'International revenue share' may sound benign but not with the word 'fraud' appended. In fact some members of this industry argue that international revenue share fraud (IRSF) is one of the most serious fraud issues that mobile communications has faced. Essentially gangs or organised groups use connections obtained by fraudulent means and make multiple calls into high-cost revenue share numbers while roaming.

Anette Svendsen, product manager at MACH, a global clearing and settlement partner for mobile-based transactions, explains why IRSF is becoming a widespread issue in the mobile industry. "The professional fraudsters have turned their attention to mobile roaming because it is so easy to set up a premium rate service with an operator," she says. "They are becoming increasingly global and resourceful in their activities."

Some estimates of losses run into the ten of millions across the globe. However, the extent of losses experienced by individual operators is harder to estimate. The implications of roaming fraud, however, are clear, as are, from MACH's point of view, the ways to minimise losses from fraudulent activities.

As operators are aware, Near Real Time Roaming Data Exchange (NRTRDE) systems are set to become a GSM Association requirement to minimise roaming fraud loss. However, prior to NRTRDE (and even now in many cases) High Usage Reports (HURs) are, or were the norm. What are the pros and cons of HURs?

Svendsen points out that one key advantage of using HURs is that they contain a list of International Mobile Subscriber Identities (IMSIs) which can track unusually high usage levels and indicate potential fraudsters. "However," she adds, "the disadvantage is that this information isn't relayed back until 36 hours after the high usage has been detected."

Hence the need for a real-time solution, although it may appear to non-specialists that it has taken a long time to bring NRTRDE into play. How urgent is the need? As Svendsen explains: "Not all operators experience fraud loss and implementing NRTRDE is primarily to the benefit of the receiver, so to some operators there is not a commercial incentive to change existing procedures."

As for how it works, with NRTRDE you will no longer receive a list of suspected IMSIs within the HURs. What you will receive instead are multiple files that provide a record of what usage has taken place during the last four hours from which the operator can identify fraudulent behaviour. Another advantage of using an NRTRDE system is that you can collect Call Data Records (CDRs) within the time frame needed for them to be generated into the correct format to be transferred to the receiving operator. And MACH, not surprisingly, has a potential part to play here. As Svendsen says: "If you are a large operator with over 300 roaming partners, then the advantage of using a central hub like MACH is that you only have to send the files to one single point of contact."

But of course, this will mean a few adjustments. Svendsen says: "On the administrative side of things existing roaming agreements need to be updated with details of the NRTRDE deployment. This also means that the current fraud procedure at an operator will need to be redesigned to ensure a smooth transition between HUR and NRTRDE. In terms of liability the late visibility of the CDRs can result in claims from roaming partners that the CDRs were delivered too late. Training staff to understand the importance of CDRs and how to follow up on possible claims from roaming partners can help to minimise this type of dispute." And minimise IRSF - until the fraudsters come up with a new approach.