



BICS FRAUD PREVENTION SOLUTIONS

Proactive approach to prevent international and roaming voice fraud

Fraud in international traffic

Since international fraud incidents take place using sophisticated techniques within the home network or when roaming, fraud events are almost impossible to stop before revenue losses and reputational damage have already occurred. The fraud management approach driven by detection – causing inherent delays – have always created opportunities for fraudsters.

- Lack of control over cross-border traffic
- A siloed view limits visibility of fraud incidents outside of network boundaries
- Increasingly sophisticated fraud methods used
- Fraud is a multinational business
- Jurisdiction limitations
- Delayed availability of call data in roaming

Impacts of International telecoms fraud

Financial impact

- International telecoms fraud costs operators over US\$18 billion annually
- Losses amount to 1% of global telecom revenues
- While roaming, a single fraudulent SIM has shown to generate 18 hours of traffic and revenue loss of US\$4,800

Other business impacts

- Bill shock, subscriber dissatisfaction and churn
- Pressures on infrastructure and customer services
- Privacy breaches and regulatory repercussions
- Reputational damage

Prevent all types of international voice telecom fraud

BICS fraud prevention solutions for international voice and roaming are effective against all types of fraud tied to them, including, but not limited to:

- International revenue share fraud
- Wangiri
- Artificial inflation of traffic
- Arbitrage exploitation
- Premium rate and high-priced destination exploitation
- PBX / IPBX hacking
- Malware originated calls
- Bypass detection and prevention





The network behind the world's top networks





BICS FRAUD PREVENTION SOLUTIONS

Proactive approach to prevent international and roaming voice fraud

BICS Crowdsourcing Platform

BICS sits at the heart of global mobile communications, giving it a unique and global multi-network view of quality of international traffic.

 **One in ten** of all international voice calls pass through BICS network

 **25%** of all international roaming signaling passes through the BICS network

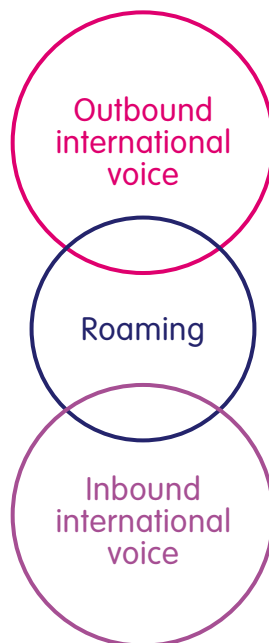
BICS innovative crowdsourcing platform uncovers new fraud attacks ongoing within global international traffic and feeds the intelligence into its fraud prevention solutions for international voice and roaming. This serves as a powerful weapon to not only detect, but also proactively block the majority of international voice telecoms fraud.



BICS international and roaming fraud solutions have blocked over **600 million** fraudulent call attempts in less than five years, saving our customers over **US\$2.2 billion.**

Proactive protection through Fraud Intelligence Repository

Crowdsourcing powered with details of over 50 million known fraudulent numbers collected across our global base of over 1,200 partners. By matching numbers against the database, BICS fraud prevention solutions can identify and automatically block calls from and to any known fraudulent number.



What our customers say...



"...the service has provided great benefits to Swisscom in terms of protecting against international fraud incidents and limiting financial exposure..."

...BICS is a committed and reliable partner and we highly recommend their FraudGuard Fraud Protection services..."

Marcus Schranz, Carrier Relation Manager



"Protecting revenue from fraudulent activity is a key priority for Bouygues and we have already reaped the benefits from adopting BICS FraudGuard platform, with over 200 fraud attempts blocked at the start of this year and no incidences of legitimate calls being prevented – all with minimal input from our operational team."

Thierry Nedellec, Wholesales Manager



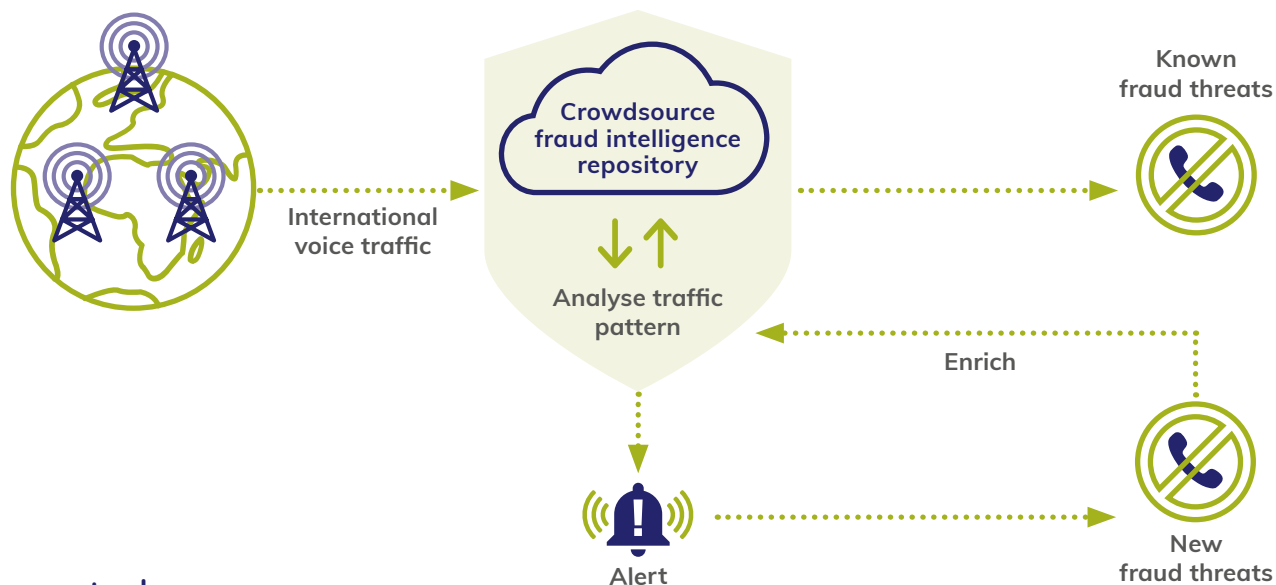


FraudGuard is our international voice fraud prevention service. The solution can automatically block all calls to **known** fraudulent numbers. In addition, our team of fraud experts can identify, investigate and block potential new fraud incidents proactively.

Key features

- Traffic surveillance for detection and prevention of international fraud
- Proactive blocking of more than 50 million field proven fraudulent numbers
- Automated identification and blocking of new fraudulent activity
- Crowdsourced, unique multi-network aggregated view of fraud trends
- Analytics capabilities for transparent reporting and tracking
- 24/7 fraud expert surveillance and support

How it works



Case study

Traffic Monitored	Fraudulent Call Attempts Blocked	Fraudulent Wholesale Exposure Prevented*	Traffic Cost Reduction
62 million minutes	1 million	US\$5.1 million in less than 2 years*	Around 25% of total traffic cost to the operator

* Based on a conservative calculation of potential wholesale exposure prevented



The network behind the world's top networks



BICS VOICE ROAMING FIREWALL WITH FRAUDGUARD NRTRDE

Proactive prevention from roaming voice fraud

It's particularly difficult for the home operator to detect roaming fraud as it does not originate on the home network. In the best cases, the home network has to wait three to four hours until the fraud traffic is visible through a NRTRDE file.

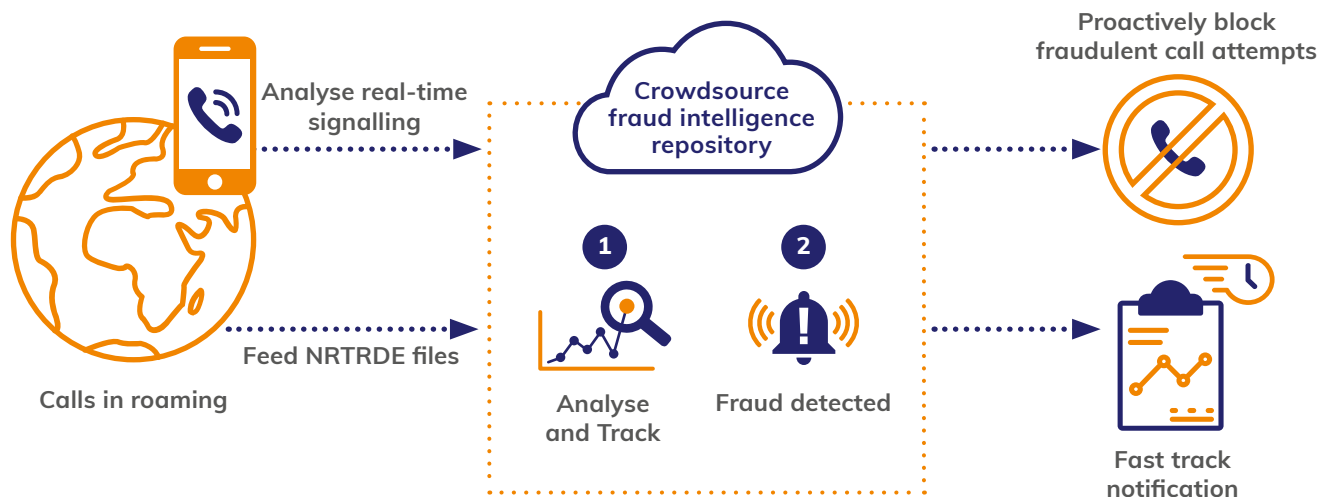
The BICS Roaming Fraud Protection puts the home operator back in control, using the BICS Fraud Intelligence Repository alongside CAMEL signalling to identify and block fraud attempts within outbound roaming voice traffic, so fraudulent calls are shut down before they happen.

Key features

- Real-time visibility of roaming voice traffic for CAMEL enabled visited mobile networks
- Proactive blocking of all traffic by proven fraud numbers
- Automated identification and blocking of voice fraud traffic to new fraud numbers based on real-time analysis of multi-network traffic
- Global view of fraud trends for comprehensive protection
- 24/7 expert surveillance and support

Also, for non-CAMEL enabled visited mobile networks, BICS Roaming Fraud Protection uses NRTRDE files to provide extremely early detection of fraud incidents delivering fast-track alerts to operators, with comprehensive reporting.

How it works



Case study

BICS Roaming Fraud Protection*	Fraudulent Call Attempts Blocked	Fraudulent Roaming Exposure Prevented*	Proactive Blocking Success Rate
Over US\$700,000* saved in 4 months	Over 123,000	Potentially over US\$700,000* saved in 4 months	93%
(A large European MVNO)			in CAMEL-enabled visited mobile networks

* Based on a very conservative assumption for roaming exposure prevention calculation