squire technologies

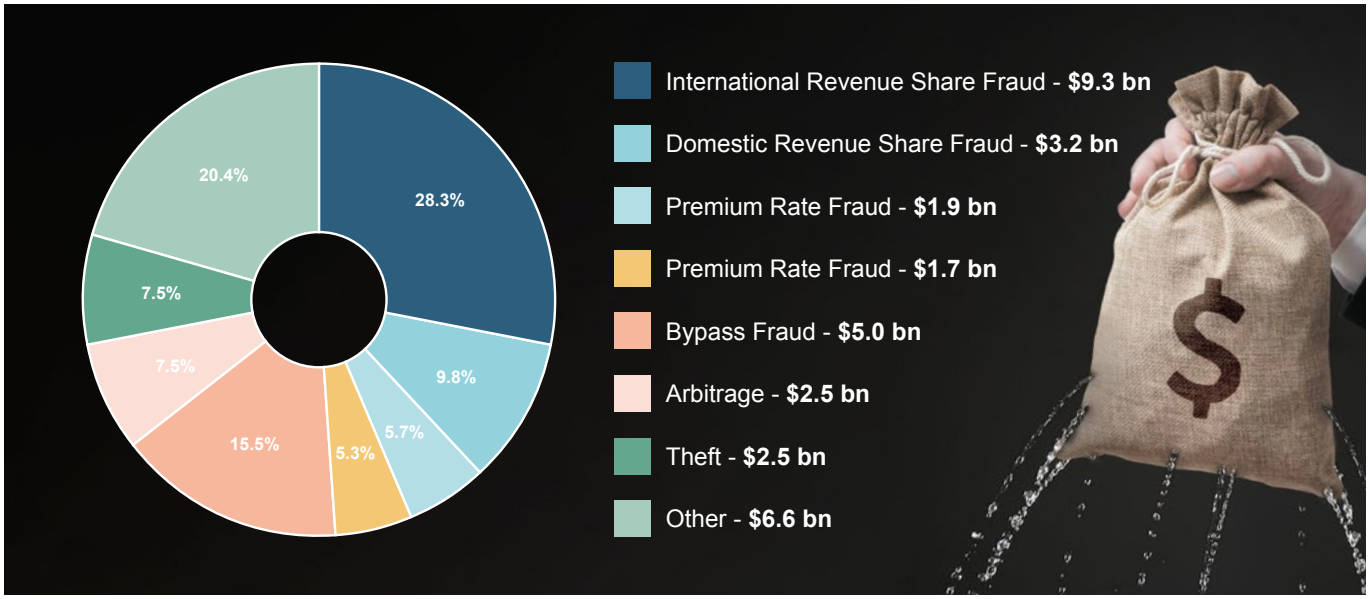
WINNING THE WAR ON TELECOM FRAUD

No mobile operator is immune to the threat of fraud, and one global expansion that's defying any recession, competition or pandemic, is telecoms network fraud.

With increasingly sophisticated ways to avoid detection, telecoms fraud is now one of the primary sources of revenue leakage. Operators are currently sharing billions of dollars in profits with fraudsters, a trend that is only set to rise as the ubiquity of all IP networks takes hold.

What was once quite a limited avenue for fraudsters is now big business, and often seen as a low-risk alternative to traditional methods of financial crime.

The impact that telecoms fraud has on consumers, and the scale of the challenge, is reflected by industry bodies like the GSMA operating their own working-groups, who liaise directly with intelligence agencies like Interpol, illustrating how seriously the industry is taking the problem.



Telecom fraud is an ever-present drain on profitability and operators have long tried to limit the losses that it inflicts upon them. However as well as hitting an operators bottom-line, fraud has a far wider impact by critically affecting customers quality of service. This in turn damages the value of a brand and stifles its ability to promote development through mobile connectivity.

- **Revenue Leakage**
  Fraud directly affects the bottomline, and the operating margins of your business
- **Loss of Brand Value**
  Telecom fraud leaves lasting effects upon your brand awareness and reputation with customers
- **Customer Churn**
  Customers tend not to contest small losses and QoS issues - instead they opt to leave upon contract renewal
- **Company Valuation**
  Loss of brand reputation and customer numbers directly impacts your company valuation
- **Service interruption**
  Operators face greater challenges rolling out new and innovative services as a result of fraud
- **Proceeds of Crime**
  Proceeds from fraud are frequently used by organised crime and terrorist networks all around the world

The Traditional Approach Failing Telecom Operators

All too often the losses from telecoms fraud have been viewed as part and parcel of the industry. Twenty years ago losses were negligible, while calls where carried over TDM networks dependant upon specialist hardware that is inherently difficult to attack and defraud.

While these networks have evolved around IP, thus losing this architectural safety net, operators attitudes and their ability to counter fraud has not, remaining largely reactive, as opposed to being proactive.

Traditional 'reactive' methods largely orientate around spotting fraudulent activity via large scale monitoring platforms, followed by recouping losses after the event. This approach does little to appease and retain customers, not to mention deter fraudsters.

What is required is a multi-layered approach. Seeking solutions that can intelligently identify fraud in real-time to provide network managers the opportunity to rapidly provision counter measures is what is required to have the edge over the criminals.

At Squire Technologies our fraud prevention solutions play a crucial part in that multi-layered approach to reducing the losses from telecoms fraud.

The New Approach to Fraud Prevention

MavenShield provides telecom operators with a highly flexible real-time method of countering network fraud.

Designed to sit outside any service affecting critical-path, the MavenShield Fraud Prevention Gateway enables users to interrogate network components and resources to rapidly identify fraudulent behaviour. Upon the detection of threats, remedial counter-measures can be provisioned, such as session tear-down, forwarding, redirects and transfers etc.

MavenShield seamlessly integrates with deployed network monitoring platforms, providing operators with a formidable weapon in the fight against fraud.

- Real-time fraud prevention increases overall cost savings
- Helps to reduce customer churn
- Fully integrates with existing network monitoring solutions
- Network agnostic, 3G, 4G, 5G, supports HTTP/2, all Diameter, SIP & SS7 networks
- Enables rapid response to new threats
- Allows operators to proactively combat network fraud
- Non-intrusive real-time solution
- Deployed in a non-critical path of the core network
- Fixed, mobile or virtual networks
- Compliant with GSMA FS.24 CAMEL Roaming Fraud Management Handbook.

Another Tool in Your Anti-Fraud Toolkit

Multi-layered strategies are crucial to winning the fight against telecoms fraud, and MavenShield is designed to complement existing solutions. Adding speed and remarkable flexibility, it seamlessly integrates with Big Data platforms, BSS and Business Intelligence systems, via comprehensive API support.

Squire Technologies network solutions have been deployed by global vendors, telecoms operators and security agencies. With two decades of providing signalling know-how to the telecoms industry, and a speciality in legacy protocol technology we're well placed to help you combat the ever increasing threat of telecoms fraud on your business.

For more information about our MavenShield Fraud Prevention Gateway, and our complete range of core network products call our team today on **+44 1305 757314**