Voice SafeGuard

Product Introduction

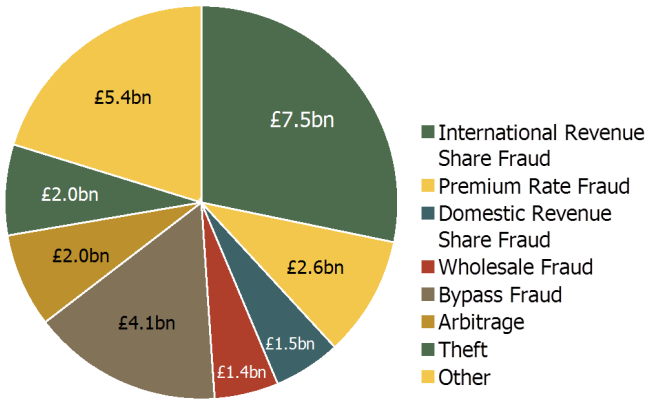
According to the Communications Fraud Control Association's 2015 fraud report, global losses attributable to telephony fraud are estimated to be £26.5bn or 1.7% of global telecom revenues. Of this, they estimated £7.5bn was due to International Revenue Share Fraud - making it the most common type of fraud.

Network Operators need to protect against these losses especially when surveys indicate that customers see fraud prevention as an increasingly important factor when making a decision about their choice of network operator.

Telsis Voice SafeGuard offers a proven, industry leading solution to protect your network from fraud in real time before it becomes a costly problem.

Telsis Intelligence for Your Network

Telephony fraud is evolving rapidly. In the past, criminals had to trick users into performing some action that allowed the fraud to take place. As we move into the world of IP telephony new techniques are being developed by fraudsters that no longer require any user intervention. As a result, customers may not spot the fraud until a large bill from the operator drops through their door.



Source: CFCA

Of the many types of telephony fraud, International Revenue Share Fraud (IRSF) accounts for almost one third. An increasing proportion of IRSF is due to PBX and residential VoIP device hacking.

International Revenue Share Fraud (IRSF) is a type of premium rate fraud, where calls are made to premium rate numbers across international boundaries. The fraudster makes a call to a premium rate number which they own in another country. They then take their share of revenue for running the premium rate service.

As the demand for the remote administration of devices increases, so do the risks; for instance unchanged default passwords or bugs in the user interface code can easily lead to unauthorised access to a PBX. Once unauthorised access is gained a fraudster can place calls that generate huge costs in just a few hours.

Although contractually the cost of any calls made as a result of PBX hacking may be attributable to the company running the PBX, it is often in the Network Operator's interest – for business and adverse brand name publicity reasons – to come to an agreement to bear some or all of the costs.

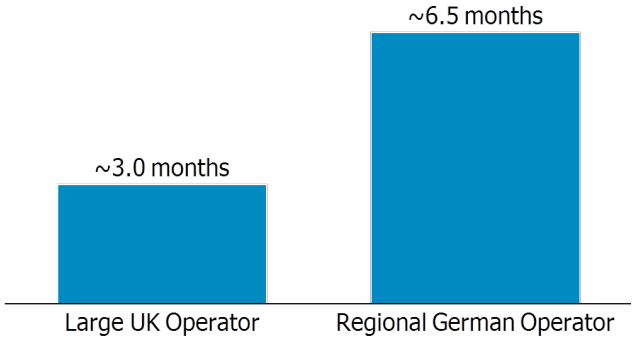
Telsis Voice SafeGuard allows Network Operators in real-time to monitor calls, identify patterns that may indicate that device has been hacked and is committing IRSF or other types of fraud.

Once a source of fraud has been identified, the Network Operator's fraud team can either be alerted and/or calls can be automatically blocked.

Voice SafeGuard is a comprehensive and scalable fraud prevention solution:

- Proactively blocks or **tears down fraudulent calls in real-time** (versus reactive checking of CDRs after the fraud event)
- **Protects against International Revenue Share Fraud, Domestic Revenue Share Fraud, Premium Rate Fraud, Wholesale/Interconnect Fraud** and other types of fraud
- Ability to **customise fraud thresholds** by destination, country or carrier
- Strong business case with an **attractive payback period** (see below)
- **Rapid and non-intrusive deployment** in less than 4 weeks (hosted or non-hosted)
- **Integrates easily** into any network (SIP, SS7 INAP) and with leading vendor platforms (Huawei, Nokia/ ALU, Ericsson, Siemens, etc.)
- **Available with flexible commercial models** – capex or opex

Recent deployments - payback period



Contact: contactus@telsis.com

UK
T: +44 (0) 1489 76 00 00

Germany
T: +49 (0) 6151 827 850