telesign | bics | routemobile

Proximus Global

Fraud has scaled. Have our defences?

BEREC external workshop on combating fraud, 21 May 2026

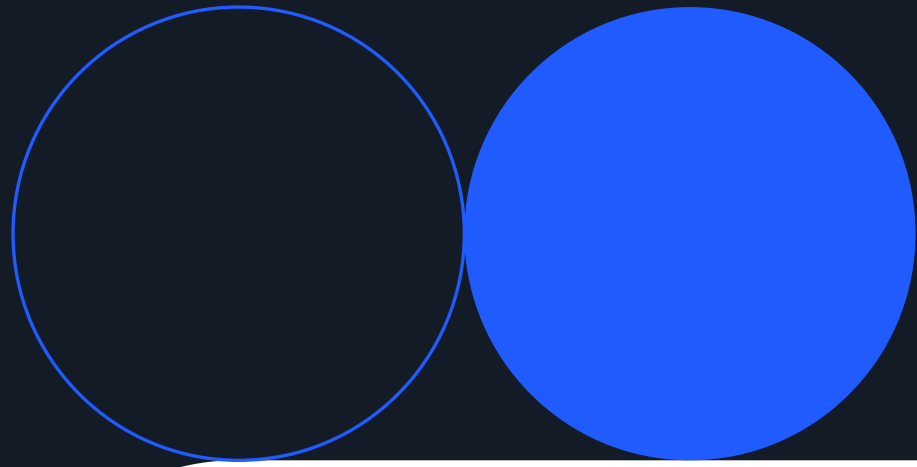
Arturs Alksnis, VP Public Policy, Proximus Global

Fraud is global, organised, and AI-accelerated.

Defence is national, reactive, and human-paced.

Can we get our act together?

1. Context



The scale of the problem in 2026

$442 billion

lost to scams globally in 2025 (GASA Global State of Scams 2025)

57%

of adults worldwide encountered a scam in the past 12 months

23%

of adults lost money to scams

Top channel

Phone calls and SMS remain among the leading attack vectors

Europol IOCTA 2025: "Steal, Deal and Repeat": stolen data underpins a fully commoditised crime-as-a-service market. Technical skills are no longer a barrier to entry.

AI has industrialised impersonation fraud

Deepfakes and voice cloning are no longer the future, they are the current attack tooling

€1.3B+

reported deepfake-linked fraud losses,
€860M in 2025 alone

~$200M

in deepfake fraud losses in Q1 2025 alone

1 in 4 adults

has experienced or knows someone affected by a voice-cloning scam

Example case

Italian luxury and automotive executives were impersonated using cloned voices in coordinated scams. In at least one case, a victim transferred €1 million to a Hong Kong-based account.

2. How we respond

Examples of what Proximus Global is deploying

FraudGuard

BICS' machine-learning-driven anti-fraud platform: voice, SMS, roaming, signaling. 90-95% block rate; award-winning robocall mitigation.

365guard

AI-powered SMS spam & fraud protection (launched April 2025): defending P2P and A2P channels with region-adaptive learning.

Fraud Management Suite with PCI Pal

Telesign × PCI Pal (July 2025): AI-driven detection of card-not-present fraud at the moment of payment.

Recycled Number Fraud Prevention API

With EnStream (Canada): closes the SIM / number-reassignment gap that fuels account takeover.

Network APIs partnership with Nokia

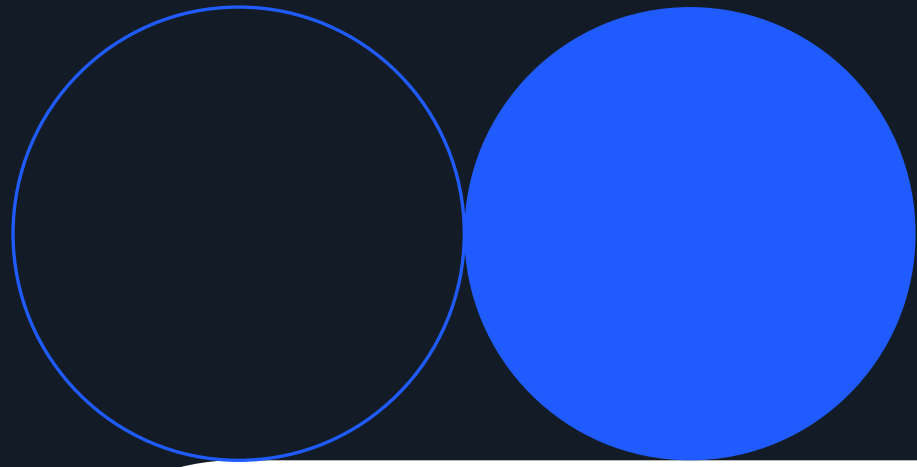
Programmable fraud-prevention signals for the developer ecosystem, anchored in CAMARA.

Telesign Trust Engine

Built on 2,200+ digital identity signals. With ~1 in 3 people globally affected by fraud, identity intelligence is now a core layer of protection.

The tooling is real, deployed, and producing measurable results.
The bottleneck is what the legal framework lets us do with it across borders.

3. Fragmentation



Fragmentation is the fraudster's business model

Local vs. international

National measures work but they stop at the border. Fraud does not. Two-thirds of all fraud losses are tied to international traffic.

Multiplicity of authorities

Telecom, data protection, financial, consumer, law enforcement. Each holds part of the picture; none holds it all.

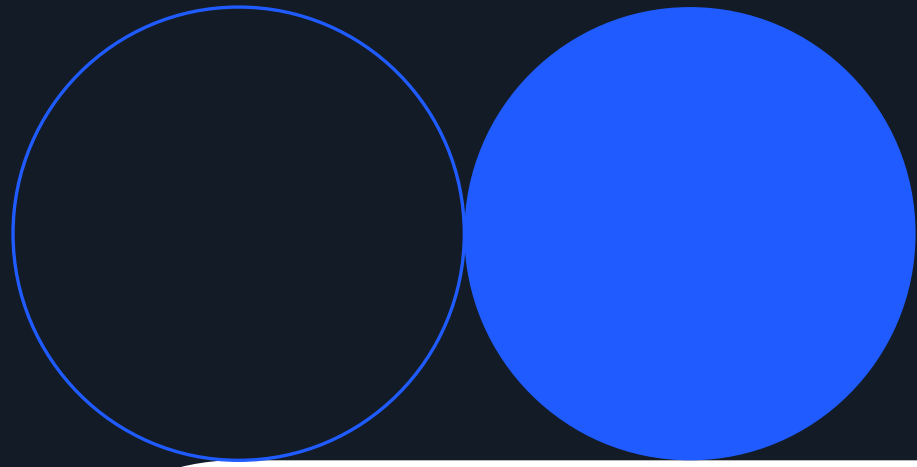
Conflicting obligations

The current framework leaves operators uncertain when they act in good faith to disrupt fraud.

The pace problem

Fraudsters iterate in weeks; rules in years. Europol dismantled 12 scam call centres in 2024, traffic rebounded within two months.

4. What it takes to restore trust?



The ecosystem is already organising

A global, purpose-built initiative to combat fraudulent communications

One Consortium

Industry pillar · hosted by i3Forum

50+ Members

Active workstreams:

- Survey of Industry Landscape
- Survey of Regulatory Initiatives
- International Traceback
- Illegitimate Spoofing
- Messaging

GIRAF

Global Informal Regulatory Anti-Fraud Forum

39 NRAs across 5 continents

Monthly plenary meetings, working groups, joint sessions with One Consortium

How to bridge the gap

A collective commitment and the right regulatory and legislative framework

Global Coordinated Approach

Regulators and industry advancing together.

Regulatory Balance

Privacy and fraud protection are the same objective, not a trade-off. Legal clarity for traffic analysis, signal sharing and cross-border collaboration would make everything else work.

Flexible Regulation

Principles, not prescriptions. Rules that anticipate the next attack technique outlive ones that codify the last one.

Sustainable, Accountable Business

Minimum baseline obligations across the chain (operators, aggregators, OTTs, platforms, banks) so legitimate actors are not undercut by those that look the other way.

The tools exist.

The intelligence exists.

What's missing is permission to use them together.

Ask on our side: cross-border fraud defence should be a clear, named workstream of the EU regulatory framework.

proximus
Global