Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 12, Issue 5

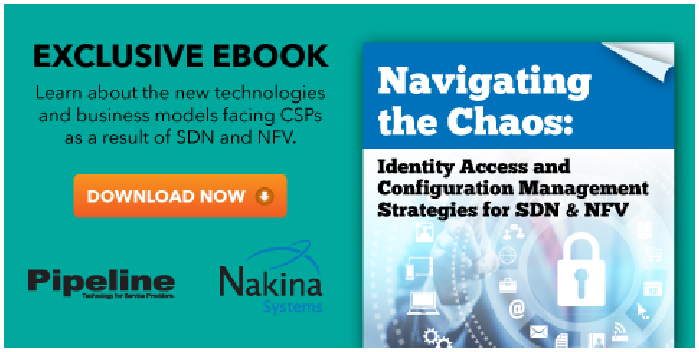
Industry Report on Telecom Fraud Management Services, Software & Strategies

By Dan Baker

The global village has fallen in love with the versatility that telecom industry progress has brought us. Unfortunately, there's a trade-off because communications advances bring with them new fraud and security risks.

Take the business PBX. Its ability to redirect phone calls is wonderful for business people. But that feature opens the door for PBXs to be exploited through International Revenue Share Fraud (IRSF), a fraud which costs telecoms $4 billion a year according to the CFCA.

GSM is another example. It triumphed over CDMA partly because it was more versatile. Users loved the idea of popping a SIM card in and out of a handset. But that versatility also came at a cost, for it has enabled SIM box bypass, a growing fraud issue across the globe.

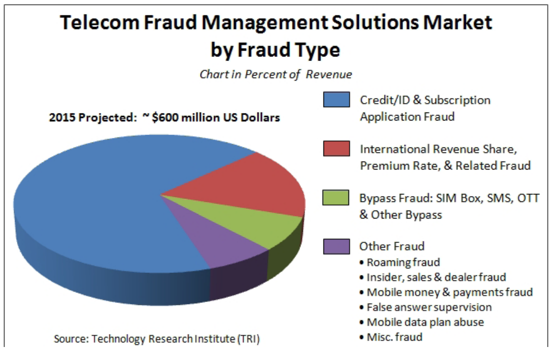


To explore how telecoms are keeping a lid on their old and new fraud problems, Technology Research Institute (TRI) conducted three dozen interviews with fraud management solution suppliers, service provider experts, and consultants. The result of this research is a 239-page report entitled, **Telecom Fraud Management Services, Software & Strategies**.

Overall we forecast the global market for telecom fraud management solutions – including software, service bureau, databases, test call generation equipment, and managed services – will reach about $600 million in 2015 as show in the forecast chart below.

A Collaborative Effort to Tame International Revenue Share Fraud

A Collaborative Effort to Tame International Revenue Share Fraud A Collaborative Effort to Tame International Revenue Share Fraud International Revenue Share Fraud (IRSF) is one of the telecom industry's most enduring problems. PBXs are the leading gateway to IRSF. Groups based in countries like the Philippines are continually dialing out to nations of the world to hack PBXs. Once they gain entry, they sell that intelligence to their organized crime partners who make the IRSF calls. The favorite time to initiate IRSF fraud is Friday evening and the idea to rack up $50,000 worth of fraudulent traffic before Monday morning when the operator's fraud management team comes back to work to discover the security breach. One particularly successful form of IRSF fraud is Wangiri (Japanese for "one ring"). With Wangiri, the fraudsters generate tens of thousands of very short duration calls then hang up. And if the fraudsters are lucky, as many as 20% of the people who missed the call will ring back to find out who it was and be connected to an IVR. And the message will say something like: you've



Source: Technology Research Institute (TRI) just won a new iPhone – or anything to keep the caller on the call as long as possible.

Well, the good news is that IRSF fraud is getting plenty of telco attention these days. The net effect, we predict, is that the financial damage caused by IRSF fraud will decline. Here are the solution forces at play:

- **Leading international wholesalers are taking steps to help their retail partners** – These wholesalers have launched a significant anti-fraud prevention program to help their retail carrier partners. They initiate programs to either share fraud intelligence with each other or simply stop the traffic according to a blocking policy approved by the retailer.

- **Fraud Detection Integration with Billing and Routing** – Telarix recently announced support of IRSF fraud capabilities: it's an important milestone because the majority of tier 1 wholesale providers use its unified billing and routing platform.

- **Pre-Call SIP Invite Blocking of Fraud is a Major Trend** – TransNexus has pioneered the use of SIP invite as a method of blocking blacklisted numbers before calls are made. Meanwhile Equinox Information Systems plans to combine SIP invite capability to create a hybrid solution to buttress its U.S.-market-leading CDR analytics-based FMS.

Fraudsters are Winning the Stealth Game in Bypass Fraud

A few years back, the term "bypass fraud" was practically synonymous with voice fraud via the SIM box. But the march of network, software, and mobile technology has brought new stealth tools and fresh avenues to deliver bypass fraud. The effect has been to open the bypass floodgates for fraudsters.

In the SIM box area alone, human behavioral simulation tools have made it devilishly hard to detect bypass SIM boxes via CDR analysis alone. And SIM Servers are automating multi-national bypass operations by rotating cards from a central bank of SIM cards located halfway around the world from the infected country.

What's more, bypass is spreading to SMS and is finding avenues through ghost trunks and OTT apps such as VIBER on the mobile phone.

Still, SIM Box bypass is the problem that refuses to go away. In 2013, the CFCA estimated the telecom loss through bypass to be about $2 billion a year. Other reports claim losses of $3 billion to $5 billion per year.

> *The effect has been to open the bypass floodgates for fraudsters.*

So, why does the fraud continue to cause such massive losses? In fact, operators in some countries affected by SIM box fraud will privately tell you that their international inbound traffic has decreased by as much as 50% in recent years!

What's more, these same operators have invested heavily in anti-fraud campaigns - and they actually do detect and block fairly large volumes of SIM boxes on a daily basis.

So what does this mean? It means that the fraudsters are succeeding despite the anti-fraud efforts of the carriers. They are replacing the blocked SIM cards with fresh supplies of SIMs and continue their bypass.

Here are some crucial developments in taming bypass fraud:

- **Test Call Generators (TCGs)** – TCGs are the key to examining the grey routes where bypass traffic is coming from. Araxxe deploys TCGs as a managed service for operators in the Middle East and North Africa and claims the secrets to stopping bypass are two: 1) be highly selective in the interconnect routes you monitor; and 2) run test call programs during the opportune calling periods of the country being served.

- **Integrated Bypass Solutions are Comin**g – SIGOS, the global leader in test call systems, has announced a new bypass-specific solution that combines the virtues of a next-gen FMS and TCGs in a single platform.

- **Protocol Signature Analysis**, a new probe technology developed by LATRO Services, stops bypass by recognizing the unique behavior of the SIM box as it signs onto the network.

- **SMS Bypass Blocking has Arrived** – As demand for A2P SMS traffic goes up, mobile operators are flooded with unauthorized marketing messages and other fraudulent uses of A2P. SMS specialty firms such as Infobip are delivering fraud protection through managed services solutions that detect and block illicit traffic. CSG International, through its test call machines, is checking SMS quality and SMSC network element mapping to ensure contracts are being followed and A2P traffic is truly routed via premium routes.

- **OTT Bypass is Not Fraud**, but it's Killing Mobile Operator Profits – The growing practice of wholesalers redirecting mobile-to-mobile traffic from the PSTN to a VoIP application like VIBER or WeChat is seriously cutting into mobile operator revenue. The big mobile groups are thus eager to discover which wholesalers are causing the bypass, so commercial solutions to monitor this bypass are appearing from SIGOS and IPsoft.

Credit/ID & Subscription Application FraudOur communications-driven world is blessed and cursed by greater access and "convenience".

The blessing of convenience is that information is at our fingertips. We've moved from checking email messages once a day by smart computer. . . to once an hour by smart phone. . . to once every 10 minutes via smart watch. But the curse of convenience is we've made it much easier for fraudsters, con artists, and hackers to rob us.

That's where credit bureaus come in. Credit bureaus protect businesses and consumers by throwing inconvenient obstacles in the path of the fraudsters. The emphasis at credit bureaus today is on using fraud prevention tactics that are also customer-experience-friendly, such as predictive scores, device risk assessment, and linkage analysis.

Several innovative solutions have either arrived or are under development in the credit area:

- **Fraud Alerts via Device Intelligence** – Through a big data platform, Experian maintains a history of activities associated with a particular device (smartphone, tablet, computer, etc.) The system recognizes whenever a particular device visits a website or opens up a mobile app, then creates fraud alerts where a suspicious linkage of a device to other websites and behaviors is found.

- **Real-time Point of Sale Subscription Application** Checks are an invaluable aid to stopping fraudsters from exploiting ID theft, credit mules, and the near-simultaneous ordering of expensive handsets by teams of fraudsters going to multiple stores. FRS Labs has delivered this new capability at Vodafone Ireland. And cVidya has recently integrated fuzzy matching technology into its FraudView for the same purpose.

> *While the telecom fraud threats are many and highly diverse, operators are cooperating with others like never before and some innovative software and managed service solutions have emerged.*

- **New Technologies will Simplify Identity Checks** – Biometric technologies such as voice-printing shows great promise in making identity/fraud checks easier. The race is on for fraud management suppliers to offer solutions.

Solutions for Future Fraud Threats

Finally, some fraud solution categories have a relatively small market share today, but may loom large in the years ahead. Here's TRI's analysis:

- **Insider, Sales & Dealer Fraud Solutions** become far more valuable as other frauds are brought under the control. For instance, if SIM box bypass is being effectively blocked, inside fraudsters can establish "ghost trunks" that operate outside B/OSS control. TRI believes solutions will appear that automate the investigative processes that make Insider fraud checks more manageable. For instance, Subex offers pre-built topology libraries and metrics called Dynamic Network Analytics (DNA) that auto-configures processes across an operator's revenue management systems.

- **Anti-Fraud Solutions for Mobile Money and Payments** is a promising market for unbanked regions of the world because telecoms have a wonderful opportunity to serve the financial needs of people whose banks cannot cost effectively serve. Anti-fraud solutions are emerging here from firms like Neural Technologies who currently protects the popular M-PESA service in Kenya, securing the movement of $10 billion of

- **Consumer Abuse of Mobile Data Plans** is a worry as operators roll out premium usage plans that people access illegally. cVidya is attacking the problem with a solution that combines DPI data feeds and Hadoop technology.

While the telecom fraud threats are many and highly diverse, operators are cooperating with others like never before and some innovative software and managed service solutions have emerged. But history proves the criminal mind always finds ways to exploit our industry's weaknesses. To maintain control over fraud, then, operators must step up their investments in rules- and behavioral-learning-based analytics and employ expert investigators who are thoroughly versed in operating processes and B/OSS systems.