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.

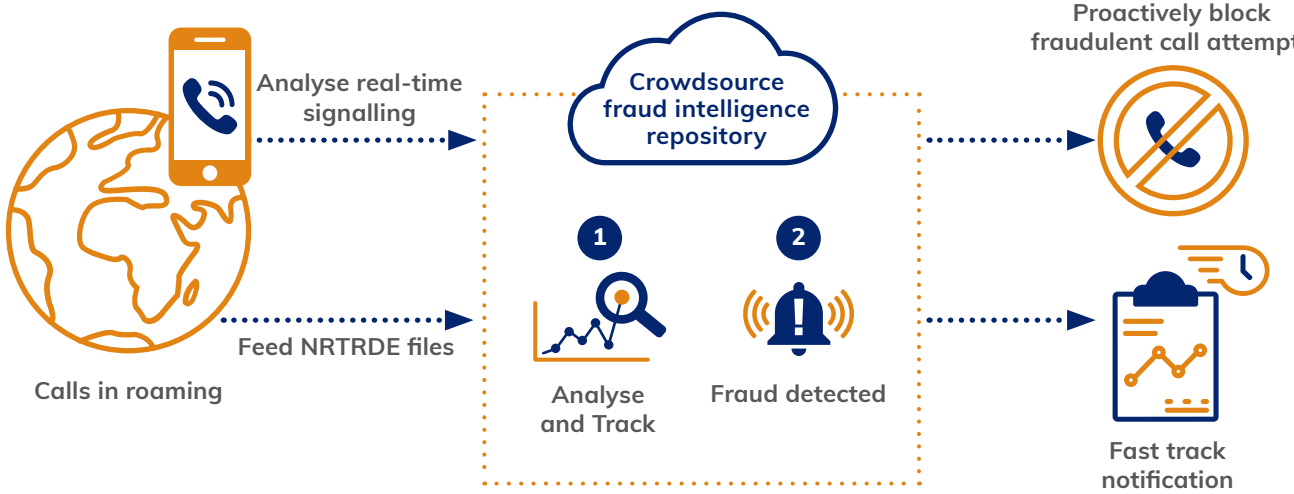
The BICS Roaming Fraud Protection puts the home operator back in control, using the BICS Fraud Intelligence Repository alongside CAMEL signalling to identify and block fraud attempts within outbound roaming voice traffic, so fraudulent calls are shut own before they happen.

## 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 (A large European MVNO) | Over 123,000 | Potentially over US$700,000* saved in 4 months | 93% in CAMEL-enabled visited mobile networks |

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