

---

## The £1.2m o2 iPhone Scam: How did it happen?

Published by Ewan  
Friday 17th September 2010

Like many people I was very interested to read this story about the recent scams committed on the o2 network (and others). At first it was rather funny to read. It was a bit of ingenuity, a clever ruse and a way to get back at the operators that charge too much anyway. Yeah, yeah, they shouldn't have done it and it was a bit 'naughty', but maybe a modern day Robin Hood story.

At least that was my first thought, then I read it a bit more closely:  
If they targeted the five UK operators equally, then that's £6m a month. Yes, **a month**. Even if o2 was the hardest hit then it's probably still in the region of £3m a month. So how the hell did the UK operators let this happen? It surely can't be that difficult to spot in excess of £1m walking out the door. Or can it? And is it negligence in spotting this that keeps my tariffs (and yours) so high?

So I thought I'd ask a couple of experts if they could help explain it to me.

First up, I spoke to Tal Eisner, Senior Director of Product strategy for cVidya Networks. I asked him what his first reaction was to the news:

"In my opinion, the case in question was a master plan and therefore it was quite successful for the people who committed it. The fraudsters not only stole some phones and produced calls, they shipped the phones abroad in order for these calls to go unnoticed, or at least unnoticed while in progress."

"GSM Operators have been utilising a procedure in the past 2-3 years that goes under the name NRTRDE (Near Real Time Roaming Data exchange). This procedure obligated the operator to send details of roaming calls to the home network of the roamer in time frames of 4 hours, that's in order to decrease the amount of abuse and fraud while roaming."

"I strongly suspect that these fraudsters knew which countries to ship their phones to. They did it to countries that have NOT deployed these procedures and thus the time frame of reporting is like the "old times", pre NRTRDE, which is up to 72 hours. A long enough time to perform many calls – costing the operators a fortune. Smart guys!"

### So how this could have happened, how was the international calls element of this important?

"These calls have been deliberately done on roaming because in such cases the operators have no real time detection of the traffic. Moreover, the fraudsters, I suspect, knew in advance where to ship the stolen phones to and originate the calls from. They did it from countries where there is no NRTRDE procedure in place and therefore the home networks received the data of the calls after a 72 hours delay."

"Operators should deploy NRTRDE ASAP. [They should also have] a Fraud Management System that has all the sufficient tools in order to have as much control as possible over roaming traffic. Roaming is highly expensive and controlling it with 24/7 tools can save millions of dollars every month."

He was too polite to mention that the cVidya Fraud View product could help here!

Then, I spoke to Paul Paterson, the Operations Director for ImpulsePay. I also asked him what his first reaction was.

"I wasn't particularly surprised that this sort of thing was going on, but I was surprised with both the amount of money involved and the time it was allowed to go on for. I think o2 must be relieved that they spotted it when they did and I can understand that they might think that it is a victory against fraudsters. But the reality is that they actually lost £1.2million in a single month!"

**Premium rate calls seemed to play an important part in this, why?**

“Because it’s easy. Setting up a premium phone line abroad takes minutes, and there aren’t really many safeguards against bad debt, as mobile contracts are credit based. So if a fraudster is willing to use stolen information to set up a new contract phone, they can pretty much get away with this type of activity for at least a short time. There are also similar scams involving premium rate messages.”

“Fraud prevention systems are key. For example, if o2 had a system in place which allowed it to flag possible fraudulent activities in real-time, they could avoid this happening in the first place. I think the operators need to look into investing in new systems that flag up, say, a brand new user who is suddenly calling [or texting] premium rated phone lines abroad at hundreds of pounds a month. Given this latest story, and I’m sure a few others that we haven’t heard of, it would be a very worthwhile investment for them.”

- - - - -

Thanks guys, a really interesting take on it.

I keep on having to remind myself that many mobile operator systems are held together with what appears to be very expensive pieces of string. Dear me.