bics

Understanding international telecoms fraud: protect revenue, mitigate risk

Introduction

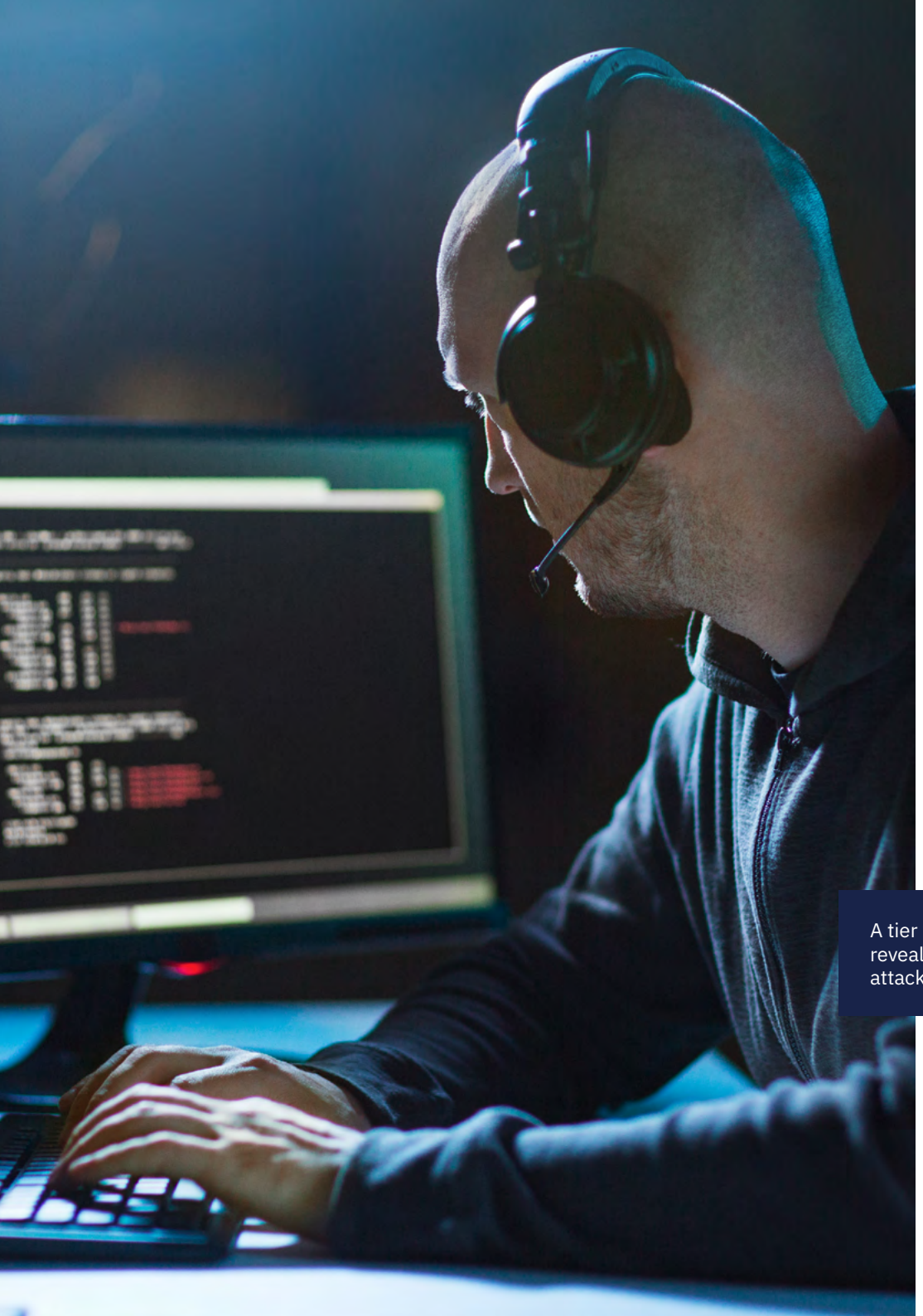
Telecoms fraud is increasing at an alarming rate globally and is one of the biggest sources of revenue erosion for every telecoms operator. According to the CFCA, global fraud loss was estimated at US$ 28.3 billion in 2019, equating to 1.74% of 2019's estimated global telecom revenues, with the top 5 fraud types accounting for 54% of all fraud losses.

The alarming fact is that two-thirds of all fraud losses, especially voice fraud losses, are tied to international traffic. For example, losses from *International Revenue Share Fraud* (IRSF), exceeded US$ 5 billion in 2019, while Wangiri attacks cost mobile operators US$ 1.8 billion[1].

Industry today is spending millions protecting itself from fraudsters post-facto, after attacks have already taken place. As a result, it is perpetually on the defensive and in reactive mode.

With bottom lines under tremendous pressure, it is now time for telecom executives to invest and collaborate in fraud protection solutions that will safeguard their networks from attacks effectively & proactively.

[1] https://cfca.org/putting-telecom-fraud-loss-into-perspective/



What is telecoms fraud and how big is the problem?

The GSMA defines telecommunications fraud as something that is perpetrated where process, control or technical weaknesses are intentionally exploited, resulting in a financial or other loss. The GSMA acknowledges that the term ‘fraud’ is defined in many national legal frameworks, and operators may use different definitions within their own businesses and countries. The perpetrators can either steal telecommunication services or misuse them to incur losses or defraud innocent subscribers into incurring huge bills or stealing private data.

In the world of highly interconnected 4G and 5G networks, fraud can originate from any location. Barely a day passes without criminals making fraud attempts somewhere in the world, so operators need to be vigilant about traffic from and to any location.

BICS fraud prevention solutions have detected and blocked more than 1.3 million fraudulent call attempts on customers’ networks, saving them on the upwards of US$2.4 billion in international voice revenues.

In 2019 telecom fraud was worth US$ 28.3 billion according to the CFCA. 89% of operators surveyed said fraud losses had increased or stayed the same within their own companies, however many companies are now reporting far fewer cases to law enforcement.

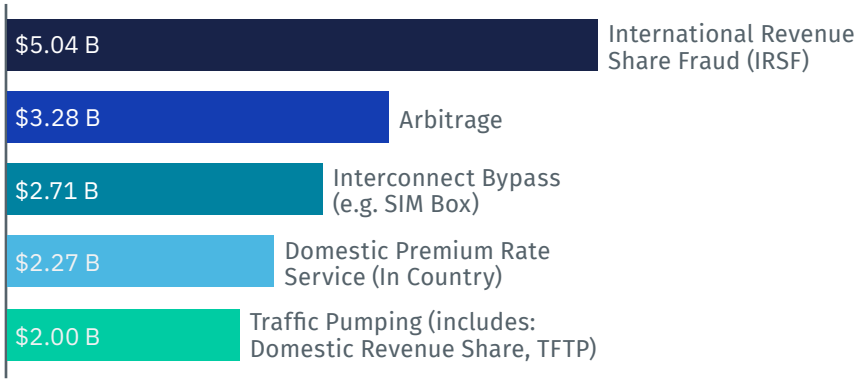
A tier 1 European operator fell victim to widespread PBX hacking fraud. Post incident analysis revealed that within just three months the operator was being hit by more than 200 attempted attacks, costing an estimated €130,000 in revenues

Estimating the scale of telecom fraud

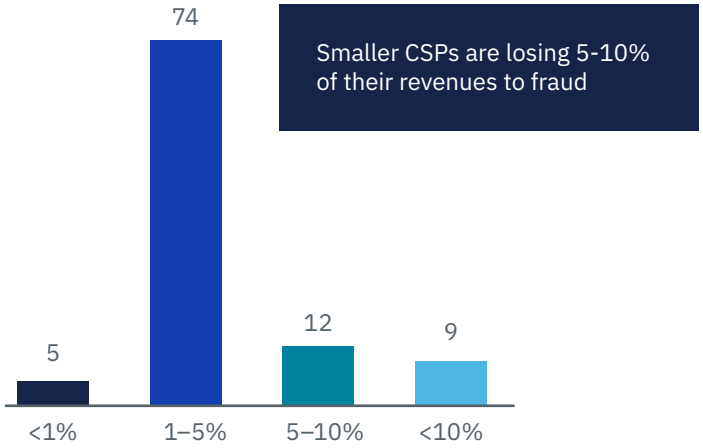
Total telecom fraud
US$ 28 billion

66% of MNOs
experienced growth
in fraud in 2019

Most widespread types of telecom fraud



The % of global telecom revenue operators think is fraud



Source: CFCA 2019 fraud loss survey

The impact of fraud

For operators

- Loss of revenue
- Damage to brand and reputation
- Increased spending on customer service
- Time and manpower to repair damage

For consumers

- Loss of money
- Loss of personal data and repercussion from it
- Time spent to recover data / inaccurate billing
- Frustration / Stress / Loss of trust

Types of fraud and how they work

Many different types of fraud currently permeate international telecoms markets, impacting 3 main areas:

1. Voice

Voice fraud is a common term given to a number of schemes that criminals use to generate illegal or abusive voice calls, in general to get a financial benefit from it. Voice fraud can force subscribers to rack up huge bills and often force operators to pay out *call termination charges*, which they can get a share of. The most common international fraud schemes are voice-based, costing operators millions in revenue.

International Revenue Share Fraud (IRSF)
A practice where fraudsters obtain access to operators' networks to make many calls to premium rate numbers or international calls to destinations with high termination rates. The criminals then receive a share of the revenue generated from the termination charge.

The most prevalent access methods leading to IRSF are:

- **IP PBX / PBX hacking:**
  To perpetrate this fraud scam, fraudsters hack into enterprise PBX systems to generate illegitimate voice traffic. Often, they make as many calls as possible to international premium rate numbers or other international expensive destinations that they own or where they intend to receive a share of the revenue generated.

- **Roaming fraud:**
  Criminals committing roaming fraud acquire SIM cards and use them from overseas markets to call international revenue share numbers. It takes a minimum of 3 - 4 hours for call records to get back to the home network in the form of NRTRDE files (Near Real Time Roaming Data Exchange) for analysis and decision making. During that time, fraudsters can generate huge amounts of traffic.

Recently, a single Western European number roaming in a neighbor European mobile network generated 9,000 calls or 149,000 minutes of traffic to premium rate numbers located in an expensive African country in just five hours. The criminals used call forwarding over calls coming from a market in the Middle East to generate the traffic.

Interconnect Bypass
A practice where international inbound calls exploit the difference between high international interconnect rates and low retail prices for both on-net and off-net calls. The operator loses the revenues from international call termination, which can be significant.

Interconnect bypass schemes currently on the rise include:

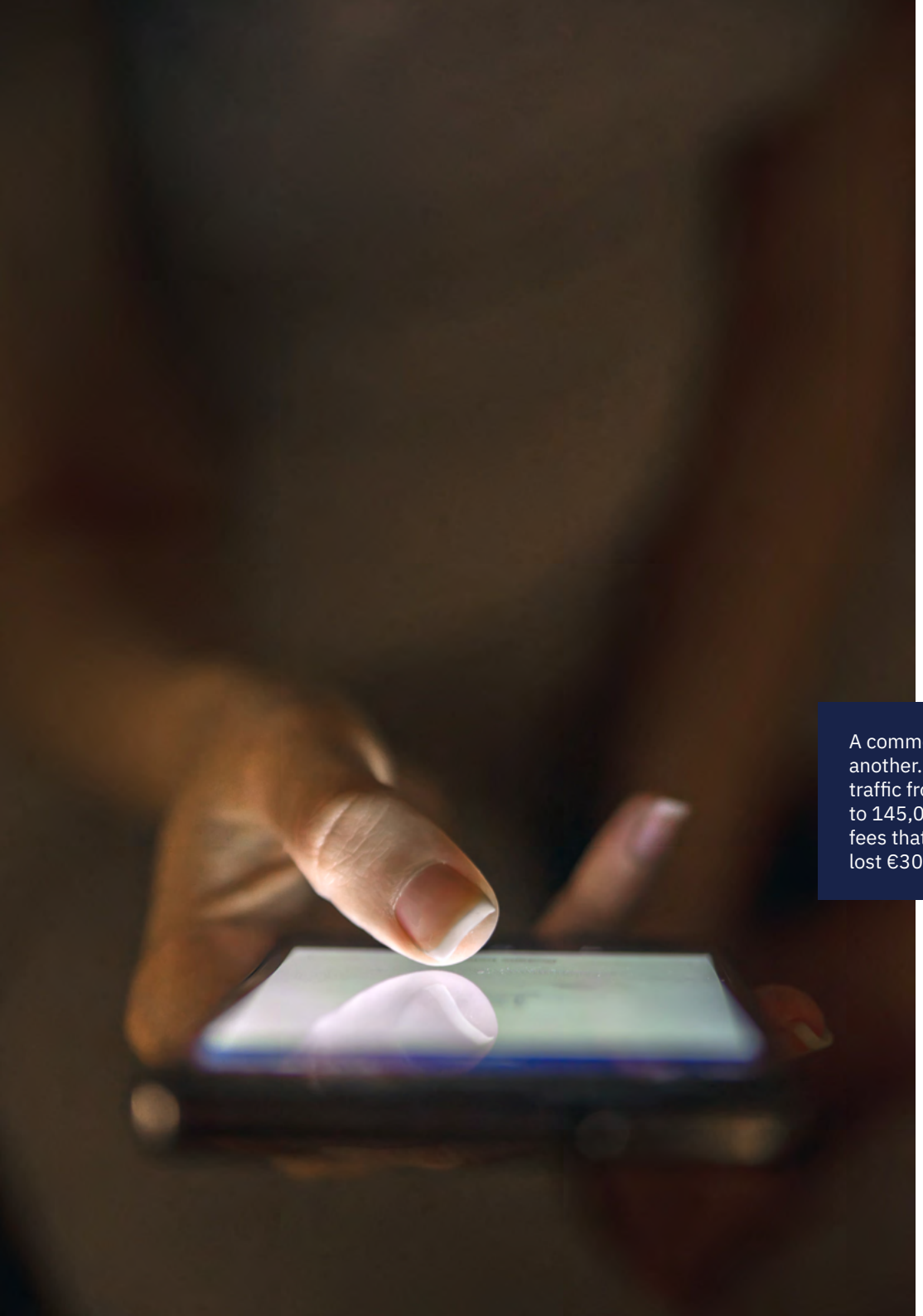
- **SIM Box fraud**, where illegal international VoIP calls are diverted onto local mobile networks through SIM boxes, allowing fraudsters to bypass international interconnect fees.

- **Refiling**, where carriers falsify the CLIs of calls to benefit from low international termination rates. This traditional fraud scheme is becoming more prevalent.

False Answer Supervision (FAS)

There are two variants of this fraud. In both cases, a party in the traffic flow chain returns a false answer signal to the earlier carriers in the chain, either starting billing too early for all parties (early answer) or finishing it too late (late disconnection). The objective always remains the same: keeping the calling customer on the line and paying for the call for as long as possible.

FAS is a particularly difficult fraud scheme to detect as in many cases only a percentage of traffic is diverted to FAS-enabled routes and the FAS-route only activates for well-defined originating countries.



2. SMS

SMS fraud exploits the fact that text messages sent internationally can be routed in several different ways to reach their destination, and each route has a different cost attached to it.

Grey or black routes
A practice where unscrupulous SMS aggregators use unauthorized or even illegal routes to deliver SMS messages at the lowest possible cost. This practice harms operators, depriving them of their legitimate termination revenues.

SMS hacking
Criminals can hack an operator's SMS center or even take control of it at the signaling level and use it to send malicious traffic all over the world. This traffic could solicit consumers to make calls to premium numbers or even contain viruses or other malware that could infect the recipient's phone.

A common symptom of SMS fraud is abnormal spikes in SMS traffic volumes from one operator to another. In a recent instance, an Australian operator, suddenly began receiving huge volumes of SMS traffic from an African country. The daily SMS volumes, which were typically in the hundreds, went up to 145,000 messages per day, costing the Australian operator €10,000 per day in SMS termination fees that could not be invoiced. If the case had gone undetected, the Australian operator would have lost €300,000 to SMS fraud in just one month.

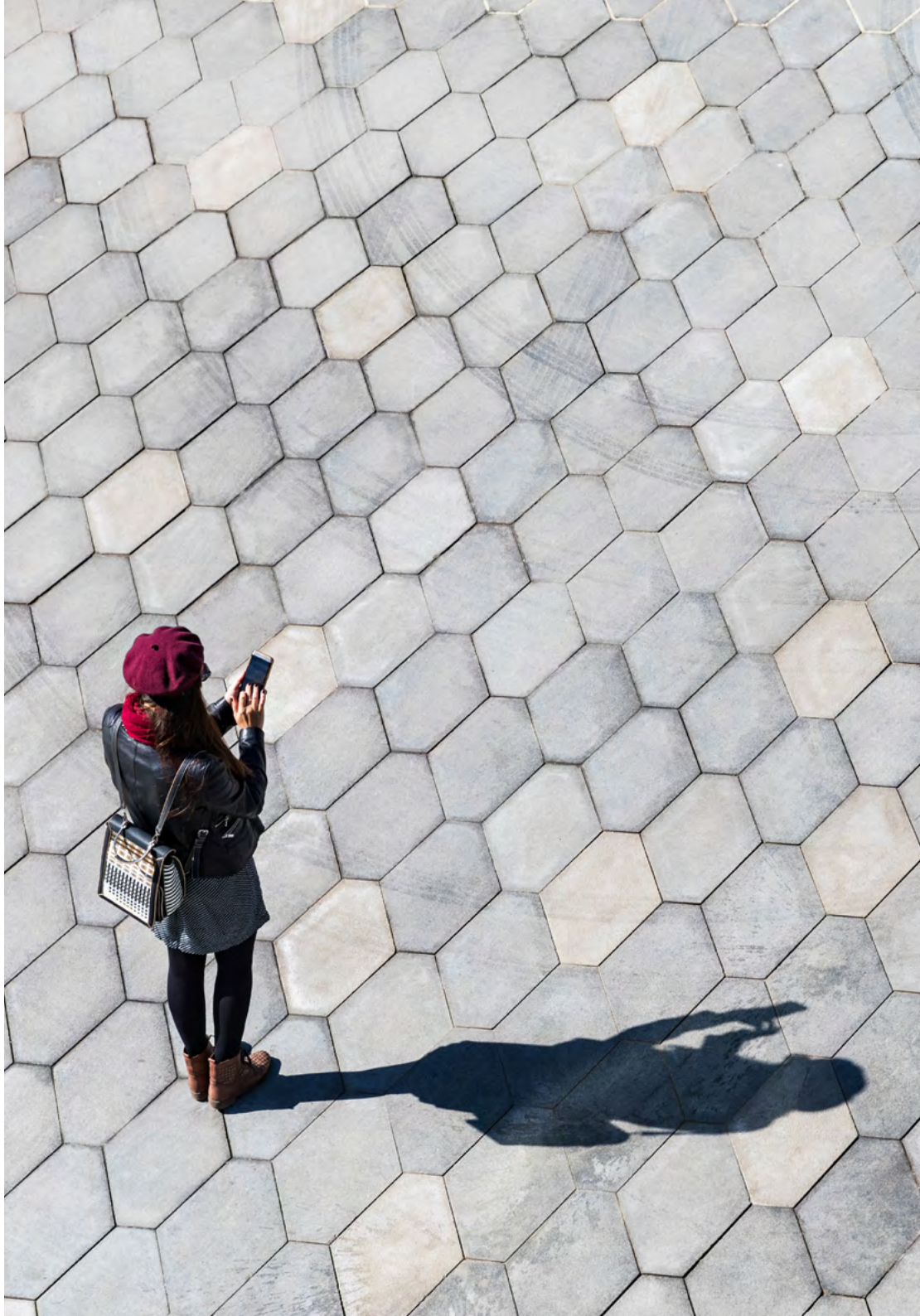
3. IPX and signalling

In today's interconnected world, operator networks interface with hundreds of other networks. If some operator networks or the interface between networks have vulnerabilities, criminals can exploit these to commit IPX and signaling fraud.

SS7 Signaling fraud
This type of fraud takes advantage of operators' vulnerabilities at the signaling control level used during roaming and making international calls. Fraudsters may hijack a roaming subscriber's phone and send fake or spam SMS messages to their contacts. This type of fraud can spread from operator to operator very quickly.

Steal personal data
Hackers can gain access to sensitive personal data about roaming customers. They can spy on user traffic and sell on sensitive user data to other criminals.

Distribute malware
Hackers can gain access to operator control systems and distribute malware to roaming consumers. For instance, a mobile virus within an app that looks normal but runs secret activity by sending huge amounts of data back to its host. This causes users to inadvertently incur huge bills.



Challenges in combating telecom fraud

The global reach of the internet, combined with changes to call and data roaming rules means telecoms fraud is no longer contained to a particular network or country. Today, fraudsters located in country ‘A’ can generate fraudulent traffic that originates in country ‘B’ and terminates in country ‘C’ with fraud behaving like a virus – spreading outward very fast, infecting network after network in succession and generating colossal revenue losses as a result.

Operators are unable to fight effectively against international telecoms fraud, for a number of reasons:

Cross-border jurisdiction: The lack of cross-border jurisdiction and cooperation hampers operators in their fight against fraud. More than 42% of mobile operators reported less than ten fraud cases to law enforcement authorities in 2021.[2]

Limited operational coverage (generally 8x5): Most fraud occurs during non-business hours but not many operators have 24 X 7 operational models in place.

Limited visibility of global fraud trends: Apart from some industry forums and regional operator groups, there is no platform to gather international fraud intelligence.

Roaming, one of the biggest voice fraud enablers, delays detection: Roaming has become a preferred vehicle to carry out international telecom fraud, because it introduces delays in fraud detection which may last anywhere between 4 hours and 3 days, until reconciliation takes place.

As a result of all these factors, historically, the cost of trying to block fraud and identify the perpetrators often exceeded the cost of writing off the loss.

[2] CFCA Fraud Loss Survey 2019

Concerted offensive needed to stop telecoms fraud

This historical ‘write it off’ approach is no longer a viable option for operators and the industry needs to go on the offensive in fighting fraud.

Fraud costs operators millions of dollars in revenue annually. An increasingly competitive telecoms industry is facing fast-declining ARPU and profit margins. The revenue generating cycle for new products and services in the telecoms sector is slow. The R&D–trial–testing–deployment cycle can last from eighteen months to over two years, and it is now accepted industry wisdom that a new product typically needs three years before it can generate revenues.

Following a year-long investigation involving law enforcement agencies from 35 countries worldwide, Interpol seized more than US$ 150 million worth of illicit funds from telecoms fraud in over 10,000 different locations. This demonstrates the difficulties of tracking down international telecoms frauds.[3]

An effective anti-fraud solution with minimal upfront investment would have a positive impact on the bottom line straightaway.

[3] INTERPOL, Operation First Light, Nov 2020

What can be done to limit fraud?

Despite the various international bodies investigating the problem (including the i3forum and the GSMA's Fraud and Security Group amongst others) and the efforts deployed by operators to install systems and processes to combat fraud, operators are still focusing on limiting losses once they're hit by fraud.

As with any criminal activity, protecting from the initial threat is much more cost effective than post-attack measures deployed in an attempt to repair damage and recoup lost revenue. The ability to act proactively is the most important factor in the success of the battle against fraud.

To prevent voice fraud, operators may use and benefit from the experience of other fellow operators. This will ensure they are not hit by fraud schemes and fraudulent numbers still active globally. The accuracy of the data (fraud numbers and fraud schemes) is key to ensure there is no impact on legitimate traffic. For example, accurate, real-time fraud intelligence can be useful in preventing roaming fraud.

SMS fraud can be reduced or eliminated by using a reputable and secure SMS hub that can close any 'open doors' and route traffic through official routes. Through deep dive analysis into network traffic it is possible to detect fraudulent traffic, which can be rerouted through legitimate routes or even blocked if necessary.

To protect operator networks from fraud that enters at the signaling level, a firewall approach is advisable to detect fraudulent traffic patterns or anomalous messages.

The globalization of telecoms fraud means that it cannot be dealt with on a standalone basis. The scale uncovered in some recent fraud-related arrests show that fraudsters are highly organized and operators should be the same.

While the criminals behind fraud are shadowy and difficult to track down, the telecoms community has **strength in numbers**.

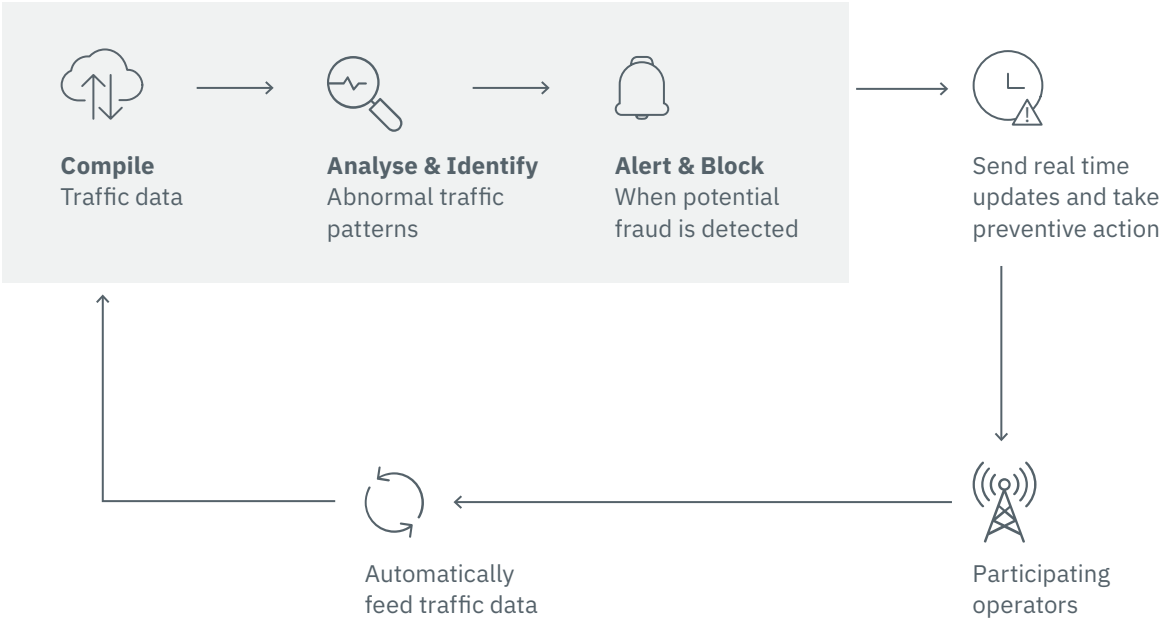
If the telecoms industry wants to succeed in its battle against fraud, co-operating operators and service providers need to work together to develop dynamic, real-time anti-fraud tools, so they can detect telecom fraud **as it happens** and act appropriately.

Crowdsourcing to beat fraud

A cloud-based crowdsourcing approach enables wholesale operators to proactively protect against fraud on a range of networks. By crowdsourcing details of suspicious network activity across a global customer base, a crowdsourced anti-fraud platform can identify and block activity to known fraud destinations.

Using the crowd to tackle telecoms fraud in the cloud

BICS cloud-based fraud prevention platform



Increased role for wholesale carrier in defeating fraud

As telecoms becomes more sophisticated, so too does telecoms fraud and international fraud can go viral within hours.

With their broad international footprint, huge volumes of daily network traffic, and extensive peering and interconnect relationships with other networks, wholesale carriers have the scale and reach essential to identify and, with the right dedicated tools and focus, analyze abnormal traffic trends and take accurate conclusions. The huge amount of traffic they carry across their networks enables them to spot fraud and build a holistic view with the necessary information to grant fraud prevention to their peers (fraud numbers, fraud schemes, and so on).

Many types of voice, SMS and signaling fraud are committed in the wholesale environment. Wholesale networks are therefore the perfect environment to detect fraud and act immediately on it.

Merits of using experts for fraud prevention

The advantages to using dedicated expertise for fraud prevention are many, including quick rollout and 24 x 7 access to dedicated, specialized knowledge and expertise.

In-house operator anti-fraud teams are typically specialists at retail fraud scams such as impersonation, subscription fraud, etc. Entrusting fraud detection and prevention to an international fraud specialist can be the best way to avoid crippling financial impacts.

However the most compelling reason is the comprehensive range of protection provided. The right anti-fraud service can detect a wide range of fraud scenarios in real time and proactively push this intelligence to operators, allowing immediate reaction to neutralize threats before they reach a network and business. It can also provide ongoing guidance and counsel on how to detect and prevent fraud for the different types of traffic on the network.

Here are some criteria that may help in selecting the right anti-fraud partner:

1. Comprehensive range.
Can the provider offer protection on vulnerabilities in the different services (voice, SMS or IPX fraud)

2. Timeframe.
Cloud-based solutions offer instant protection and easy rollout within just days rather than weeks and months.

3. Crowd-based intelligence.
Fraud is rarely confined to just one network. Will the service give access to intelligence from a global community of operators?

4. Comprehensive fraud database.
How granular and accurate is the provider's database of numbers around the world associated with criminal activity? What is the risk of inadvertently blocking genuine numbers through 'false positives'?

5. Global reach.
The right anti-fraud vendor should have a consistent track record of strong results across all regions and operator types.

6. Costs and service delivery.
If the anti-fraud solution needs minimal upfront investment, is cloud-based and can be bought as a service it can be absorbed into operating expenses and is easier to justify.

Conclusion

Telecoms fraud is a multi-faceted and ever mutating problem, made more complex by the constantly converging nature of this industry, which attracts frauds from parallel industries or domains.

It is not limited to any country or operator size or maturity and can be responsible for significant bottom line erosion, increased cost, legal complexities, complications in partner relations, reduced subscriber satisfaction, increased churn and service disruptions.

Fraudsters are constantly innovating, deploying sophisticated tactics and techniques that involve the combination of multiple complex methods and scenarios. Eroding revenues, high service quality upgrade costs, competitive environment and low ARPU mean that operators urgently need to adapt more strategic and proactive initiatives against fraud.

Fraud cannot be seen as a one-time risk. It must be continuously assessed and an operator’s methods to limit fraud exposure need to be nimble and evolve quickly to keep them one step ahead of the fraudsters themselves.

With this principle, BICS has developed an additional comprehensive range of fraud protection services covering the operators’ needs in the International fraud environment.

Types of fraud and their solutions

Types of fraud	Subscriber impacts			Operator impacts			BICS offering
	Bill shock	Churn	Privacy breach	Revenue loss	Customer experience	Industry ties	
Voice frauds • AIT, IRSF and PRS fraud • Roaming fraud • Refilling & CLI manipulation							 Voice FraudGuard Voice Roaming FraudGuard Voice Roaming Firewall
SMS frauds • Spamming • Spoofing / Faking • A2P bypass							 SMS FraudGuard SMS Firewall (with SMS Hub) SMS Bypass Detection
IPX frauds • Hacking and takeover • Service disruption • Spoofing							 IPX Security Security audit and security monitoring (SS7, Diameter and GTP Roaming Interworking)
Signaling frauds • Unlawful tracking/ modification • Non-competitive behaviours • Powering other frauds							 Risk consultancy, assessment and testing

For more information, please visit:
www.bics.com