bics

Securing international telecommunications

Proactive, comprehensive protection from telecoms fraud

Fraud prevention solutions

BICS headquarters:
Boulevard du Roi Albert II, 27
1030 Brussels, Belgium
bics-com@bics.com

Brussels | Bern | Beijing | Dubai | New York | San Francisco | Singapore

Safeguard your business and customers from the threat of telecoms fraud. BICS provides the industry's most comprehensive range of fraud prevention and security solutions to protect any form of telecoms service (voice, SMS, roaming, and signaling). Our solutions provide near-real time protection against known and new security threats.

Our solutions use crowdsourced intelligence, behavioral traffic analysis and machine learning to stay ahead of new fraud schemes. Our security experts are cross-domain and cross-service specialists who work 24/7 to ensure your network, bottom line and subscribers are protected.

The growing threat of international telecoms fraud

In the world of highly interconnected 4G and 5G networks, fraud can originate from any location. The complexity of international telecommunications and the roaming environment makes it an attractive ecosystem for fraudsters. The global, interconnected nature of telecoms networks often makes fraud hard to detect, and even more challenging to prevent.

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 $6 billion in 2020, while Wangiri attacks cost mobile operators $1.8 billion. Add to this the rising number of new fraud types and services that can be exploited (SMS, for example, has experienced a steep increase in fraud attacks in the past 2 years), and operators face a growing threat. This not only affects their bottom line, reputation, and customer loyalty, but can even open them up to regulatory action.

What makes fraud prevention so challenging?

An ever-changing landscape

Fraud is constantly evolving. Staying ahead of criminals means keeping up to date with all the tools they have in their arsenal. New technologies and use cases – such as IoT and A2P SMS – continually create new attack surfaces for fraudsters to exploit.

Embedded network vulnerabilities

Some telecoms networks have inherent weaknesses that make them susceptible to certain types of fraud. For example, a network's signaling protocol may lack appropriate security mechanisms. More commonly, most networks have insufficient threat monitoring and vulnerability assessments. These act as openings for fraudsters to enter.

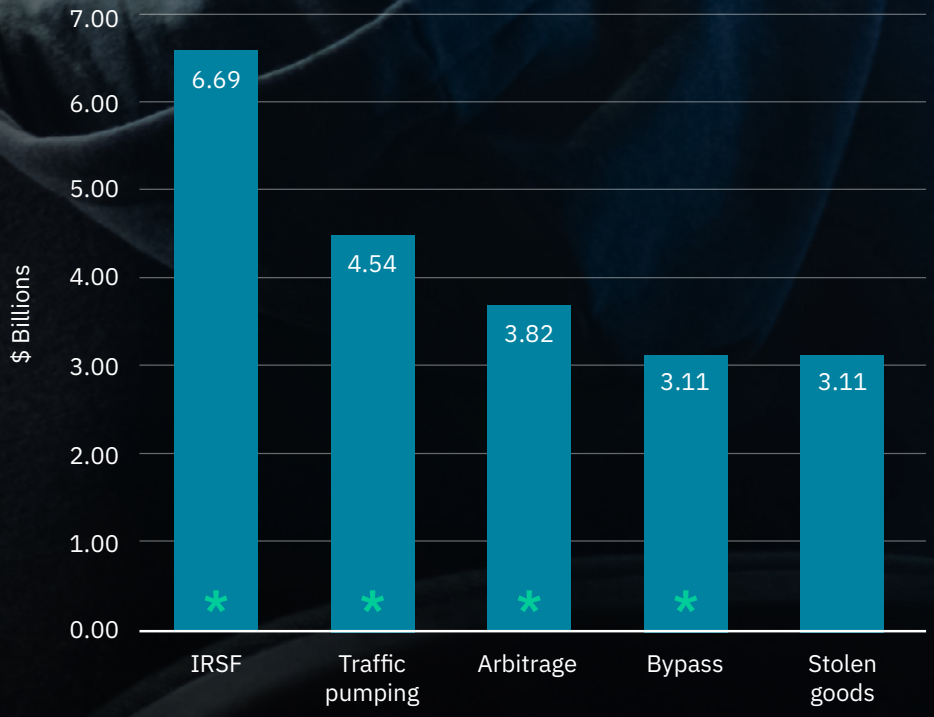
International telecoms fraud cost telcos on average **2.22%** of revenues in 2020
(up from 1.79% in 2019)

Aggressive, multi-service attack types are **posing new threats**

Roaming acts as an accelerator for losses **(50% of IRSF losses happen while roaming)**

Drastic increase in CLI spoofing and spam attacks across services

Complex, interconnected networks and telecoms services **create new vulnerabilities**



Source: CFCA 2021 Fraud loss survey

* International

Combat fraud with a multi-dimensional, multi-service approach

With such a range of fraud types, a reactive or piecemeal approach is not enough. Telecoms operators need proactive, 24/7, comprehensive fraud protection that proactively stops both existing and emerging fraud types before they can enter the network.

BICS is globally recognized for its fraud and security solutions in the telecommunications domain, offering total protection from:

- All types of international voice and messaging, and both inbound and outbound roaming frauds.
- Signaling threats that exploit network vulnerabilities across SS7, Diameter, and GTP technologies.

Enhance your security setup with BICS

Comprehensive fraud prevention across voice, messaging, signaling, and roaming

Proactively blocked more than 850 million fraud attacks

Saved customers more than €2.1 billion

Blocked 14 million fraud attempt per quarter (excluding robocalls)

Crowdsource intelligence from more than 2,200 market players

BICS fraud prevention hub

Combining technology, expertise, and advanced threat intelligence

Advanced threat intelligence

Identify global fraud trends worldwide by analyzing millions of internal and external data points. With the world's largest threat intelligence database, our platform uses crowdsourcing to detect emerging fraud patterns, compromised numbers, and vulnerabilities.

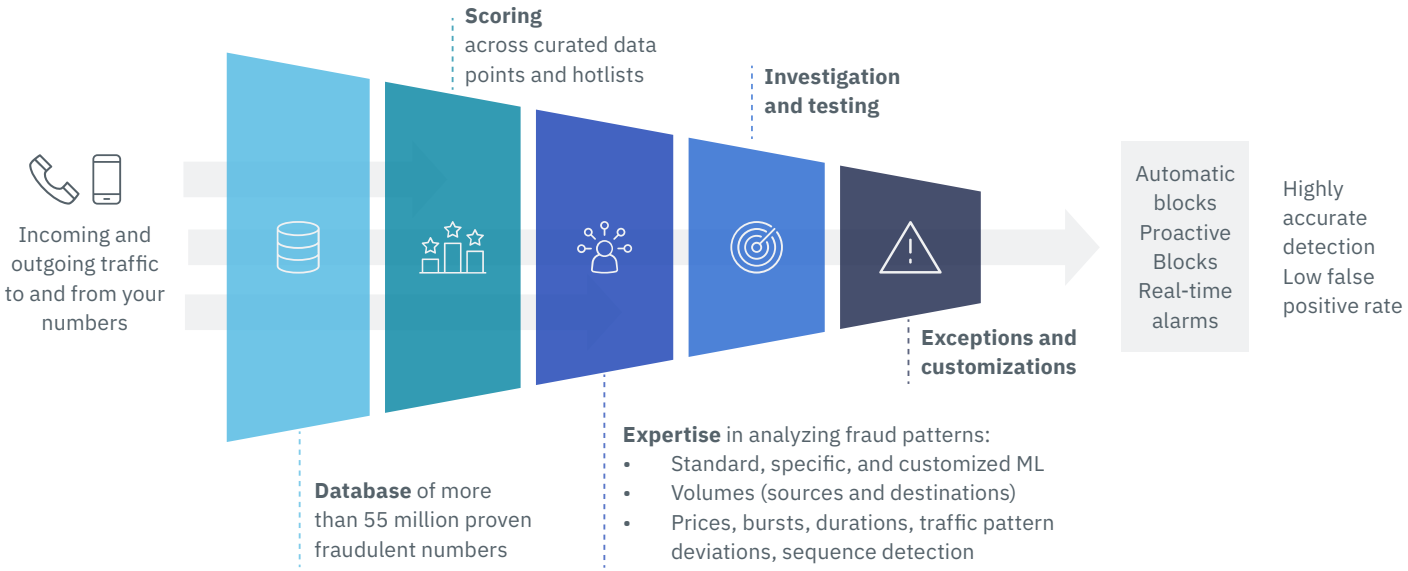
Technology

Thanks to state-of-the-art technology, using machine learning models, we offer proven solutions that secure your network in near-real time from both existing and new types of threats.

Expertise

With the help of our cross-domain and cross-service specialists, you can build comprehensive 24/ 7 monitoring into your business. We enable you to integrate fraud detection into every part of your business.

How BICS fraud prevention solutions work



☆☆☆☆☆

"Safeguarding our revenue from fraudulent activity and protecting our customers' user experience is a major priority at Swisscom. Reinforcing the focus on fraud protection, Swisscom has chosen the innovative FraudGuard service from its long-standing partner BICS to help block fraudulent international call attempts, in and out of our network proactively as an additional benefit to the other functionalities of the solution."

Reto Meier
Fraud Manager at Swisscom

Voice fraud prevention

BICS offers innovative and proactive voice fraud prevention services for mobile operators who want to protect their networks from fraud on international voice traffic.

Proactive prevention of both inbound and outbound fraud related to international voice

Near-real time traffic monitoring, mitigation, and alerting of ongoing threats

Protection from known fraud numbers and patterns based on the BICS' threat intelligence database

90%-95% of fraud attempts are proactively blocked

Auto-barring to drastically reduce fraud run-time

No call degradation

Protect from:

- AIT, International Revenue Share Fraud, and PRS fraud
- Refilling and CLI manipulation
- Spam, Wangiri, phishing, smishing, robocalling
- Hacking of infrastructure to generate fraudulent calls, call hijacking, IRSF, AIT
- Call bypass

SMS fraud prevention

BICS SMS fraud prevention solutions provide protection from all types of SMS fraud, including monitoring of SMS traffic, and identification, detection, and blocking of fraudulent messages.

- Protection and control for all SMS streams
- Hosted or on-premise SMS interoperability model for legitimate termination of traffic, filtering out grey and black routes
- Advanced SMS firewalling capabilities for incoming and outgoing traffic, and blocking SMS spam or malware
- Protection for both A2P and P2P traffic

Protect from

- Spam, Wangiri, phishing, smishing Loss of personal information and money
- Malware and malicious apps in handsets to obtain personal data and generate SMS
- 2FA SMS interception and spoofing of end consumers
- Revenue loss from A2P and P2P SMS bypass (also through malware and apps)
- International Revenue Share Fraud

Roaming fraud prevention

Roaming has become a preferred vehicle to carry out international telecoms fraud, because it introduces delays in fraud detection that may last anywhere between 4 hours and 3 days, until reconciliation takes place. BICS blocks fraud attacks in real time while analyzing global traffic in near-real time. This creates a complete overview of fraud trends and minimizes possible fraud.

Protection and control over fraud beyond the operator's network boundaries

Increased control over the activity of outbound roamers including the ability to define where they can call to based on where they are roaming from

Two-level approach to cover 99.5% of fraud events:

- Real-time fraud prevention and monitoring via CAMEL signaling
- Near-real time fraud monitoring via NRTRDE and TAPfile analysis

Protect from

- AIT, IRSF and PRS fraud
- Voice and SMS International Revenue Share Fraud
- Fraudulent service acquisition

Protection from signaling attacks

The interconnected nature of mobile networks makes them particularly exposed to international threats. As a result, signaling attacks and fraud can cost operators hundreds of thousands of dollars each year. They can impact the network infrastructure and the wholesale business, and affect subscribers, businesses, and mobile operators. A signaling attack can be very damaging to brand reputation.

Mobile subscribers – corporate, consumer, and IoT – are the target of a growing number of signaling attacks that take advantage of vulnerabilities on the operator network. Spying and tracking, as well as hacking into bank and social media accounts, have been publicly reported, but signaling fraud also powers other fraud types such as voice and SMS frauds.

BICS offers an advanced telecoms intrusion detection solution and protection against signaling threats on 2G, 3G and 4G interworking.

Telecoms security expertise to assess, define, and build network security

Comprehensive range of signaling and IPX security solutions for 2G, 3G, and 4G interworking

Experience-based best practice covering SS7, diameter and GTProaming interworking.

Protect from

- Signaling attacks
- Location tracking
- Call and SMS interception
- Denial of Service on networks and subscribers
- Wholesale frauds
- Spam, spoofing, impersonation, and more

Consultancy and expertise

Tackle telecoms fraud globally with consultancy services from an experienced team with cross-domain expertise. Audit and test international threats with machine learning, crowdsourcing, smart data correlation and data mining. Benefit from industry best practices, the knowledge and expertise stemming from more than 15 years' experience working with global MNOs to manage managing international telecoms fraud.

Our consultancy services can assist with all types of voice, messaging, roaming, and signaling fraud, including: IRSF exposure analysis on voice and messaging, SMS bypass, network penetration testing, and more. Our vulnerability assessments take a comprehensive view of your network and its attack surface for different generations of mobile technology, use cases, and interworking strategies to provide you with a holistic view of threats and how to prevent them.

Extend your vigilance and response to fraud events even outside of office hours, during night shifts and weekends. Gain confidence with follow-the-sun support and expertise, complete with real-time request acknowledgement. Our operations center works round the clock, 365 days a year, to ensure that your protection never falters.

Why BICS for telecoms fraud prevention?

Our solutions protect your network, customers and revenues from fraud and hackers in real time, combining crowdsourced intelligence and traffic analysis using ever-evolving machine learning models to keep abreast of the latest threats. All underpinned by expert consultancy and turnkey custom fraud prevention solutions tailored to your needs.

- **Comprehensive range of fraud prevention and protection solutions**
  Our fraud prevention solutions leverage our unique cross-domain intelligence and cross-platform capabilities.
- **Detect fraud on both your own and partner networks**
  Our monitoring services, which cover more than 700 operators globally, provide extensive reach and depth of data. Allowing you to benefit in near real-time from unrivalled visibility of attacks on telecoms network at a global scale.
- **World's largest threat intelligence database**
  Keep traffic from more than 55 million known fraudulent numbers out of your network. Our global threat intelligence database is constantly updated with qualified information gathered globally from ongoing attacks.
- **Easy-to-access hosted model**
  Simplify rollout with a hosted deployment model that combines zero upfront capital expenditure, ease of implementation and fast time to results.

Focus on your core business. Our solutions, backed by our state-of-the-art fraud operations center, act as seamless extensions of your fraud management team. Stay protected round the clock, while streamlining the time, resources, and staffing required for fraud prevention.

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

bics