



# Chasing the tail of fraud

In fraud operators face a constantly changing enemy often without a face. Mark Dye spoke with some of those tasked with helping to prevent this to gauge where we are in the evolution of this revenue sapping threat.

With the mobile phone becoming ubiquitous its data presents a goldmine of opportunity for carriers. Yet in the wrong hands this definitive map of who we are and how we live our lives presents a very real threat of lost revenue and very real implications in terms of data privacy.

“The trust we’re putting in a mobile device already is really quite astonishing,” warns Dale Youngs, product manager for fraud, revenue assurance and credit risk management at **Subex**. “The banks think this is a trusted piece of kit and if they actually looked underneath and looked at operator procedures for managing customer credentials and things like that I think they would sometimes be horrified.”

Strong words. But with the mobile industry not the gravy train it once was Youngs says financial pressure to consolidate and cut costs is directly affecting fraud teams seeking to tackle attacks that are becoming increasingly technical in nature.

Jason Lane-Sellers, principal consultant at **Connectiva Systems**, believes that this impact

and squeeze on operators via their customer base and finances means the fraud department is often one of the first challenged as it can be seen as a cost centre.

And with the focus firmly on that customer base he says a big push is often made to keep customers happy via improved offers and incentives to retain them.

“Both these mean that the fraudsters can shift their emphasis in times like this and rather than target new connections, they actually increasingly target fraud against existing account holders, known as account takeover or facility fraud,” he says. “This attack is often due to the fact that existing customer bases often have much less fraud team focus when the squeeze is on, but the returns can be much higher as existing customers can get the best deals with little or no checking or validation by the network due to the desire to keep the customer.”

Tal Eisner, senior director of product strategy at **cVidya**, adds that in the last few years more ‘classical’ fraud types such as PBX hacking ▶



Dale Youngs, Subex: Being flexible and agile is the key



Tal Eisner, cVidya: Classical fraud has become routine

and various Premium Rate Service (PRS) schemes - including International Revenue Share Fraud - have become routine worldwide.

"PRS related fraud is organised crime that relies on PRS numbers globally and is characterised by the distribution of such numbers and the artificial inflation of traffic to [them], along with inflation of traffic that results from calls coming out of stolen phones," he explains. "Thus, this is a more mature, organised and efficient way to commit fraud and it involves more personnel and not just the single fraudster committing single local or specific frauds."

Yet, Lane-Sellers says that with fraud still being a business, the simplest and quickest attacks are the most prevalent.

"This is why account takeover is such a growing trend at the moment," he adds. "For the fraudster, the revenues can produce a good, high value return with relatively small effort required and minimal technical or support resource."

Of course, such attacks can be sustained over time and are very flexible, with fraudsters being aware that they target areas that traditionally have little active fraud coverage or monitoring, as they are based on process manipulation rather than traditional usage methods.

According to Lane-Sellers, account takeover fraud is also one of the worst things for a company to suffer at this time.

"This is because for every fraud instance, a genuine innocent customer will feel an impact and this can mean a double blow to revenue costs, via goodwill or account reimbursement, a third blow, due to the massive loss of trust and hugely negative customer experience, and finally a fourth mortal blow, which can be to the brand via the implied lack of data security or management of customer data indicated by such a fraud," he adds.

Simon Collins, vice president for business consulting at **Praesidium**, believes that another major change in the pressure faced by operators has been in the separation of the bearers that link customers to networks - compared to the services that are carried.

"This means that there is a need for fraud services and bearer fraud detection as two

separate items," he explains - something which applies particularly in next generation network services like fixed mobile convergence, IMS and VoIP based service offerings.

"Closer links are growing between fraud and revenue assurance," he adds. "IP security is something we also see growing as people, data sources and systems merge."

Interestingly, Praesidium often finds that vendors of fraud systems do not understand IP and the event record. This often means many say they can include these in an existing fraud system data feed, but do not consider the use of the record in the system and do not have the tools to adequately use the data.


"If operators are looking to have IP and data services in their existing systems, they must fully understand the direction of NGN services and the data sources plus the IP fraud control rules they need to use," says Collins.

As a result, Youngs points to a more holistic approach in the future where fraud is looked at in conjunction with related areas like revenue assurance and credit risk. "I think we're seeing an increase in the need for managed services, for cloud applications, and also quirkier things like risk reward share models," he says.

"One other thing here is not just looking at it from fraud and related applications like revenue assurance and credit risk, but looking wider and sweating the assets and looking at completely different applications like law enforcement liaison," he adds.

He reasons that fraud systems are ideal for running queries and extracting data for agencies whilst also being good for managing things like bill shock.

Unfortunately for operators Youngs thinks we're some way off winning the battle with fraud though and, rather soberingly, wonders if we'll ever get there.

"It's so difficult to pre-empt where fraud will go or where any clever new frauds will emerge," he adds. "Being flexible and agile is the key. If you look at just the brainpower out there and the motivation of fraudsters it's always going to be that much higher than those trying to stop it. We're probably where we've always been; in the shadow of the fraudsters, hanging onto their coat tails." 



Simon Collins, Praesidium: Often fraud systems don't understand IP