telesign | bics | routemobile

Proximus Global

What are we missing to beat fraudsters?

Use-case review on Info Sharing to fight fraud

May 2025

Agenda for today

01 Context

02 Traffic-based insights

03 Challenges

04 What next?

01 Context

Telecommunication services play a significant role in facilitating scams and online threats that affect not only end-users and businesses but also the entire ecosystem.

Context

The entire digital and telecommunications ecosystem is **actively seeking enhanced methods to safeguard against and reduce scams and fraudulent activities.**

The industry is focused on **developing technology**, refining processes, and protecting customers, businesses and consumers.

Telecommunications regulators are formulating **national strategies and regulations** aimed at curbing these attacks and ensuring the protection of end-users.

However,
our efforts to combat fraud and
scams appear to be falling short.

What are we lacking?

The $1 trillion war against scams

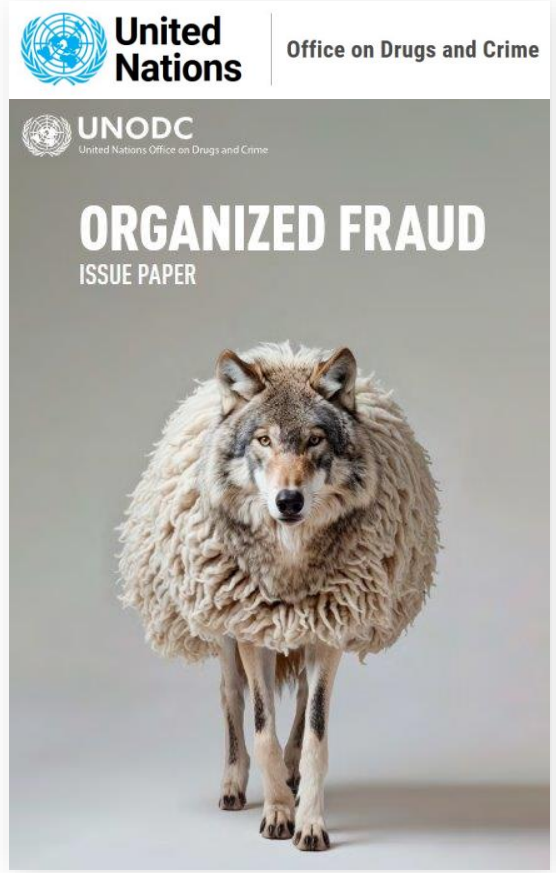
United Nations Convention against Transnational Organized Crime

UNTOC adopted by UN General Assembly: November 2000, (resolution 55/25); Entry into force: Sept 2003; signatories: 147 ; parties: 192 (as of 20 October 2023)

- Main international instrument in the fight against transnational organized crime.
- recognition by Member States of the seriousness of the problem, and the need to enhance close international cooperation
- States that ratify this instrument commit themselves to taking a series of measures against transnational organized crime, including

UNODC Global Programme on Implementing UNTOC

- Issue Paper on Organized Fraud (October 2024)
  - Chapter I : understanding organized fraud, definition of fraud
  - Chapter II : typology of organized fraud
  - Chapter III : discussion of organized fraud offenders, profiles and pathways into offending
  - Chapter IV : description of the cross-cutting facilitators of fraud
  - Chapter V : national and international responses,, gaps and areas for improving prevention and law enforcement
- Legistative Guide to implementing UNTOC : work in progress



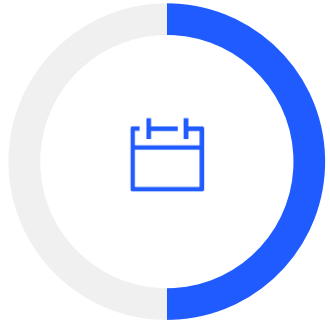
The $1 trillion war against scams

2024 Global State of Scams report shows that
phone calls and texts remain primary methods reported
(approx. 64% of cases)

Only **13%** of victims **recover** their funds (GASA)

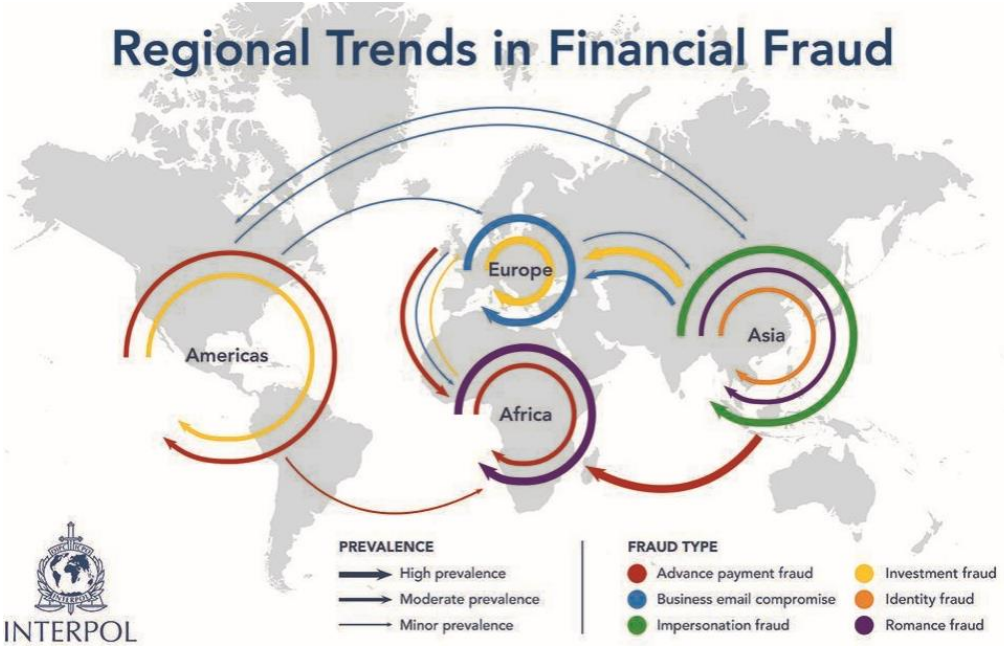
A mere **0.05%** of all cybercriminals face **prosecution** (WEF)

75% of individuals report being exposed to scams at the same rate or more frequently than in 2023



50% encounter scams **at least once a week**

The $1 trillion war against scams



The increased use of technology is enabling organized crime groups to better target victims with growingly **sophisticated phishing** and ransomware attacks

Fraud is Global

scammers operate globally and react
faster than our ecosystem does

The industry focuses on individual and local approaches that can rarely become proactive and truly collaborative

02 Traffic-based Insights Challenge

- Every carrier and mobile network operator has dedicated resources to technology and process enhancements.
- Sharing intelligence and fostering collaboration are essential for improvement.

SMS phishing

Attack profile

- **SMS Phishing attacks** against Greek and Georgian end-users subsequently
- **Malicious urls** impersonate several local postal services and Netflix
- **One single origin number** generated +200K SMS

First attack in May 2024, **impacting all Greek operators** with more than 1,5Mio SMS in a week. The SMS originated out of a European Tier1 operator

Subsequent attack in May 2024, **impacting all Georgian operators** with more than 1Mio SMS in a week. The SMS originated out of a European Tier1 operator

Sample origin numbers towards Greece

SOURCE_ADDRESS	Total
0689100	208916
2662623	75665
6229222	60023
7861223	59247
9311439	56043
1461844	51665
5209212	47813

Sample origin numbers towards Georgia

SOURCE_ADDRESS	Total
0013526	60000
2813772	56199
6259577	49480
8789947	49433
2240537	49327
9921208	43370
4438656	41426

Sharing information on urls / origin numbers, attack profile etc. can help prevent subsequent attacks globally

SMS phishing

Attack profile

- Phishing SMS attacks against **Slovenia and Guyana end-users** simultaneously
- Malicious urls faking a login request
- One single origin number generated +210K SMS in 2 days

During the attack in April 2024 each end-user received more than 100 SMS in only 2 days. The SMS originated out of a European Tier1 operator

Voice call phishing

Attack profile

- Phishing calls against **Puerto Rico and UAE end-users** subsequently
- Malicious calls in a period of 2 weeks

During the attack in Jun 2024, the end-users made 15K calls back to the fraudsters

During the attack in Nov 2024, the end-users made 590K calls back to the fraudsters

Sharing information on the urls / origin numbers, calling numbers, attack profile etc. can help prevent subsequent attacks globally

Industry solutions

Technical Solutions

All telecom SPs operators, International SPs, aggregators, ... have deployed technology to protect their networks, activity and direct customers against fraud

Collaboration

To gain end-to-end view and understanding of the attacks
To improve protection and mitigation cross-industry and cross-sector

Intelligence sharing

Leverage Intelligence gathered globally to learn of experience, react faster and protect better.
Improve cross-industry and cross-sector collaboration

Reactive approach: hit - analyze - decide
Individual and local approach no matter the technology or process: AI, APIs, real-time and near real-time, KYC, internal processes, etc

Collaboration requires openness to allow for investigation and end-to-end understanding of the attacks cross-industry and cross-sector

All parties understand that intelligence sharing is a need, yet these remain shy, partial and unstructured

Scam Signal API (CAMARA standard)

Description

Aim: **help banks improve the detection and prevention of bank transfer related frauds in real-time**. In case of a suspicious transaction, the bank may call the Scam Signal API and receive information based on real-time network traffic data

Use-case

Authorized push payment [SCAM] prevention: preventing criminals from manipulating their victims into making payments through impersonation scams. Typically, a fraudster socially engineers the victim to authorize a payment to the fraudster's account

Source of data

Real-time network traffic data from traffic carrying companies

Solution

Input parameter: phone number

PhoneNumber	A public identifier addressing a telephone subscription. In mobile networks it corresponds to the MSISDN

Output parameter

Parameter	Values
callInProgress	'true' - The phone number is on a voice call (Busy) 'false' - The phone number is not on a voice call (Not Busy)
callDirection	Direction of the call. Only present if 'callInProgress' is 'true' 'OUTBOUND' - Outbound call from mobile. Mobile originated call (MO). 'INBOUND' - Inbound call to mobile. Mobile terminated call (MT)
callDuration	Duration of the call in minutes. Only present if 'callInProgress' is 'true'
callStartTime	Timestamp (including date) of when the call started. Only present if 'callInProgress' is 'true'

03 **Regulatory Challenges**

Regulatory fragmentation and limitations

The regulatory approach is fragmented, creating loopholes for fraud and even conflictual obligations

Regulatory fragmentation

We need to address the international nature of fraud, foster collaboration and enhance intelligence sharing

We need to address the international nature of fraud, foster collaboration and enhance intelligence sharing

Local vs International

International Coordination

Multiplicity of Authorities

Outdated Regulations

Wider ecosystem collaboration through **Restore Trust**

A global purpose-built initiative to combat fraudulent communications

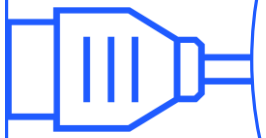
One Consortium
i3Forum

Started in March 2024

The Industry pillar, not-for-profit, members driven, members funded

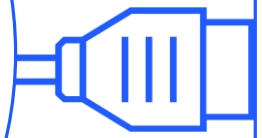
Objectives:
- co-develop global guidance and vendor neutral "toolbox" to combat intl fraud
- drive adoption and build an industry-wide self governance

Membership:
- Industry parties and associations (48 members to date)



Restore Trust

Topics addressed
- Voice and Messaging enabled frauds and scams
- Calling number spoofing
- International traceback
- KYC
- Number suballocation
- Information sharing mechanisms



GIRAF

Started in June 2024

The regulatory pillar, an informal group of experts. Neutral, independent and NRA sovereign

Objectives:
- Enhance the fight against fraud through multilateral NRA collaboration and cooperation with Industry and other stakeholders

Membership:
- Industry parties and associations (38 members to date)

04 What next?

- Strategies for closing the divide between our current situation and our desired goals
- A unique initiative to Restore Trust: One Consortium and GIRAF

How to bridge the gap?

In the mid-term and long-term, preventing and combating fraud and scams needs a **collective commitment from all parties and the right regulatory and legislative framework**

Global Coordinated Approach

Including Industry and Regulators to allow for end-to-end efficiency

Regulatory Balance

Between privacy protection and fraud protection (eg. Analysis of traffic data, collaboration and intelligence sharing to fight fraud

Flexible Regulation

To allow for future-proof interpretations and avoid a ‘regulatory-monster-machine’

Foster Sustainable Business

Where each party decides consciously on who to work with and how to do it.

Restore Trust

A global purpose-built initiative to combat fraudulent communications

proximus
Global