Sophisticated Scams Are Driving a New Industry Approach: Real-Time Fraud Data Sharing

SIPNOC, September 2025

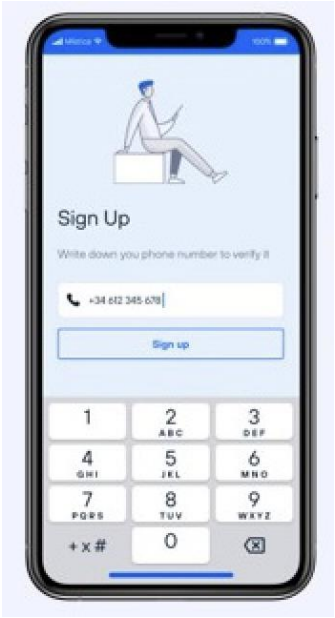
The Mighty Telephone Number (TN)

Telephone numbers were first used in 1879 in Massachusetts.

Before that, callers had to request subscriber names to the the switchboard operator.

The TN Is More Important Than Ever

With RCS, text messaging is end-to-end encrypted. Content inspection is no longer an option. Insights of the sender and the receiving number can help detect fraud.



Network APIs rely on the telephone number to enable new use cases by leveraging authoritative mobile operator data.

The telephone number as unique identifier across communication channels and services acts as key identifier and common denominator for fraud data sharing

Telco Fraud: What's New?

Fraud Remains High Despite All Efforts

- Scammers steal over $1 trillion in 12 months
- 70% of scam victims did not report the scam
- Only 4% of victims recover their losses
- Majority of scams are delivered via phone calls or text messages

Source: Global Anti-Scam Alliance (GASA)

Top Fraud Types

United States
- Robocalling / Robotexting
- Phishing
- Social engineering (pig butchering)
- Brand impersonation
- Financial fraud

Can be mitigated with →

DNO
STIR/SHAKEN
Network APIs
Fraud Data Sharing

Non-US
- AIT / AGT
- IRSF
- Phishing
- Social engineering (pig butchering)
- Financial fraud

Can be mitigated with →

Number Check
Network APIs
Fraud Data Sharing

Network APIs

Success Drivers

Trends that accelerate the demand for Digital Identity Solutions

- Fake Accounts
  - 1 in 4 online accounts is assumed to be fake
- SMS traffic and price inflation
  - Enterprises look for alternative authentication methods
- Account Takeover
  - Password Reset is the new Login
- SIM Swap Fraud
  - OTP via SMS is weak, because the SMS can be intercepted
- APP Fraud (Authorized Push Payment)
  - Victims get convinced to actively transfer money to fraudulent accounts
- Helpdesk Fraud
  - Impersonation of reputable brands helps with social engineering to defraud victims
- Regulatory Updates
  - E.g.: UK and Germany allowing network signals for account protection; India requiring SIM Swap signal before number porting

Successful Network APIs

Digital Identity APIs to safeguard customer journey

Location Verification

Trusted Conversation

Device Roaming Status

Account Protection

SIM Swap

Seamless Authentication

KYC Match

Identity Verification

Reject Bots

Scam Signal

Tenure Signal

Device Binding

Device Swap

Number Verify

Image by Sprinklr

Number Check

What is Number Check?

Is a phone number **valid (reachable)** or **invalid (unreachable)**?

Has the phone number been flagged for **fraud**?

Global coverage, any phone number anywhere in the world

Number Check Use Cases

Routing

➡ Avoid unnecessary termination costs, reduce fraudulent traffic

Customer Onboarding / KYC

➡ Screen out malicious users to avoid expensive identity data and other onboarding costs

Marketing

➡ Eliminate unreachable numbers from marketing lists – Reduce costs and increase campaign effectiveness

Fraud Data Sharing

Outside Telecom, Fraud Data Sharing Works

- Malicious domain names and IP addresses are **broadly shared** within the industry
- The shared data is used in **real-time** to protect web browsing and email

In Telecom, Fraud Data Sharing is Fragmented

Within Trade Groups

- Some trade groups have their own fraud data sharing mechanism, typically for members only
- These are often based on file distribution (sometimes as rarely as once per month) or even non-automated processes (data posted posted on web pages)

On a 1:1 Basis

- Occasional / ad-hoc exchanges between some carriers, some CPaaS providers and some enterprises (e.g., banks)
- Most of these are 1-to-1 or 1-to-few, so there are no scale benefits across the ecosystem

FRAUD PREVENTION REGISTRY (FPR)

MALICIOUS SENDERS

Phone numbers used as originators:

- Sender IDs of text messages
- CLIs of voice calls

→ Flag and / or block fraudulent communication

VICTIM NUMBERS

Phone numbers that belong to victims of fraud attacks like phishing and data breaches. These victims are at high risk of fraud facilitated via telecom services, e.g., account takeover.

→ Use this signal for risk assessment

→ Reset account passwords

→ Introduce additional steps to verify high value transactions

Data Sources

Financial Institutions

Carriers

Data Breaches

Phishing Victims

Why More Fraud Data Sharing Matters

Proactive beats reactive

- Fraudsters attack multiple telco providers and enterprises simultaneously. As soon as one of them reports the incident, the others can benefit, and fraud gets shut down faster.
- The fraud method or the communication channel might change, but unique identifiers like the telephone number simplify ongoing fraud tracking.
- Strong, automated feedback loops help spend time and money on growing the business, not on fighting incidents.


netnumber