



NEAR REAL TIME ROAMING DATA EXCHANGE – CURRENT SITUATION AND HOW WILL THIS BE IMPACTED BY EU ROAMING REGULATION 111?

Over 4 years have now passed since the 1 October 2008 date when all GSM operators were expected to implement NRTRDE and reduce the deadline for shifting the roaming fraud loss liability from the HPMN to the VPMN (down to 4 hours). Regrettably there are still many operators who are not NRTRDE compliant. Some of these may be technically compliant, however have not re-signed the AA14 documents with their roaming partners to initiate the 4-hour reporting period, preferring to retain the longer period as a way to manage their liability for fraud losses as the VPMN for late reporting.

There is little doubt that NRTRDE has been responsible for a reduction in 'roaming related' fraud losses for many of those operators and their roaming partners who are fully compliant, and those who have invested in the systems, processes and resources to effectively manage and analyse the NRTRDE files received. We still hear of some operators who are fully NRTRDE compliant, however have the incoming files dropping into a 'black hole' during out of hour working periods. A recent evaluation of IRSF impacting 3 European operators' found that almost 80% of this fraud occurred between Friday night and Monday morning when the Fraud team were out of the office. This was not by accident – the fraudsters had done their homework and were aware of this 'opportunity'.

The industry is being impacted more and more by consolidation and cost cutting, which is translating to increased staff cuts, many in the Fraud, RA and Revenue Risk areas. 24 x 7 monitoring functions are often those that suffer from these re-organisations so it is important to replace any reduction in this monitoring activity with cost effective automated fraud or RA tools.

NRTRDE was not designed to be a short term fraud management initiative. Roaming related fraud (particularly IRSF) continues to be a major fraud risk, and NRTRDE is the most effective detection mechanism to identify incidents before losses grow.

Reliance on NRTRDE will increase, and this could be likely in European Union countries as a result of the new EU Roaming Regulation III initiative. This introduces an obligation for mobile operators to allow their customers an option, as of 1 July 2014, to purchase roaming within the EU as a separate service. This is aimed at enhancing competition in the EU roaming market, and driving down costs (which will be regulated within the EU community and likely to be between Eur 0,21 and 0,24c per minute for outgoing calls). This provides the opportunity for new players to enter the roaming industry, including existing operators such as MVNO's to become an Alternative Roaming Provider (ARP). ARP's, who do not have their own networks are to be offered easier access to the roaming market, requiring network operators in other member states to grant them access to their networks at regulated wholesale prices. ARP's may also extend their roaming offer to include 'unregulated' destinations outside the EU.

This initiative will introduce some fraud risk, such as IRSF, international call forwarding and bypassing hot 'B' number blocking to name a few. Certainly the impact of this initiative on IRSF terminating within the EU will be interesting. Analysis of the GSM Fraud Forum High Risk Range list reveals that 16.3% of PBX, IRS and Wangiri fraud has terminated in either EU or EU acceding or candidate countries. It also shows that almost 80% of these fraud reports were from a source country located within these EU, acceding or candidate countries.

It is noted that the EU Roaming Regulation 111 High Level Technical Specification document clearly states that a visited MNO must make NRTRDE data available to the Home MNO in line with the current GSMA rules or become liable for any fraud losses suffered outside that reporting period. The Home MNO must then make these NRTRDE records available to the ARP in line with the same GSMA rules, or they then become liable for roaming fraud losses outside the reporting period (with slight modifications such as timing and inclusion of the visited MNO). Fraud is the responsibility of the operator implementing the retail billing, so in the case of roaming unbundling, this will be the ARP, and the Domestic Provider if the customer elects to remain with their domestic provider to provide EU roaming services.

This creates an interesting situation, where the HPMN now has some responsibility towards the VPMN for roaming traffic generated by an ARP's customer. NRTRDE files will be delivered from the VPMN to the HPMN, who must then identify records that relate to the ARP's customers, and forward these records on. In this situation, the fraud risk increases significantly if either (or both) the HPMN and the ARP do not have systems or processes in place for 24/7 monitoring of inbound NRTRDE records.

It is understood that a current proposal for Fraud Management involves using an On-line Charging System (OCS) through CAMEL however this requires all Local Break-Out Operators (LBO's) to support, and move Post-Pay services, to CAMEL.

While the OCS initiative would provide significant advantages for real time roaming fraud management, the value of NRTRDE as an effective fraud detection tool when monitored 24x7 should not be under-estimated, and depending on how the EU Roaming Initiative develops, could deliver increased value for European operators providing EU regulated roaming solutions. If the decision is taken that OCS will be required to support the EU Roaming Regulation initiative, this will require significant investment by European operators and it is likely that implementation could suffer similar delays to those experienced with NRTRDE implementation. With a mandatory date of 1 July 2014 for European operators to provide these new regulated roaming services, NRTRDE may remain a preferred alternative to some roaming access service providers.

Colin Yates
February 2013
Email: colin@yatesfraudconsulting.com