International Revenue Share Fraud

BIG DATA SOLUTION: INTERNATIONAL REVENUE SHARE FRAUD IRSF

Overview

International Revenue Share Fraud (IRSF) is one of the most menacing frauds plaguing the telecom industry. IRSF is caused by the artificial inflation of traffic or traffic pumping to the premium rate numbers in the world. Datanomers' International Revenue Share Fraud tool is a big data analytical solution that detects International Revenue Share Fraud (IRSF) and remediates it in near real time which will avert huge financial losses for enterprise customers, mobile operators, service providers and wholesale carriers.

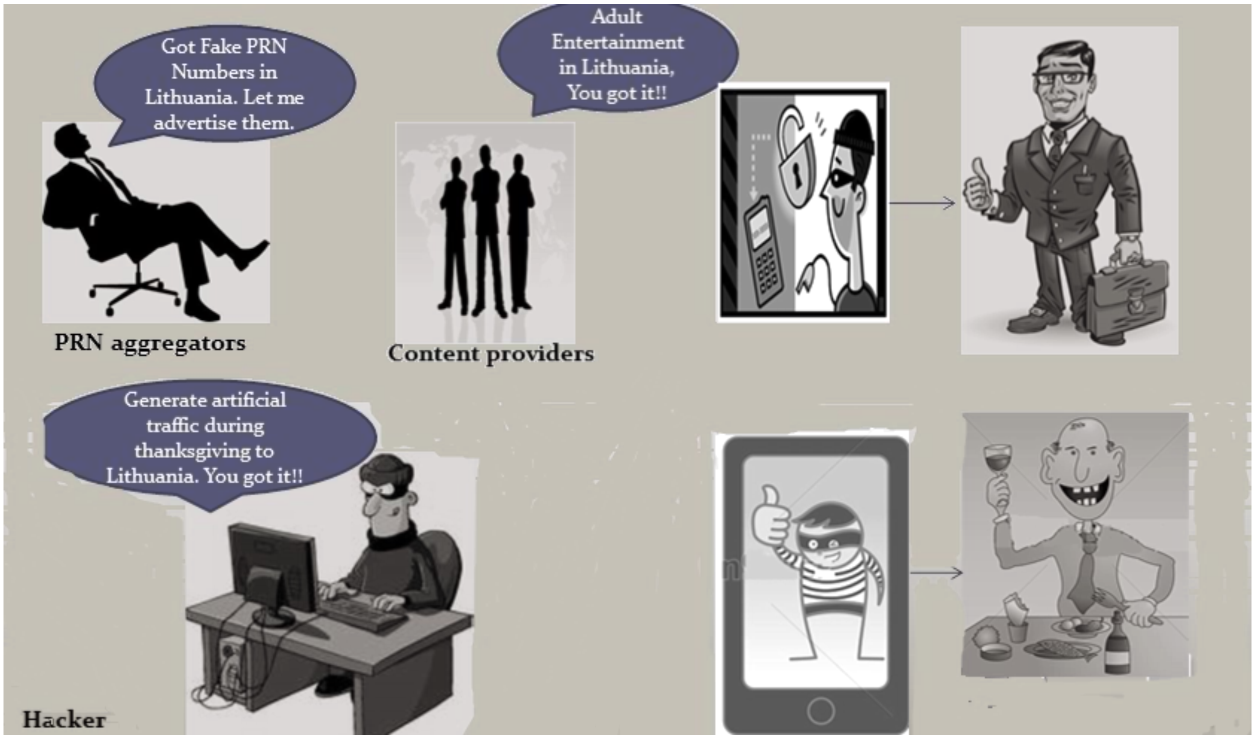
The Challenge

According to the Communications Fraud Control Association (CFCA), telecom industry lost close to $4B billion to revenue share fraud.

Typically IRSF involves a nexus between the following.

- PRN (Premium Rate Number) Aggregators: who obtain range of fraudulent premium rate numbers (PRN) countries like Lithuania, Sao Tome and enter into an agreement with service providers falsely claiming entertainment services.
- Hackers or the fraudsters who generate traffic. They either hack a PBX of a company, or clone SIM cards and generate millions of artificial calls to premium numbers.

Hackers and the revenue share providers share the revenue generated by the fraudulent calls which will be billed either to the end customer or some carrier in the routing flow.


Got Fake PRN Numbers in Lithuania. Let me advertise them.
PRN aggregators
Adult Entertainment in Lithuania, You got it!!
Content providers
Generate artificial traffic during thanksgiving to Lithuania. You got it!!
Hacker

- The alarming fact about IRSF is that it is triggered by many other means of fraud like PBX hacking, SIM card cloning, International roaming fraud, subscription theft.
- These premium rate services are the eternal cash cow for the telecom carriers and they are more than willing to buy premium rate services without sufficient checks and balances to distinguish between a rigged and a genuine player.
- The delays in identification of the nature and volume of the calls, delays in blocking the numbers makes IRSF extremely difficult to detect and combat.
- The final straw is the nature of the carrier model, the money transfer has already been done to fraudulent providers who cannot be traced after the fraud has been discovered.

The Solution

Datanomers has come up with the state of the art big data analytical solution that detects and remediates IRSF in near real time. Below are

Features	Datanomers Solution	Competitor Solutions
Accuracy	95% Accuracy Patented Algorithms Advanced Statistics like Central Limit Theorem, entropy of random variables Industry Expertise	Rely heavily on industry expertise and hot lists of premium service ranges Elementary Statistics Pre-defined patterns which generates a slew of False positives
Coverage	Low Grade IRSF and Blended IRSF are caught in near real time.	Pre-defined pattern to detect

	Advanced Machine Learning working off the 200-300 million CDRs Algorithms based on Covariance , K-Mean clustering of random variables Low-Grade IRSF, Blended IRSF is caught and alerted	Missed True positives
Remediation	Auto-Removal/blockage of fraudulent ranges in near real time ACTIONABLE INTELLIGENCE	Delays in detection and remediation
Evidence	CDR(Call Detail Record) Repository stores fraudulent CDRs as irrefutable evidence	No CDR evidence for missed true positives and wrong CDRs for false
Scalability	Scalable solution based on big data analytics	Questionable scalability
Process Improvement	Email/SNMP notification Better Operations KPI Better SLAs	Operations team work with a myriad of tools and troubleshooting is slow and tedious
IRSF Dashboard	Customers get a peek on how well fraud is kept under check Rich set of reporting	Basic Reports

In a nutshell Datanomers’ IRSF solution helps you to Grow business strategically with a quality message. Big deals on the anvil rely on this. Quality is going to be the key in the years to come and Datanomers will help you be the game changer.