telesign | bics | routemobile

Proximus Global

GLF whitepaper

Evolving trust in the AI era

How AI-powered fraud is eroding trust in digital communications, and how the global telecom ecosystem can restore it.

Executive summary

Trust is now central to the long-term relevance and resilience of the telecom industry. Digital communications remain essential to banking, commerce, public services, and everyday life, but the signals people use to spot whether a message, call, or identity interaction is legitimate are becoming less reliable.

Generative AI changes the nature of fraud. It makes fraudulent content more realistic, easier to personalize, multilingual by default, and scalable at low cost. As a result, the content of communication is no longer a sufficient signal of trust.

For telecoms, this creates both responsibility and opportunity. Networks carry the communications through which fraud is executed, but they also generate context, routing, identity, and behavioral signals that other ecosystem players cannot easily replicate.

This paper outlines four coordinated shifts required to restore trust in the AI era:

- Move from reactive fraud management to AI-native fraud operations.
- Build layered trust architectures that combine strong foundations, contextual controls, and emerging GenAI defenses.
- Strengthen ecosystem accountability through benchmarking, shared standards, and international regulatory alignment.
- Reframe fraud prevention as ecosystem value, where telecom intelligence helps protect banks, enterprises, and end users.

The paper concludes with a practical industry call to action for operators, vendors, regulators, and the GLF.

1. Trust in digital communications today

1.1 From channel confidence to systemic doubt

Digital communications rely on a basic assumption: users must believe that the channel is safe to act. That assumption now faces pressure. Fraud has always existed, but many attacks once contained recognizable warning signs: poor language, generic requests, inconsistent branding, or implausible scenarios.

AI is rapidly eroding these traditional warning signs. When fraudulent communications look and sound legitimate, trust can no longer rely mainly on user intuition or content quality. The ecosystem must move toward trust based on stronger contextual signals: origin, routing, identity consistency, device behaviour, and verified provenance.

1.2 Why operators are at the centre

Telecom networks carry traffic that underpins all critical communications. When telco channels are abused, the impact extends beyond the immediate victim and weakens confidence in the communication itself.

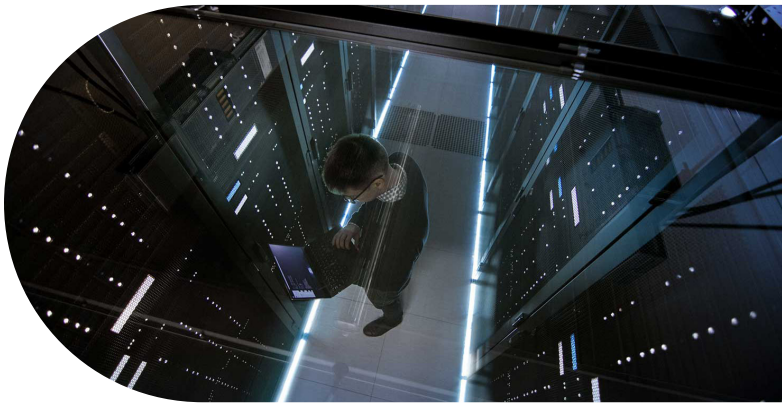
Operators are not responsible for every fraudulent interaction that crosses their networks, but they are uniquely positioned to observe patterns that others cannot see.

This gives telecoms a dual role: safeguarding network integrity and helping the wider digital ecosystem restore confidence in the channels it depends on.

1.3 Where the industry stands

The industry is not starting from zero. Operators use fraud management tools, monitoring processes, intelligence sharing, and industry frameworks. Standardization bodies and codes of conduct have helped define baseline expectations. Yet the level of maturity remains uneven, and many organizations are operationally stretched.

The gap is increasingly operational as much as technical. Tools only create value when there are teams, processes, governance, and escalation paths capable of acting on what those tools detect. These challenges become more pronounced in an AI-driven threat landscape, where speed, scale, and adaptability redefine fraud risk.



2. The AI inflection point

2.1 The end of obvious fraud

AI is turning fraud from something often recognizable into something designed to appear normal. Phishing and smishing messages can be fluent, locally adapted, and personalized. Voice cloning can imitate trusted individuals. AI-assisted scripts can sustain interactive conversations that feel credible.

2.2 Scale, adaptation, and cost asymmetry

AI fundamentally reshapes the economics of fraud. It lowers the skill and effort required to launch credible attacks while increasing the ability to test, adapt, and scale campaigns. Attackers can iterate quickly; defenders face more signals, more ambiguity, and higher response complexity.

This asymmetry is structural. Fraudsters benefit from lower costs and faster experimentation, while operators must invest in stronger detection, better operations, and broader ecosystem coordination. Traditional fraud models based on static rules, periodic tuning, and manual review are increasingly mismatched in this environment.

2.3 The next step: Agentic fraud

The next stage is likely to involve more autonomous fraud operations. AI agents may coordinate steps, adapt messages, interact with victims, and respond to defensive friction with limited human intervention. This is not the dominant threat today, but it is the direction of travel, and it should shape how the industry prepares now.

3. Why the current approach is not sufficient

Current defenses were built for a different threat model. Rule-based systems identify known patterns. Behavioural analytics flag anomalies. Human reviews often rely on visible inconsistencies. AI-enabled fraud is different because it is designed to look legitimate and adapt quickly.

The problem is therefore not simply a tools problem. It is a structural readiness problem. Operators need operating models, vendor accountability, governance, standards, and regulatory alignment that can evolve at the same pace as the threat.

Structural gap	What it means
Operational gap	Detection without response creates false confidence. Many operators have detection tools but lack the operational capacity to act at scale.
Signal gap	Content-level cues are weaker. The industry must rely more on contextual, behavioral, and network-level signals.
Accountability gap	AI claims are widespread, but operators need credible evidence of performance in real telecom fraud scenarios.
Coordination gap	Fraud is inherently cross borders while regulation, standards, and enforcement remain fragmented.

4. Rebuilding trust through operations and architecture

4.1 AI-Native fraud operations

Technology does not prevent fraud on its own. Alerts must be interpreted, cases investigated, decisions made, and actions coordinated. As AI makes fraud more convincing, the human role becomes more crucial , but it must be augmented by better tools and workflows.

An AI-native fraud operation uses AI across the lifecycle of fraud management: signal prioritization, case investigation, pattern discovery, threat intelligence, and knowledge sharing. The aim is not to replace analysts, but to make expert judgments faster and more scalable.

Equip teams with AI-assisted tools that surface relevant signals from high-volume data environments.

Use AI to accelerate investigation, summarize case context, and reduce time from alert to action.

Create structured processes to monitor emerging AI-enabled fraud techniques and translate lessons into control.

Design human-in-the-loop workflows for high-impact decisions, model oversight, and escalation.

4.2 Layered trust architecture

Operators also need a disciplined technical architecture. Advanced AI defenses cannot compensate for weak foundations. Misconfigured systems, incomplete monitoring, or irregular testing undermine every layer above them.

The AI-native fraud detection market is still forming. Operators should test solutions against realistic scenarios and avoid treating AI-labelled features as proof of effectiveness.

4.3 Visible security without excessive friction

Trust is ultimately experienced by users at the point of interaction. Fraud alerts, identity prompts, and confirmation flows can help rebuild confidence when they are clear and proportionate.

> The objective is not to add friction everywhere, but to make security visible at the moments where users need reassurance.

4.4 Feedback-loop learning and simulation

One of the key characteristics that differentiates an AI-native fraud platform from a traditional platform with an AI interface is continuous learning. The system should continuously improve its detection logic based on analyst feedback, whether that is confirming a fraud case, dismissing a false positive, escalating an investigation, or overriding a recommendation. These actions can be fed back into the learning pipeline to refine detection logic, prioritization, and rule tuning over time, allowing the platform to adapt more effectively as fraud patterns evolve rather than relying solely on periodic manual tuning.

This naturally complements the ability to simulate new detection rules, attack scenarios, or emerging fraud patterns before deployment, providing operators with a safe way to validate changes, measure their impact, and accelerate adaptation.

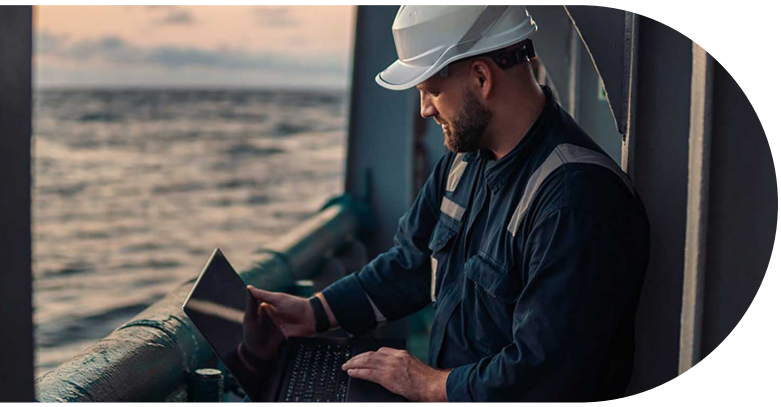
Layer	Purpose	Typical capabilities
Foundation	Establish a reliable security and monitoring baseline.	Correctly configured firewalls; continuous monitoring; alerting; penetration testing; vulnerability management; baseline compliance.
Contextual controls	Assess whether an interaction is consistent with legitimate behavior.	Behavioral analytics; identity verification layers; real-time traffic analysis; visible trust signals.
AI-era defenses	Prepare for fraud generated, adapted, or coordinated by AI.	AI-generated content detection; synthetic media risk analysis; generative red-teaming; human-in-the-loop review.

5. Ecosystem organization: Benchmarking, standards, and regulation

5.1 Vendor accountability

As AI becomes central to fraud prevention, vendor accountability becomes critical. Many solutions now claim AI capabilities, but operators need to understand how those capabilities perform in practice and how their effectiveness is evaluated. Platforms claiming to offer AI-native detection should not automatically be assumed to represent the most innovative or effective approach. In some cases, such claims may reflect the addition of a GenAI interface layered on top of existing detection logic rather than fundamentally new detection capabilities.

Independent, telecom-specific benchmarking can help separate capability claims from demonstrated performance. It can also provide operators with a practical framework to evaluate vendor claims and encourage greater transparency around what AI capabilities actually deliver.



5.2 Standards and international regulatory alignment

Telecom fraud is structurally cross-border. Fraudulent traffic may originate in one jurisdiction, transit through several networks, and target consumers in another market. Regional regulation alone cannot close these gaps.

The industry should support minimum fraud prevention expectations for traffic entering regulated markets, mechanisms for cross-border enforcement and intelligence sharing, and regulatory frameworks that enable responsible collaboration between telcos, financial institutions, and public authorities.

5.3 The role of the GLF

The GLF is well positioned to convene this agenda because international carriers sit at the center of cross-border communications. It can help translate individual operator experience into common principles, strengthen codes of conduct, and engage regulators on the need for coordinated action.

6. Fraud prevention as ecosystem value

6.1 Changing the investment logic

Fraud prevention has often been treated as a cost to be managed. In the AI era, this framing is too narrow. The investment required is increasing, while the benefits of prevention are distributed across banks, enterprises, consumers, and public services.

A more sustainable model is to reposition fraud prevention as ecosystem value. The same capabilities that help operators defend their networks can also help downstream partners reduce fraud and improve digital trust.

6.2 The telco advantage

Operators hold network-level signals that other industries cannot easily replicate: device behavior, number status, routing patterns, traffic characteristics, location consistency, and identity-related indicators. These signals can help financial institutions and digital service providers assess risk in ways they cannot achieve independently.

Responsible signal sharing can support identity verification, transaction risk scoring, suspicious activity alerts, and account protection. National-level collaboration is often the most practical starting point, where data sovereignty, privacy, and regulatory considerations can be managed within a clearer legal framework.

6.3 Funding better defences

Reframing fraud prevention as ecosystem value changes the internal business case. If operators can responsibly monetize fraud intelligence responsibly, they can fund stronger operations, better tooling, and participation in industry initiatives. This is not only a commercial opportunity; it is a mechanism to enable sustained, long-term investment in digital trust.

7. Industry call to action

Restoring trust in the AI era requires coordinated action. The priorities below are deliberately practical and action oriented.

Stakeholder	Priority actions
Operators	Audit baseline security and close foundational gaps. Build AI-native fraud operations and equip analysts with appropriate tools. Define fraud and trust KPIs at leadership level. Explore responsible signal-sharing models with banks and digital platforms.
Vendors	Provide independently verifiable performance evidence. Be transparent about maturity, limitations, and operating assumptions. Support human-in-the-loop workflows and realistic testing.
Regulators	Develop minimum expectations for traffic entering regulated markets. Support international alignment and enforcement cooperation. Enable responsible telco-financial institution collaboration.
The GLF	Coordinate the international carrier position on AI-enabled fraud and trust. Support benchmarking and standards discussions. Strengthen codes of conduct for AI-era fraud scenarios. Engage regulators globally on cross-border alignment.

Conclusion

AI has changed the trust challenge facing digital communications. Fraud is no longer only a question of blocking known patterns or educating users to spot suspicious messages. It is becoming a systemic risk for the communications layer itself.

The telecom industry has a central role because it operates the infrastructure through which digital trust is exercised every day. Restoring that trust will require stronger operations, layered architecture, credible vendor accountability, commercial collaboration, and international alignment.

The opportunity for the GLF is to help the industry move from fragmented fraud prevention to collective trust restoration. In the AI era, trust will be rebuilt by an ecosystem that chooses to act together.

This white paper was developed as an expert-view draft for GLF discussion and welcomes further input from member organizations.