







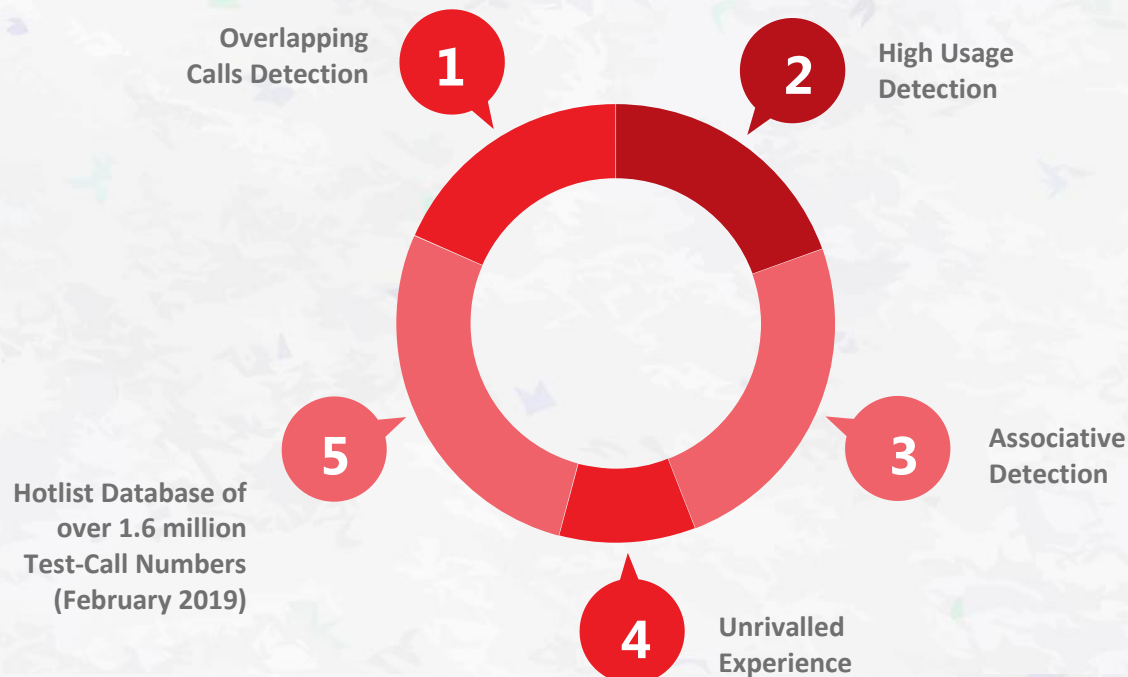
Powered by 

International Revenue Share Fraud (IRSF) is the telecommunications industry’s number one fraud problem, costing telcos billions of dollars in fraud losses each year. Despite great work by telcos and supporting organisations over the past 9 or 10 years, the problem remains, and is likely to remain for the foreseeable future. In 2017, the Communications Fraud Control Association (CFCA) commissioned a report showing that IRSF accounted for over \$6.10 billion of losses in that year alone.

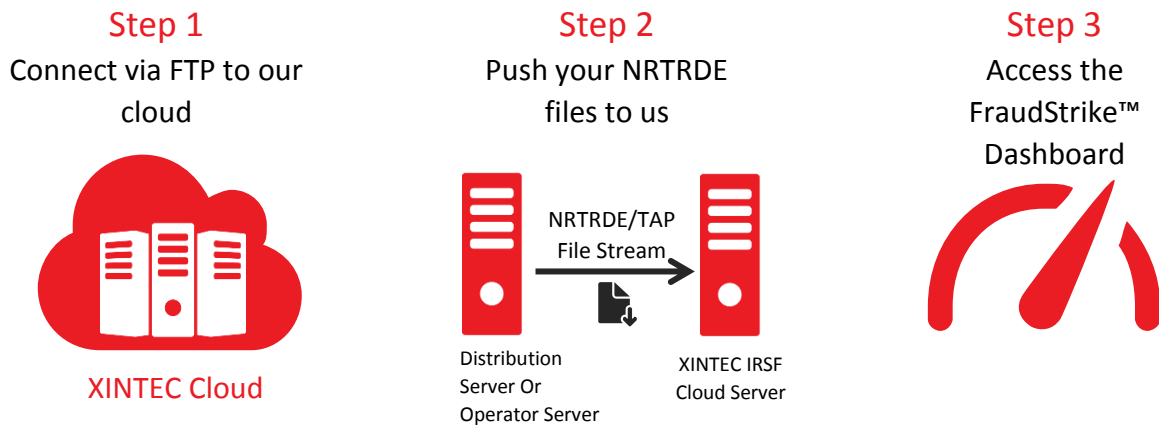
**FraudStrike™** is a specific package of complementary detection techniques and IRSF test numbers to directly target IRSF throughout the telecoms industry. Just some of the instant benefits include:

-  Early detection and prevention of IRSF incidents
-  Clear visualisation and easy analytics to enable case resolution
-  Flexible business-wide reporting for all user levels
-  Light-touch integration for minimal disruption to existing IT environments
-  Fully configurable, modular and scalable architecture that is easy to install and operate
-  Compliance with global industry standards and best practice in relation to fraud protection

**FraudStrike™** is made up of five components, rolled into one software package.



## How does it work?



**Step 1:** Customer connects via FTP to our dedicated secure server.

**Step 2:** Customer pushes the NRTRDE IN files to this server. The customer can also send NRTRDE OUT/TAP OUT files if they wish to monitor inbound roamer activity.

**Step 3:** XINTEC provide the User with login access to the Customer's own instance of the software containing the real time alerts, associated drill-down capability to xDRs from these alerts, along with various roaming reports. Users will also receive real-time emails as alerts are generated.

