A Blueprint for Building National Anti-Scam Utilities. London: FNA.
80. FNA. 2025. Announcement: FNA to Develop Fraud Portal as a Service. London: FNA.
81. FNA. 2025. Case Study: PayNet Malaysia. London: FNA. https://www.fna.fi
82. FNA. 2025. Money Trails and Fraud Intelligence Sharing – BIS Innovation Hub Analytics Challenge. London: FNA.
83. FNA. 2025. Payment Systems Broadcast Summary #25: FNA and Proto's Joint Anti-Scam Solution.
84. GRID Impact. 2025. Proto Learning Partnership: Phase 3 – UAT Data Analysis. August.
85. Innovations for Poverty Action. 2022. In the Philippines, Chatbots Help Consumer Voices Be Heard by Financial Institutions. https://poverty-action.org/philippines-chatbots-help-consumer-voices-be-heard-financial-institutions
86. Proto. 2025. 89% Automation of Financial Consumer Protection Interactions in the Philippines. Case Study. https://www.proto.cx/case-study/financial-consumer-protection-automation-in-the-philippines
87. Proto. 2025. Bank of Mozambique Deploys Proto's AI Agent to Improve Financial Education and Consumer Protection. https://www.proto.cx/resource/bank-of-mozambique-deploys-protos-ai-agent-to-improve-financial-education-and-consumer-protection
88. Proto. 2025. Proto Delivers Voice AI for Underserved Languages with Canada’s ScaleAI Funding. https://www.proto.cx/resource/proto-delivers-voice-ai-for-underserved-languages-with-canadas-scaleai-funding
89. Proto. 2025. National Bank of Rwanda Automates Consumer Protection Across 600 Financial Institutions. Case Study. https://www.proto.cx/case-study/national-bank-of-rwanda-automates-consumer-protection-across-600-financial-institutions
90. Proto. 2025. Namibia Launches AI Agents for Citizen Support and Complaint Resolution. https://www.proto.cx/resource/namibias-government-to-launch-ai-agents-for-citizen-support-and-complaint-resolution
91. Proto. 2025. Rwanda's Government and Proto Partner to Deploy Integrated AI Citizen Support Agents. https://www.proto.cx/resource/rwandas-government-and-proto-partner-to-deploy-integrated-ai-citizen-support-agents
92. Proto. 2026. Citizen Support and Redress in Digital Public Infrastructure. Whitepaper. June.

93. Proto and FNA. 2025. Proto and FNA Win the G20 TechSprint's Cybercrime and Fraud Solution Award. November.

Open-source DPI infrastructure

94. CMA. 2024. Building the Pakistan Raast System: Technical Reference Architecture. Cape Town: CMA.
95. Mojaloop Foundation. 2024. Open-Source instant payment systems for Financial Inclusion. https://mojaloop.io/
96. Mojaloop Foundation. 2025. Mojaloop Anti-Fraud Service: Reference Implementation and Roadmap. https://mojaloop.io/
97. Tazama Project. 2024. Open-Source Transaction Monitoring for Financial Inclusion. Linux Foundation. https://tazama.org/
98. Tazama Project. 2025. Tazama Quickstart and Reference Implementation. Linux Foundation.

AI, low-resourced languages and digital public infrastructure literature

99. Hussen, Kedir Yassin, Walelign Tewabe Sewunetie, Abinew Ali Ayele, et al. 2025. "The State of Large Language Models for African Languages: Progress and Challenges." arXiv:2506.02280, June 2. https://arxiv.org/abs/2506.02280
100. Tech Policy Press. 2025. No Digital Public Infrastructure Without Redress. https://www.techpolicy.press/no-digital-public-infrastructure-without-redress/
101. Ilves, Luukas, Manuel Kilian, Simone Maria Parazzoli, Tiago C. Peixoto, and Ott Velsberg. 2025. The Agentic State: Rethinking Government for the Era of Agentic AI. Global Government Technology Centre Berlin and The World Bank.
102. World Bank. 2024. AI for Development: Practical Use Cases in Public Service Delivery. Washington, DC: World Bank Group.
103. UNDP. 2025. Voice-First AI for Public Services: The Zambia 'Ask Viamo Anything' Pilot. New York: UNDP.
104. Economist, The. 2025. "Online Scams May Already Be as Big a Scourge as Illegal Drugs." February 6. https://www.economist.com/briefing/2025/02/06/online-scams-may-already-be-as-big-a-scourge-as-illegal-drugs
105. Hellerstein, Erica. 2021. "The Mexican Government Wants to Create a Massive Database with Cell Phone Users' Biometric Data." Coda Story. https://www.codastory.com/surveillance-and-control/mexico-biometric-cell-phone-law/

Country-specific sources and case studies

106. TransUnion Namibia. 2024. Consumer Fraud Exposure Study. Windhoek: TransUnion Namibia.
107. Communications Regulatory Authority of Namibia. 2025. Annual Report on Communications Sector Consumer Protection. Windhoek: CRAN.

108. Namibia Financial Institutions Supervisory Authority. 2025. Financial Sector Consumer Protection Annual Report. Windhoek: NAMFISA.
109. Profit Pakistan Today. 2025. "Pakistan Loses Over $9 Billion to Financial Scams Annually." October. https://profit.pakistantoday.com.pk/
110. 1LINK Pakistan. n.d. About 1LINK. https://www.1link.net.pk/about-us
111. Pakistan Telecommunication Authority. 2025. Annual Telecom Sector Indicators Report. Islamabad: PTA.
112. Benazir Income Support Programme. 2025. BISP Annual Performance Report 2024–25. Islamabad: BISP.
113. Securities and Exchange Commission of Pakistan. 2024. Non-Banking Finance Sector Annual Report. Islamabad: SECP.
114. Reserve Bank of New Zealand. 2024. Payment Systems Resilience and Fraud Reporting Framework. Wellington: RBNZ.
115. Payment Systems Regulator (UK). 2024. "Unmasking How Fraudsters Target UK Consumers in the Digital Age." https://www.psr.org.uk/information-for-consumers/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age/
116. UNODC. 2025. "Victimization Surveys in Latin America: Reliable Data to Strengthen Peace, Justice and Public Trust." https://www.cdeunodc.inegi.org.mx/unodc/index.php/2025/10/22/victimization-surveys-in-latin-america-reliable-data-to-strengthen-peace-justice-and-public-trust/
117. Reuters. 2024. Malaysia Opens National Fraud Portal to Pool Bank Scam Data.
118. South African Reserve Bank. 2025. anti-scam utility Reference Architecture. Pretoria: SARB.
119. CGAP. 2024. Customer Outcomes in Mobile Money: Risks, Recourse and Redress in Sub-Saharan Africa. Washington, DC: CGAP.
120. Cambridge Centre for Alternative Finance. 2024. The Global Alternative Finance Benchmarking Survey. Cambridge: CCAF.

Additional academic and applied references

121. Bradlow, Daniel. 2023. "Consumer Protection in Digital Financial Services." Journal of International Economic Law 26 (3): 421–446.
122. Bossuyt, Jeske, et al. 2024. "Designing Redress for Cross-Border Digital Financial Disputes." Law and Development Review 17 (2): 245–268.
123. Center for Global Development. 2024. Consumer Protection in the Era of Mobile Money. Working Paper. Washington, DC.
124. Demirgüç-Kunt, Asli, Leora Klapper, Dorothe Singer, and Saniya Ansar. 2022. The Global Findex Database 2021: Financial Inclusion, Digital payment, and Resilience in the Age of COVID-19. Washington, DC: World Bank.
125. Dybus, Caroline. 2023. "Authorised Push Payment Fraud and the Limits of Reimbursement." Banking Law Journal 140 (5): 297–322.
126. ITU and World Bank. 2023. Digital Financial Services Glossary. Geneva and Washington, DC.

127. Jenik, Ivo, Schan Duff, and Stefan Staschen. 2023. Open Banking and Inclusive Finance. Washington, DC: CGAP.
128. Kapur, Madhulika. 2024. "Voice AI and Inclusion in Public Services." Information Technology for Development 30 (4): 567–589.
129. Krause, Tim, and Anne Marshall. 2024. "Stakeholder Mapping in Financial Regulation: A Practitioner's Guide." Journal of Financial Regulation and Compliance 32 (2): 234–256.
130. Mader, Philip. 2018. "Contesting Financial Inclusion." Development and Change 49 (2): 461–483.
131. Mas, Ignacio, and Olga Morawczynski. 2009. "Designing Mobile Money Services: Lessons from M-PESA." Innovations: Technology, Governance, Globalization 4 (2): 77–91.
132. OECD. 2024. Behavioural Insights and Financial Consumer Protection. Paris: OECD.
133. Ozili, Peterson K. 2018. "Impact of Digital Finance on Financial Inclusion and Stability." Borsa Istanbul Review 18 (4): 329–340.
134. Suri, Tavneet, and William Jack. 2016. "The Long-Run Poverty and Gender Impacts of Mobile Money." Science 354 (6317): 1288–1292.
135. World Economic Forum. 2024. The Future of Trust in Digital Financial Services. Geneva: WEF.
136. Zetzsche, Dirk, Douglas Arner, and Ross Buckley. 2020. "Decentralised Finance." Journal of Financial Regulation 6 (2): 172–203.