FRAUD & SECURITY BUSINESS BRIEFING 2013: Buyer beware?

http://www.capacitymagazine.com

It is an oft-quoted truism among fraud investigators that in order to stop a crook, you must first stop the flow of money.
In the case of the global wholesale telecoms market, currently facing an explosion in scams that is set to cost the industry upwards of $40 billion this year alone, that is much easier said than done.
By its very nature, the infrastructure underpinning carrier-to-carrier transit is built on a complex web of bilateral deals. While no two interconnect agreements are the same, they all have one thing in common that makes the pursuit of criminals particularly hard: every deal enshrines into contract law the principle that the carrier must always pay for traffic that is handed to it, regardless of that traffic's provenance. The very rules that make the wholesale market turn, in other words, effectively conspire to halt the fight against fraud in its tracks.
The circle currently seems unbreakable: to stop money flowing to fraudsters, a carrier within the transit chain would have to default on its obligations to another carrier and to do that would put the operator in breach of contract law and indeed most national regulatory frameworks.
"When you start looking at the carrier-always-pays model, you enter a world of shades of grey. There is absolutely nothing black and white about trying to stop the payments chain in the wholesale arena", warns Jack Wraith, chief executive of the Telecommunications UK Fraud Forum (TUFF). Wraith has been trying to galvanise industry efforts to combat wholesale fraud for more than a decade, but progress is slow. The problem, he concedes, is that carriers are bound by complex interconnect, roaming and wholesale agreements that were struck long before the current surge in wholesale fraud began to manifest itself. Typically, carrier C agrees to pay carrier B, for any traffic that is delivered to it, while carrier B contracts to do the same with carrier A. The chain can extend to upwards of ten carriers and each link in the chain is dependent on money flowing from its predecessor in order to meet its own obligations. According to a recent survey by the Body of European Regulators of European Communications (BEREC), some carriers have just one interconnect partner, while others have up to 500. Only the originating and terminating carriers are likely to get an inkling as to whether fraudsters are at work on the call. "To try to tinker with that chain risks disrupting the market in a potentially catastrophic way", Wraith says.
Nowhere is payment enforced more rigorously than at the point of origination – that moment when a person picks up the phone in the first place. Consumer laws in most jurisdictions are very clear – and indeed vehemently supported by regulators: the owner of the phone is legally responsible for any charges that arise from it, regardless of who actually makes a call, let alone whether foul play is suspected. So in the eyes of the law, a company that finds itself the victim of a hacking scam is deemed to be at fault for having lax security measures in place, just as a teenager who loses a mobile phone on a night out is considered to be negligent if a crook goes on to use the device to phone premium rate numbers in Afghanistan.

What makes the whole issue of liability in telecoms fraud particularly contentious is the fact that service providers are under no legal obligation to identify fraudulent behavior or indeed to cap their customers' exposure to it. In the banking industry, by comparison, companies have a fiduciary duty to protect their customers from fraud, encouraging them to limit the liability of their account holders to illegal transactions.

TUFF's Wraith complains that a direct comparison between the two industries is disingenuous: "The banking sector has an interoperable payments system that works seamlessly across international boundaries and that can be programmed to flag up abuse 24/7." A customer will know within a matter of hours if his credit card is being illegally used on the other side of the world, he explains. No such platform underpins the telecoms market, nor is there any likelihood that there ever will be in the future.

Nevertheless, the lack of any such limit to customer liability in the telecoms sector has prompted some critics to suggest that operators might turn a blind eye to some scams knowing that the end customer, with the explicit approval of local regulators, is – quite literally on the hook and that under the "carrier-always-pays" model, wholesalers should generate more revenue from carrying additional traffic that may or may not be fraudulent, than they will lose as a victim of fraud themselves.

The debate changes subtly according to the type of fraud in question. There is little doubt, for example, that collectively, the carrier industry is doing everything in its power to close down SIM box or interconnect fraud, where crooks disguise high-margin international traffic to look like free local calls in order to dodge termination fees. There are no wholesale "winners" and "losers" in interconnect fraud – only losers: any carrier that unwittingly sends traffic down a route with a SIM box on it faces losing 80% or more of the value of that call.

But the picture is considerably murkier in the case of international revenue share fraud (IRSF), where crooks hack into networks and generate a large number of calls to high value numbers with the intention of sharing revenue with the wholesaler.

As Colin Yates, director and principal consultant at Yates Fraud Consulting, a former head of fraud for Vodafone UK and one of the leading independent experts on wholesale scams warns, "There are certainly some carriers out there who have made quite significant amounts of money transiting IRSF traffic and who do not consider that they have any responsibility to do anything to reduce another carrier's exposure to the scam".

Some transit carriers will argue that there is no mechanism in place for them to risk-assess a call originator all the way back along the chain and that they should therefore not be held accountable for any misdemeanors that subsequently take place.

It's a fair point – take, for example, the case of a retail carrier which supplies a box of SIM cards to a questionable company or individual, and those SIM cards are not only provisioned with roaming but also the ability to call forward to, say, Senegal or Sierra Leone. It would be wholly unacceptable if that carrier thought it could take a punt on supplying those customers, with the intention of clawing back some losses further down the line by holding onward payments to other carriers, if those customers did indeed turn out to be "dodgy".

But the counter argument has persuasive merits, too: the retail-facing carrier is most likely to take the hit in an IRSF scheme, either because the customer simply can't pay the bill, or because the reputational fallout associated with fighting a David-versus-Goliath case against the end customer can escalate out of control and feed unsympathetic headlines for months to come.

"I guess the hard answer to all this must be that if people accept that the only way to stop this scourge is to stop the flow of money, and that it is an industry problem, then ultimately, the industry has to collectively expect to shoulder the pain", says Yates.

TUFF's Wraith agrees. To fail to find a solution, he warns, is to provide a regulatory and legal haven where fraudsters may develop ever more complex scams virtually unhindered. "In the first instance we need a European-wide initiative that all the major telecoms providers would be willing to put their names to. It can't be done on the fly, and it won't be cheap, but it is possible."

Wraith points to Phonepay Plus, a division of Ofcom that regulates premium rate services in the UK. Before Phonepay Plus came onto the scene, fraud linked to UK premium rate services was rampant. Now it has been almost stamped out. The regulator oversees a code of practice for legitimate services and brokered a new 28-day settlement period that gives telecom operators an effective window in which to challenge suspect traffic before payment becomes due.

But despite its success, not all operators want to see the model replicated at an international level. The head of Fraud at one of Europe's largest telecoms companies, for example, is surprisingly reticent. Speaking on condition of anonymity, he argues that a new system would create more problems than it would solve: "For all its critics, the current modus operandi works extremely well. To start from scratch now with a totally new system would be very complex and very cumbersome. I categorically do not support such a proposal. To suggest that there is a simple solution out there through which the industry can fight fraud is dangerously naïve. It is incumbent on everyone with a major interest in the wholesale market to beef up their own procedures."

If you think such intransigence in the face of such an escalating problem is surprising, or even unrepresentative of the views of the industry at large, consider this.

In 2010, Vodafone UK sought to establish a groundbreaking precedent that could have advanced the cause of payment reformers by years.

Investigators at the mobile phone giant uncovered a substantial scam in which crooks had fraudulently applied for a number of SIM cards from the company, shipped them over to Europe and used them to make calls to premium rate services to a third destination with high termination rates. Because of the way in which the SIM cards had been acquired, Vodafone argued, there was no likelihood that payment for the calls would ever be made and the company therefore sought to halt payments trickling through the chain.

To support the claim, the mobile operator obtained a legal opinion stating that Vodafone would effectively be breaking the law if it went on to receive money from a third party transit carrier for traffic that it already knew to be fraudulent under Section 327 of the Proceeds of Crime Act.

At first sight, the specifics of the opinion were unambiguous: lawyers ascertained that the fraudulent acquisition of SIM cards was a crime, as well as their subsequent use in a revenue share fraud; it also found that revenues generated

from such a crime effectively amounted to “criminal property” and that in keeping with Section 343 of the Act, such property should be withheld as soon as the fraud was discovered. And in a coup de grace, lawyers also suggested that while the opinion related only to UK law, Vodafone would effectively be covered in the same way through the European Union Anti-Money Laundering Detective.
Here was the cornerstone on which a new front in the attack on fraudsters could be opened. At a top industry gathering in September 2010, Vodafone went public, announcing that it would no longer make payment for call charges arising from IRSF. But far from embracing the move, some of Vodafone’s peers came out on the attack, challenging the credibility of the opinion and without committed support from the rest of the industry, the company was forced to back down.
Yates, who was involved in the work at Vodafone back then, believes the industry wasted a great opportunity to take the fight against fraud back to the perpetrators: “It is unfortunate that no two carriers were prepared to take this through the disputes resolution process to force a decision. “ If Vodafone had indeed managed to stop the money flowing back to the fraudsters, he argues, the crooks would have been forced to move on to something new by now.
Two years on, and billions of dollars in fraud losses later, little has changed. European regulators are once again looking at the carrier-always-pays model – and specifically whether it may be possible to block payments in frauds on a case-by-case basis, as part of a review of the Universal Service Directive.
In regulatory guidance published earlier this year, BEREC accepted that it might prove difficult to rewrite bilateral agreements to block fraud payments, especially among partners that operate outside the EU. But in a sign of, frankly, unfounded optimism the regulator went on to conclude: “It is envisaged that commercial pressures will resolve these issues in time”
In public responses to the paper, BT accepted that there is a clear need to bring what it called a “higher level of control over the onward payment of call revenues” but cautioned that “contractual undertakings often prevent payments from being withheld”. BT knows a thing or two about trying to wring consensus from communications providers with very disparate interests (see box).
Arguably, the best that can be said of BEREC’s work is that it has reignited the fires of a debate that some carriers would prefer had gone out. “Three years ago there was no debate at all surrounding the issue of withholding payments in fraud. While BEREC’s conclusions are a little disappointing, the industry has at least moved on – albeit slowly”, says TUFF’s Wraith.
Just why a body of carriers would work to undermine reforms is unclear: “There are certainly a number of international jurisdictions who gain directly from fraudulent services that are offered on their watch”, Wraith says. But the determination to stamp out fraud has never been stronger. “None of our members would want to profit from fraud in any way.”
Yates is also frustrated at the slow progress. “I personally do not think we will see any significant impact on IRSF from initiatives such as BEREC for the next 2-3 years at least – if not longer, This type of fraud has been around for at least seven years and progress in combatting it has been slow.”
IN the short term, Yates adds, carriers must take matters into their own hands to disrupt fraudsters as best they can. Most remedial actions are a matter of common sense but carriers should at the very minimum invest in early warning systems that can flag up an IRFS attack as soon as possible and conduct regular

reviews to identify weak controls within the company. “I have seen far too many examples in this industry of chief financial officers who have for the sake of a E200,000 -300,000 investment in fraud detection tools, decided to take the risk that they would not be hit. IN the end fraudsters will always flush out weak links in the wholesale chain and take them for far more than an anti-fraud solution would have cost.”

BOX

There is a degree of apathy that pervades the payments system in the wholesale arena – a sense that the carrier-always-pays model is just too big and too complex to overhaul. BT’s experiences in attempting to tweak that model show on the one hand just how convoluted the process can be but on the other, how perseverance can pay dividends.

Responding to a surge in revenue share fraud, internal investigators decided in 2002 that BT would redraft its standard interconnect agreement in order to make it easier to choke off payments to suspected fraudsters. The company already had a clause in the contract for dealing with what it called “artificial inflation of traffic” (AIT). But fraud busters at the company wanted to broaden the scope of what might legally be defined as AIT, as well as embrace new processes to stop payments where AIT was suspected, BT’s specific involvement in that process and the way any resulting disputes might cordially be resolved.

After a staggering six years of consultation with the industry, BT was ready to go for broke. In May 2008 it asked every one of the 122 communications providers who are signed up to the group’s interconnect agreement, to approve the changes. Every signatory was required to approve the measures for the changes to take place. A year later, seven had refused to sign up (1RT Group; CFL Communications; Flextel; Mars Communications; Starcomm; Telxl; Tele-Lynx UK). Another four simply did not respond to repeated requests to negotiate – namely, Bestway Communications, Callagenix, Prodigy and Vectone.

Among the issues that the communications providers objected to, was that the principle of withholding payments in frauds favoured the originating network operator above pretty much anyone else in the chain. However, BT countered this worry by placing a far greater burden of proof on the originating carrier.

Other objectors specifically demanded that calls made as a result of hacking into a private branch exchange should be excluded from the withholding process, to reinforce the message that the owner of the phone system is ultimately culpable for its security. There was also concern that BT, acting as either a transit operator, an originating carrier or a terminating carrier could effectively control all points of the network by halting payments as and when it saw fit.

In July 2009 – seven years after BT first began the process, OfCom upheld the reforms as “fair and reasonable” and ordered the remaining objectors to sign up to the new interconnect agreement. In March 2010, BT finally launched the new AIT regime and following another round of consultations with the industry, updated the process again in 2011.