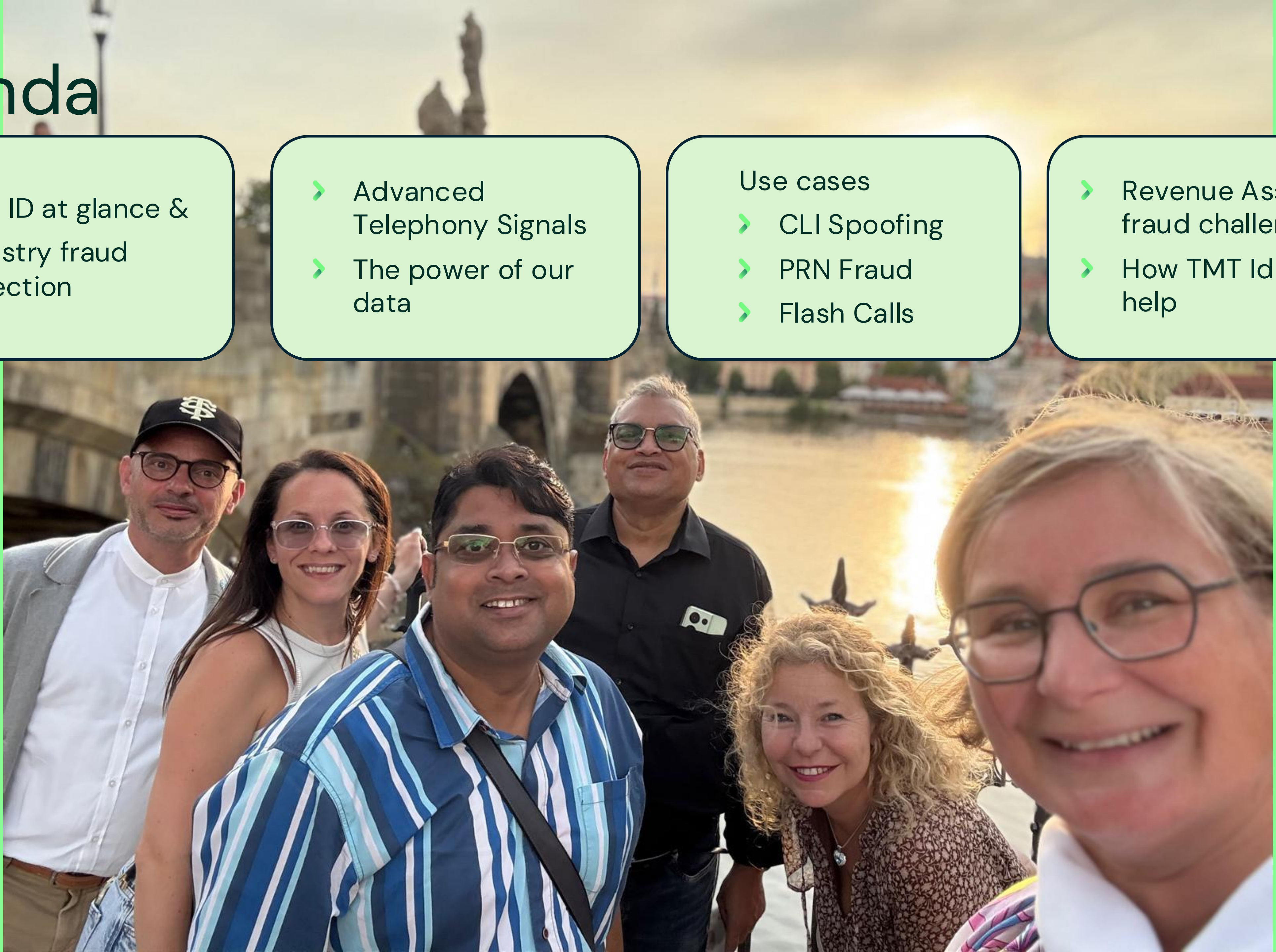
tmt id

Anti-fraud & Number Intelligence

Protect Revenues and Create Opportunities

Agenda

Agenda



- TMT ID at glance &
- Industry fraud detection

- Advanced Telephony Signals
- The power of our data

Use cases

- CLI Spoofing
- PRN Fraud
- Flash Calls

- Revenue Assurance fraud challenges
- How TMT Id can help

TMT ID at glance

A leading provider of mobile intelligence
Delivering actionable numbering information that powers the leading messaging, identity and financial services companies, enhancing and protecting their end-to-end customer journey

Providing a single gateway to the World, strengthening user verification, reducing fake accounts, improving conversations and determining the optimal channel for message delivery

- Enhanced coverage of DoB match and 18+APIs
- Provides rich liveness data on 2B numbers
- Unique MNP coverage in 110 countries, with 7 years of history
- 80 Million movements per day
- Over 2B customer queries per month
- Regulator reference data from ~240 countries/territories
- IR 21 normalization across 3,000 global networks
- 3Bn unique numbers

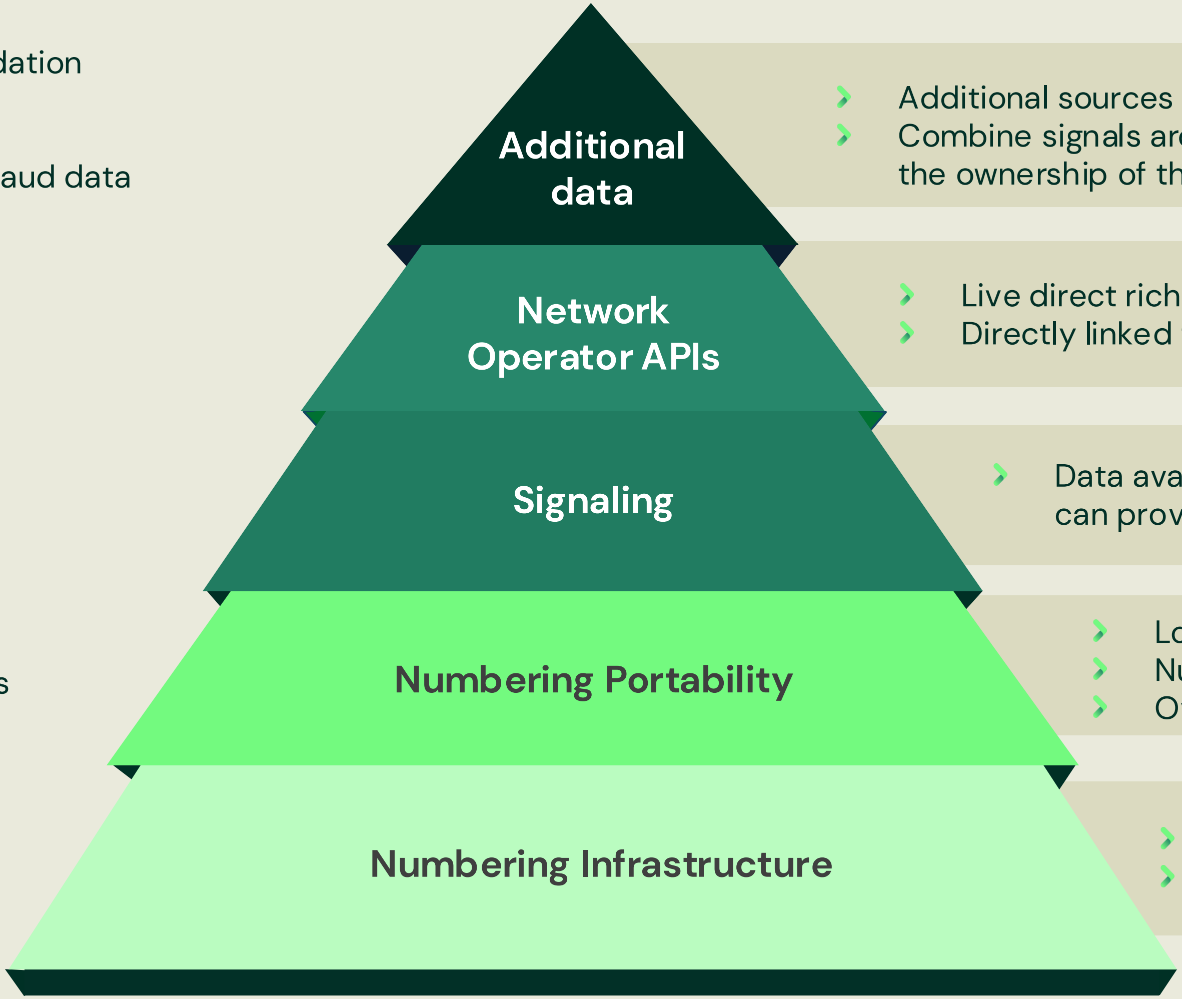
Market leading position with over 30 MNO KYC APIs live

On-net global data deliver results in less than 5ms, 100 million times/day

195 updates over 168 unique destinations monthly

Industry Fraud Detection

Using mobile Intelligence data



- Email/IP address validation
- National databases
- PEP/AML/Sanctions
- Customer supplied fraud data

Additional data

- Additional sources to enhance AI and improve signals
- Combine signals around the number with signals around the ownership of the number to complete the picture

- SIM-swap data
- Age verification data
- KYC match data
- Silent authentication

Network Operator APIs

- Live direct rich mobile network operator data
- Directly linked to the mobile number

- IMSI data
- Subscriber status
- Call status/line busy

Signaling

- Data available today to Mobile Operators that can provide intelligence on potential fraud.

- Current movements
- Historical movements
- Pre-Post paid status

Numbering Portability

- Long-term historical movements
- Number economic activity signals
- Overall number trustworthiness

- Number types
- Numbering plans
- Allocated ranges
- IR-21s

Numbering Infrastructure

- Instantly remove fake/incorrect numbers
- Identify suspicious numbers and types

tmt id

Case Study 1 – Origin Based Rating/CLI Spoofing

Customer Problem

An international Operator was billed tens of thousands of Euros in call surcharges. They did not discover it until months after they had processed the traffic. They suspected they were a victim of spoofing and requested TMT's help.

Results of the Data Analysis

- **8%** were missing valid country codes;
- **75%** had invalid formats;
- **7%** of the numbers looked valid but reviewing other attributes determined they were not available for assignment to a subscriber.

Case Study 2 – Premium Rate Number Fraud

International Revenue Share Fraud (ISRF) Example

Customer Problem

A European Network Provider discovered an ISRF attack being committed through a customer’s PBX after receiving alerts that indicated a call threshold was exceeded. By the time it was identified, 812 calls had been completed to 9 different countries.

Results of the IPRN Data Analysis

Confirmed 100% of the numbers were an exact match or were part of an identified suspicious range.

- **539** numbers were an exact match to an IPRN number in the database;
- **273** numbers were flagged as part of a suspicious Premium Rate Number (PRN) range.

tmt id

Case Study 3 – Flash Call Detection

Customer Problem

An A2P Messaging Platform provider and a Fraud Solutions provider both requested an independent review of traffic that they had confirmed to be flash calls. The objective was to assess the ability of TeleShield's service to detect flash calls.

Results of the Flash Call Analysis

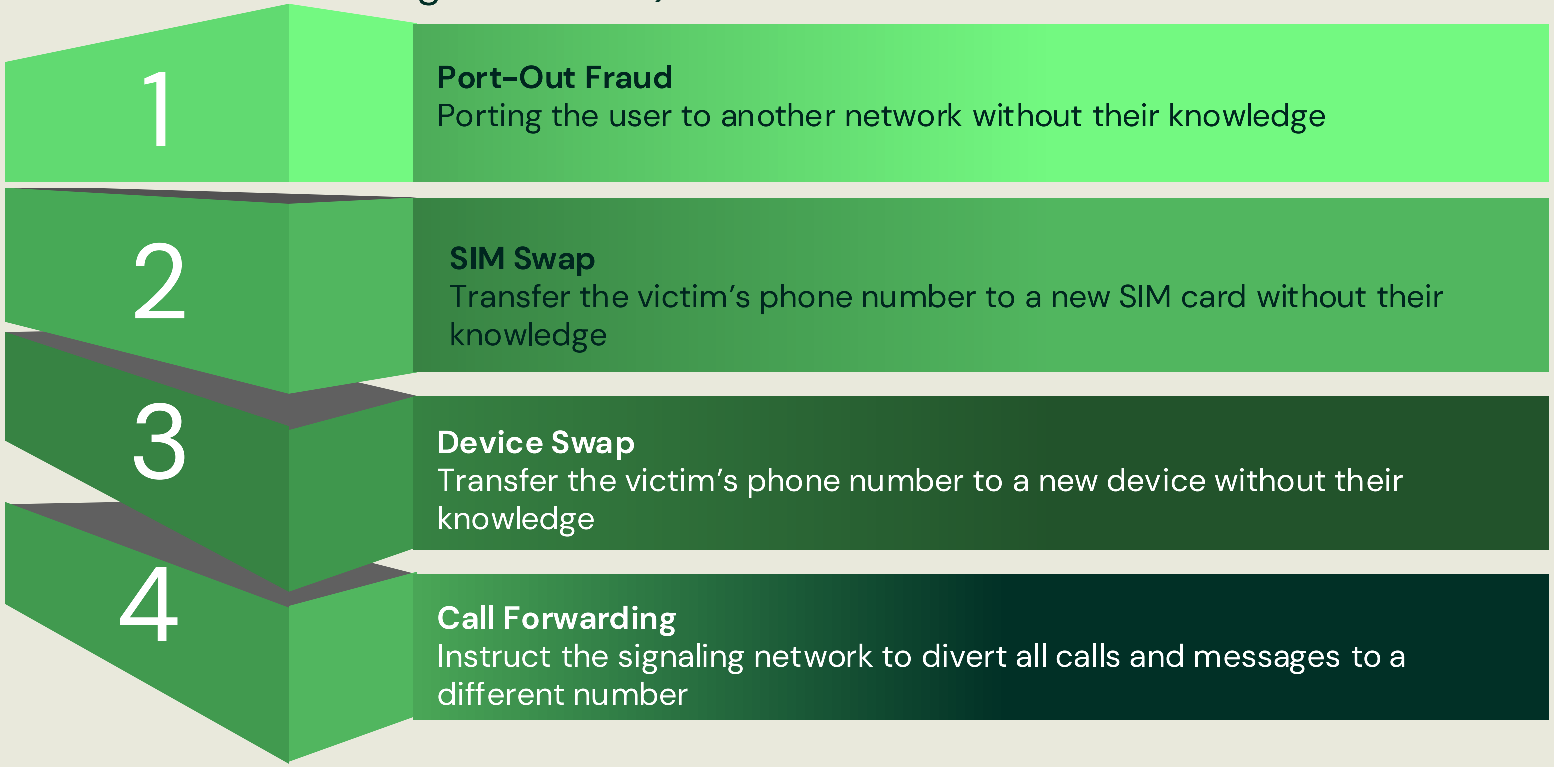
For the A2P Messaging platform provider, 53% of the calling numbers (A numbers) were identified as invalid.

For the Fraud Solutions platform provider, **70%** of the calling numbers (A numbers) were flagged as fraudulent through data attributes that were invalid.

Advanced Telephony fraud signals

Example attack vectors

Protect network & customers by identifying changes that have happened to a device or number. Typically, this fraud is not the end goal, but the enabler for criminals to then commit a wider fraud (e.g. mobile banking infiltration)



1 **Port-Out Fraud**
Porting the user to another network without their knowledge

2 **SIM Swap**
Transfer the victim's phone number to a new SIM card without their knowledge

3 **Device Swap**
Transfer the victim's phone number to a new device without their knowledge

4 **Call Forwarding**
Instruct the signaling network to divert all calls and messages to a different number

Available Information

Recent Port know if a number has ported as soon as it happens.

SIM Swap know when the last time the SIM card associated with the number changed.

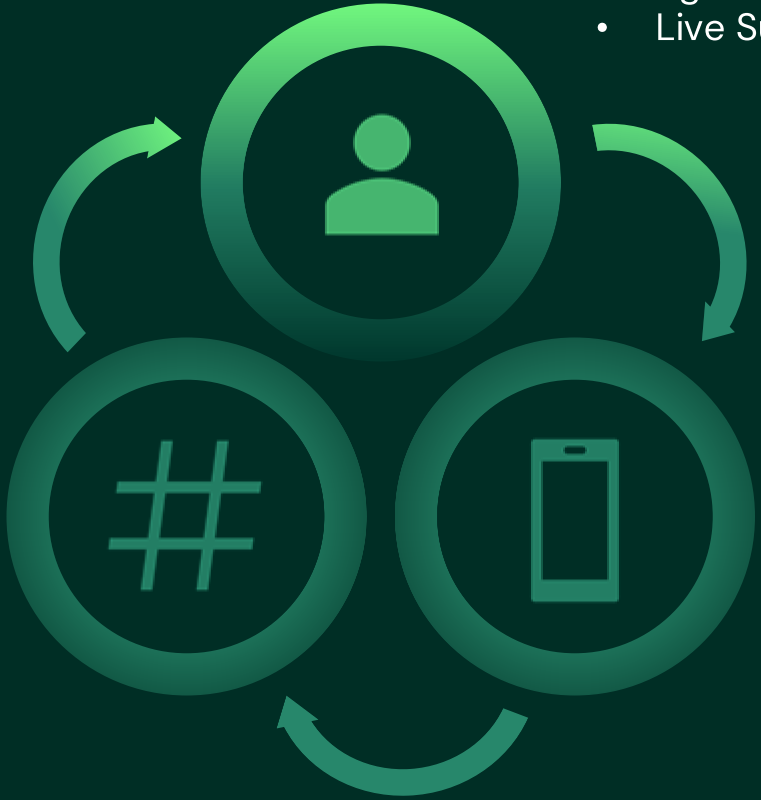
Device Swap know when the last time the handset associated with the number changed.

Call Forwarding is the unconditional call forwarding parameter set? YES/NO.

The Power of Our Data

The individual:

- Sim – Device – Mobile Account Check
- Name, Address, Age KYC Check
- Age Verification Data
- Live Subscriber Intelligence



Mobile number intelligence:

- True Number Check
- History
- Active Status
- Port History
- Pre-Pay/Post Pay

Device level intelligence:

- Sim (IMSI) to Number Check
- Device/SIM to Account Match
- Sim Swap Alert
- Device Change Alert

High assurance and low friction mobile number, device and identity verification, without the need to upload documents or a selfie.

Can be integrated into multiple work flows seamlessly – Onboarding - Age verification - Sign in – Checkout – Payments - Transactions

Revenue Assurance Fraud challenges

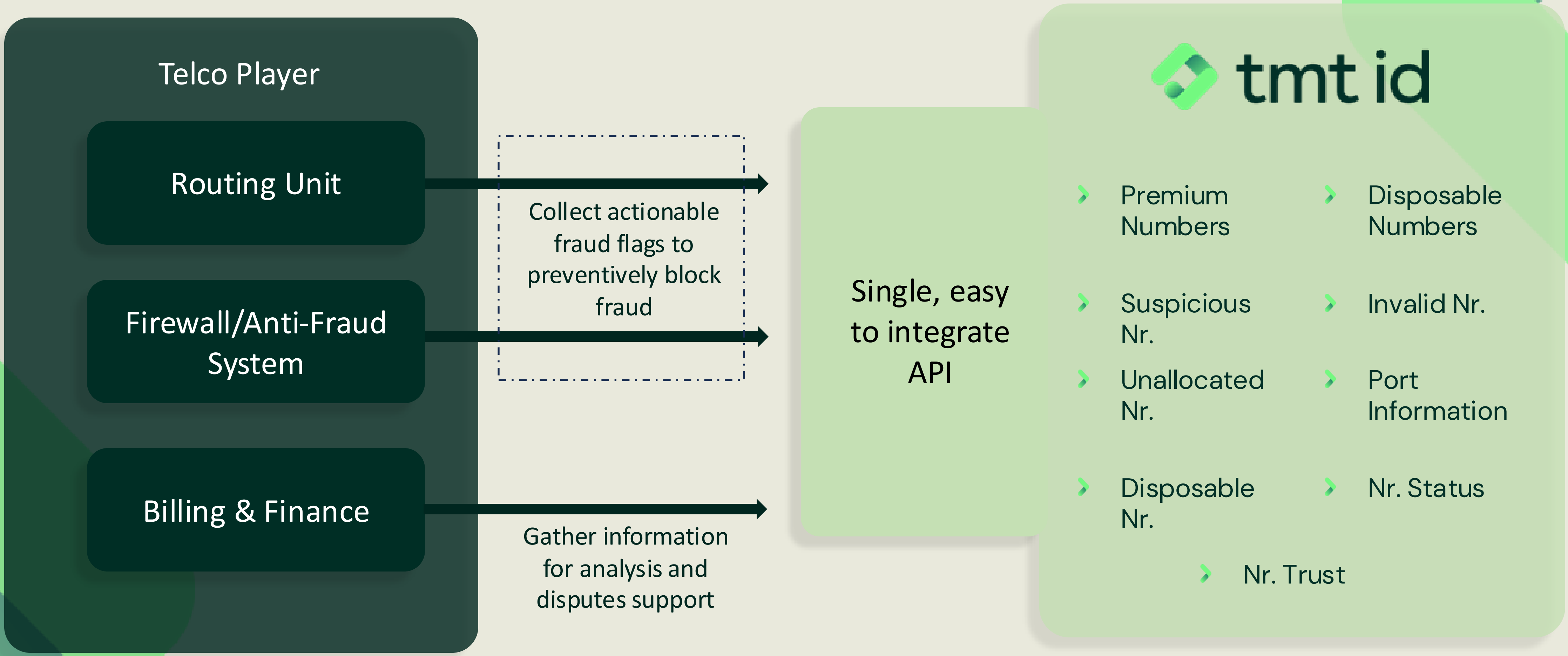
- An average fraud dispute can consume around 20K EUR in internal manpower costs only and take between 1 and 3 years to resolution.

- Common experience is that people in Revenue Assurance notice after 1.5 months or longer, and billing CDRs are the only available element for analysis.

- Investigations involve the cooperation of the receiving party which, in 80% cases, is “no answer” or denied (no interest to lose termination revenues).

- Operational troubleshooting can take up to 6 months and network people not always have the expertise to support fraud queries.

How TMT ID Can Help



Telco Player

Routing Unit

Firewall/Anti-Fraud System

Billing & Finance

Collect actionable fraud flags to preventively block fraud

Gather information for analysis and disputes support

Single, easy to integrate API

tmt id

- Premium Numbers
- Disposable Numbers
- Suspicious Nr.
- Invalid Nr.
- Unallocated Nr.
- Port Information
- Disposable Nr.
- Nr. Status
- Nr. Trust

Thank you

guendalina.rossi@tmtid.com