



## MARKET BRIEF

# Outsmart the Fraudsters

### Ever-Growing Complexity of Telecom Fraud

Telecom fraud is constantly evolving as fraudsters are finding new ways to commit fraud using your networks. Whether it is subscription fraud, Wangiri, PBX hacking or International Revenue Share Fraud (IRSF), it can be difficult even for experienced fraud managers to guard against the latest attack methods.

Although great strides have been made in mitigating fraud across the industry, fraud managers and consumers need to remain vigilant in their pursuit to keep the fraudsters at bay.

### The Ripple Effect

Fraud totaled \$38.95 billion in 2023, according to the Communications Fraud Association (CFAA). That is 2.5% of global telecom revenues.<sup>1</sup> Of course, the actual cost is much higher due to the collateral damage to your brand reputation, organizational efficiency and customer satisfaction.

In the highly competitive telecoms marketplace, you are focused on creating and launching innovative services to differentiate yourself from competitors. Each technology and service added means new opportunities for fraudsters to infiltrate your network. To combat this, your security and fraud strategies need to remain robust to stay several strides ahead of the latest techniques. For instance, detecting fraudulent numbers before connecting the call requires a detection of calls to premium and unallocated numbers as they happen. The good news is that with high-quality numbering data you can proactively protect your business from being the unwitting victim of new attacks and criminal activity.

### Staying One Step Ahead

Even for the savviest fraud managers, outsmarting the fraudsters requires enhancing existing platforms and systems. This gives you added intelligence to identify fraudulent and potentially risky traffic even if it is brand new to your network, which allows you to prevent revenue loss and improve risk management. Comprehensive solutions also allow you to proactively block calls to fraudulent numbers and perform targeted interrogation of inbound traffic for call attempts.

Whether you use customer care trouble tickets, fraud alert systems or review traffic reports and profitability margins, complementing your existing fraud strategy with proven tools should allow you to:

- Proactively identify and block calls to high-risk, unallocated numbers
- Treat specific mobile number ranges with caution
- Maintain target and exception lists for special numbers in ultra-high risk countries
- View, manipulate and export Range Holder and International Premium Rate Number data
- Warn fraud prevention teams on impending attacks before they happen
- Provide a wider implementation of detailed number plan data used as a complement to traditional fraud management systems
- Safeguard revenue, margin and customer experience

### Let's Talk About your Fraud Prevention Needs

The bottom line is that a fraudster's motivation lies in finding and utilizing new methods to steal your money and profits. Your motivation comes from detecting and stopping them and there are simple, seamless and secure solutions that will allow you to safeguard your revenue and gain valuable insights into ever-evolving fraud techniques.

1. <https://cfca.org/telecommunications-fraud-increased-12-in-2023-equating-to-an-estimated-38-95-billion-lost-to-fraud/>

**Find out how TNS can help you with a wide range of telecom solutions:**

[solutions@tnsi.com](mailto:solutions@tnsi.com)

[tnsi.com](https://tnsi.com)

USA

Europe

Asia Pacific

**+1 703 453 8300**

**+44 (0)114 292 0200**

**+61 2 9959 0800**