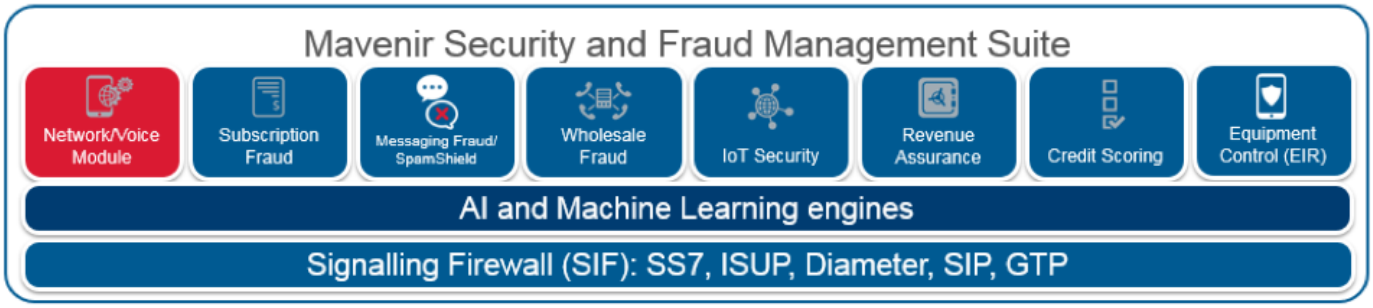
Network / Voice Module



Network Usage fraud can be extremely costly to an operator, requiring a quick and flexible detection strategy.

Revenue Share Fraud:

Fraudsters may seek to generate revenue by driving traffic towards a revenue share number they possess that is likely premium rated and international located in a country prone to fraud.

Example: Subscription Fraud:

Fraudsters call their revenue share number themselves. The Fraudster uses a phone that can't be traced, likely involving subscription fraud with fake IDs /stolen credit cards /account takeover, with no intention of paying the bills. Fraudsters will use this post-pay connection to generate calls. These calls can be made with a SIM box, hacking a PBX, or spoofing the CLI (subscriber number) of the outgoing number to delay detection.

Example: Wangiri Fraud:

Fraudsters entice others into calling the revenue share number. The number itself will call thousands of innocent subscribers, leaving missed call or SMS notifications. Subscribers often call back this number without realizing it is fraud. This fraud type doesn't usually have a significant cost for Operators, however it typically a large effect on the victims' operator brand. Wangiri Numbers are often carefully chosen to appear to be a local call and not an international call.

The need for Machine Learning:

Traditional detection approaches fall short such as Rule and threshold alerts based on high usage which fraudsters may learn over time and stay under to avoid detection and traditional Fraud systems typically struggle to detect Wangiri, as they usually operate on a 1-to-1 approach. Therefore, alert thresholds are set very low leading to high false positives.

Revenue Share fraud often occurs in combination with other sophisticated fraud methods, making it even more challenging to detect, such as: PBX Hacking, Roaming Fraud, Wangiri, Subscription Fraud, SIM box Fraud, Bypass Fraud, Stolen Handsets, Arbitrage, CLI Spoofing…

Machine Learning Approach:

A bespoke model is built based on the specific network to understand common calling patterns, destinations, times of day, frequency and typical behavior. Future traffic is scored against this constantly updating baseline to identify ‘anomalous’ traffic.

Not all anomalous activity is fraud, but all fraud is an anomaly on a network. This allows Machine Learning to detect new and future types of fraud that don’t exist yet

Enhancements with customer data possible to allow segmentation based on new/established customer or based on segment like prepay / post-pay / corporate usage

Use Case - Tier 1 European Operator

Compared to existing system, Mavenir detected:

163% more fraud

47% less false positives

2 days 9 hours faster detection (known attacks)

=Predicted savings: US $ 1.65M

*Source: Operator based on the loss experienced, and the estimated time savings due to Interconnect loss reports