Time to review your Telecom Fraud Strategy

Fraud has now become a major headache, directly and heavily impacting the EBITDA margin of the operating companies. Do you have the right strategy in place to tackle the problem?

Competition in the digital world forces service execution to be simple and seamless. But is it also secure? On the other hand, fraudsters are becoming knowledgeable, versatile and inventive in the way they perform fraud. Having the same tools and equal access to technologies, fraudsters can easily outsmart fraud systems that use machine learning algorithms. They start with testing routes and number ranges, remain silent for some time and then attack with immense power.

In the event of fraud, the operator shuts down the route or blocks the number. The extent of the damage done is proportional to the duration of the call times the tariff of the call destination. In addition, you cannot blame your fraud system vendor or your staff who maintain and improve fraud detection algorithms. Operators are reluctant to release the incident related information, but industry experts estimate IRSF accounts for more than $6 billion per year.

The debate in the industry lies between the predictive and preventive approach, to detect fraud when it starts or prevent it from happening at all. Modern methods using big data approaches incline towards the predictive method. Namely, to detect it on-the-fly, if a call is fraudulent and subsequently block it. Is it possible to block the calls at the source, where they originate?

> Is it possible to block the calls at the source, where they originate?

The solution is available and has been successfully applied in the market. The collection of valid number ranges, special number, Premium Rate Numbers, unallocated or fake mobile numbers (including their MCC/MNC, time zone, location information, valid length etc.) from all operator companies around the globe comprises the "big data" approach that already exists. It can be

applied in the operators' IN platforms, Fraud Management Systems, Switching or Real Time Blocking mechanisms.

MobileID is a daily updated database issued to the customer at least once per month with interim updates issued whenever significant changes are identified. MobileID provides 1.8 million number ranges currently covering over 245 countries and territories.

Nevapark and iconectiv, as trusted and neutral third party providers of registries, clearinghouses and interconnection services, are appropriately equipped to provide the telecom market with MobileID to meet the needs necessary to tackle telecom fraud effectively.

We are offering you a **Proof of Concept** that proves our assumptions true.

Contact us for an in-depth presentation of MobileID.

Contact details:
Angelos Noulas
Senior Consultant
E-mail: noulas@nevapark.com
www.nevapark.com