International Revenue Share Fraud (IRSF) – The on-going risk. (October 2012)

The opportunity for fraudsters to exploit some countries high termination rates, or inflate traffic into other high value numbers with the intention of sharing any revenue generated from this activity, has been a problem for CSP's for some years now. Many of these opportunities are created through number aggregator websites who openly advertise revenue share offerings to many countries, and invite visitors to their websites to register on-line and immediately start generating revenue.

Financial losses to the industry are high, estimated to be in the hundreds of millions of US dollars annually, with individual CSP losses frequently being reported in the regions of $US100,000 to $US5 million. Fraudsters who are involved in this activity are constantly searching for opportunities to access a CSP's network fraudulently to inflate traffic into these numbers. Some common methods used to gain this access include;

- Subscription fraud, including identity theft and account takeover
- PBX intrusion
- Number misappropriation (Hijack)
- Credit Card Fraud
- Mobile Malware
- Computer Virus
- Internal collusion (fraud)

The industry has been struggling to manage this particular fraud threat for many years however it continues. In 2009, there were 17 number aggregator websites offering revenue share services. In 2012 there are 41 sites, an increase of 143%, which is a strong indication that the problem is increasing. Fraudsters are constantly searching for a 'weak link', a CSP who does not have sufficiently robust controls to prevent them from using their network as an enabler for Revenue Share Fraud.

A worrying aspect to this fraud is the increasing incidence of a countries range being advertised on these number aggregator sites without the knowledge of the number range holder. These numbers are obviously being 'hijacked' and stopped short of the country to which the country code applies. This action adds further complexity to the fraud in that the number range holder then also becomes a victim to the fraud, when outside phone users making legitimate calls into the country cannot connect, or international operators block the Country when their country code is considered a high fraud risk.

There are some basic controls a CSP can take to reduce their risk to IRSF and these include;

- Remove the conference or multi call facility from a mobile connection unless specifically requested (Fraudsters frequently use this feature to establish up to 6 simultaneous calls)
- Remove the ability to call forward to international destinations, particularly 'hot' countries
- Utilise the GSMA 'Hot' number range list and/or request the PRISM IPR test number database from Yates Fraud Consulting Limited so known fraud numbers can be blocked and test numbers hotlisted
- Ensure NRTRDE or HUR's are monitored 24x7, preferably through an automated system
- Ensure NRTRDE or HUR's are delivered within the required timeframe if you are the VPMN
- Ensure up to date tariffs, particularly for premium numbers, are obtained from GSMA AA14

- Implement the BOIEXH (Barring of International Except Home) function for new, or high risk connections
- Consider implementing a low cost Fraud Management solution

For further advice, contact Colin Yates on colin@yatesfraudconsulting.com