Telecom Fraud Management Services, Software & Strategies

Executive Summary

August 2015

Technology Research Institute (TRI)
1245 N. Rocky Mountain Drive
Effort of the Poconos, PA 18330

Tel: 570--620-2320
www.technology-research.com

Copyright 2015 Technology Research Institute
A. Executive Summary

1. Introduction – Communications Advances vs. Fraud Risks

The global village has fallen in love with the convenience and versatility that telecom industry progress has brought us.

Unfortunately, there’s a trade-off because communications advances often bring with them new fraud and security risks.

Take the business PBX. Its ability to redirect phone calls is a huge convenience 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 its 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 and Strategies.

Here are some highlights of the Report’s analysis and predictions:

2. Telecom Fraud Management Solutions Market: The Big Picture

TRI forecasts 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. See the forecast chart below.
About two thirds of the solutions market, TRI estimates, is in the Credit/ID and Subscription Application Fraud sector where the business is dominated by global credit and fraud service bureaus.

Second in market size are solutions that monitor and block IRSF, premium rate, and related toll frauds, such as Wangiri. And third is the growing problem of bypass fraud, particularly SIM box bypass.

3. International Revenue Share Fraud & Premium Rate Fraud

The good news is that IRSF and Premium Rate fraud are getting plenty of attention these days. The net effect, TRI predicts, 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.** Tata Communications has launched a significant anti-fraud prevention program to help is retail carrier partners; BICS is enabling its operator partners to collaborate and share fraud intelligence with each other; and iBasis is actually stopping fraudulent traffic (as opposed to merely redirecting it) in alignment with the unique blocking policies desired by the operator partner.

- **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** will combine SIP invite capability to create a hybrid solution to buttress its US-market-leading CDR analytics-based FMS. Finally, softswitch supplier **SwitchRay** now offers SIP invite as a bolt-on fraud solution for operators who use its own or other softswitches.

• **Black Lists of IRSF Numbers** – Black lists and other lists to identify past IRSF and potential IRSF fraud numbers are helping the market stay ahead of the fraudsters. **iconetiv** has a list of global unallocated numbers and a new, low-cost global black list is being offered by **Yates Fraud Consulting** and **FRS Labs**.

4. **Bypass Fraud**

Fraudsters have stepped up their game in bypass fraud, especially via the SIM Box. One technology making this possible is the SIM Server, which allows a fraudster to rotate thousands of SIM cards across multiple target countries. Here are some crucial developments in bypass:

• **Test Call Generators (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.

• **Finer-Grained CDR Analysis** is another key strategy. **Fraudbuster** has developed a specialized FMS that analyzes individual CDRs as instantly as they are received so as to block SIM box usage as quickly as possible.

• **Integrated Bypass Solutions are Coming** – **SIGOS**, a 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. **HAUD Systems** is delivering one of the first hosted and managed services solutions that detects and blocks illicit traffic in one platform. **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**.
5. Credit/ID & Subscription Application Fraud
This category refers to the fraudulent ordering of telecom services intent of stealing equipment or never paying for services rendered. The easy accessibility of digital devices for banking and e-commerce uses has made better fraud detection in this area critical. Several innovative solutions have either arrived or are under development:

- **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.

- **Cross-Industry Fraud Intelligence** – the ability for telecoms to leverage the fraud intelligence of companies in banking, e-commerce, and retail – has not been possible before, but LexisNexis Risk Solutions is using this technique to achieve broader and more accurate fraud scoring.

- **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.

- **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.

- **The Private Data Exchange is Born** -- Imagine if companies could share information in complete anonymity and security. Such a solution is now available from XOR Data Exchange: it enables carriers, banks, and e-commerce firms to share fraud and credit intelligence with full encryption of data at the source.

6. Other Fraud Solutions
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 far 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 world because telecoms have a wonderful opportunity to serve the financial needs of people who 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.

- **False Answer Supervision (FAS)** is a highly specialized kind of fraud that is extremely hard to detect, but IPsoft is using advanced analytics techniques to detect and document FAS violations for global wholesalers.

- **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.

### About the Research Report

*Telecom Fraud Management Services, Software & Processes* is a 239-page market research report that analyses the struggles, challenges, successes, failures, and dreams of those who seek to control fraud in the telecom industry. The emphasis of the report is on solutions: the techniques, technologies, and tools that are working – and not working – to prevent or stop fraud. Authored by Dan Baker, TRI’s research director, the report draws on conversations with more than three dozen telecom fraud experts with major contributions by five top consultants in the field.

### About Technology Research Institute

Technology Research Institute (TRI) has been writing and researching telecom software and systems markets since 1994. Its industry reports cover the gamut of telecom systems from billing and service assurance. . . to customer care and provisioning. In recent years, TRI has authored major reports on Revenue Assurance and Telecom Analytics & Big Data solutions. TRI also publishes two industry blogazines: *Black Swan Telecom Journal*, focused on revenue assurance, fraud, and analytics issues; and *Telexchange Journal*, which covers the wholesale, interconnect, and digital ecosystem partnering domain. TRI’s research director, Dan Baker, speaks at conferences such as *Capacity Magazine’s Wholesale Fraud Forum* and he co-hosts podcasts on *Commsrisk*. 