TELECOM FRAUD MANAGEMENT SERVICES, SOLUTIONS & STRATEGIES 2017

CHAPTER 1
EXECUTIVE SUMMARY

TABLE OF CONTENTS

Principal Analyst: Dan Baker, Research Director, TRI

Technology Research Institute (TRI)
167 Wedgewood Chase
Athens, GA 30605 USA
Tel: 570-620-2320
www.technology-research.com

A. Research Methodology

1. Research Methodology

Having previously delivered a successful 238-page Report on the state of Telecom Fraud Management in 2015, TRI decided to update our research for 2017.

We conducted about three dozen expert interviews and organized this study over a six month period, publishing this Report in August 2017. In the end, the final Report expanded to 385 pages. And by the time we add more vendor profiles in the coming months, we expect the final page total to be 400+ pages.

All told, the Report includes commentary from TRI interviews with 49 named fraud/security control experts and dozens of anonymous contributors. Authored by Dan Baker, TRI's research director and owner, the Report is both a market analysis report for solution vendors and a guide to help fraud control managers stay abreast of the latest developments in the field.

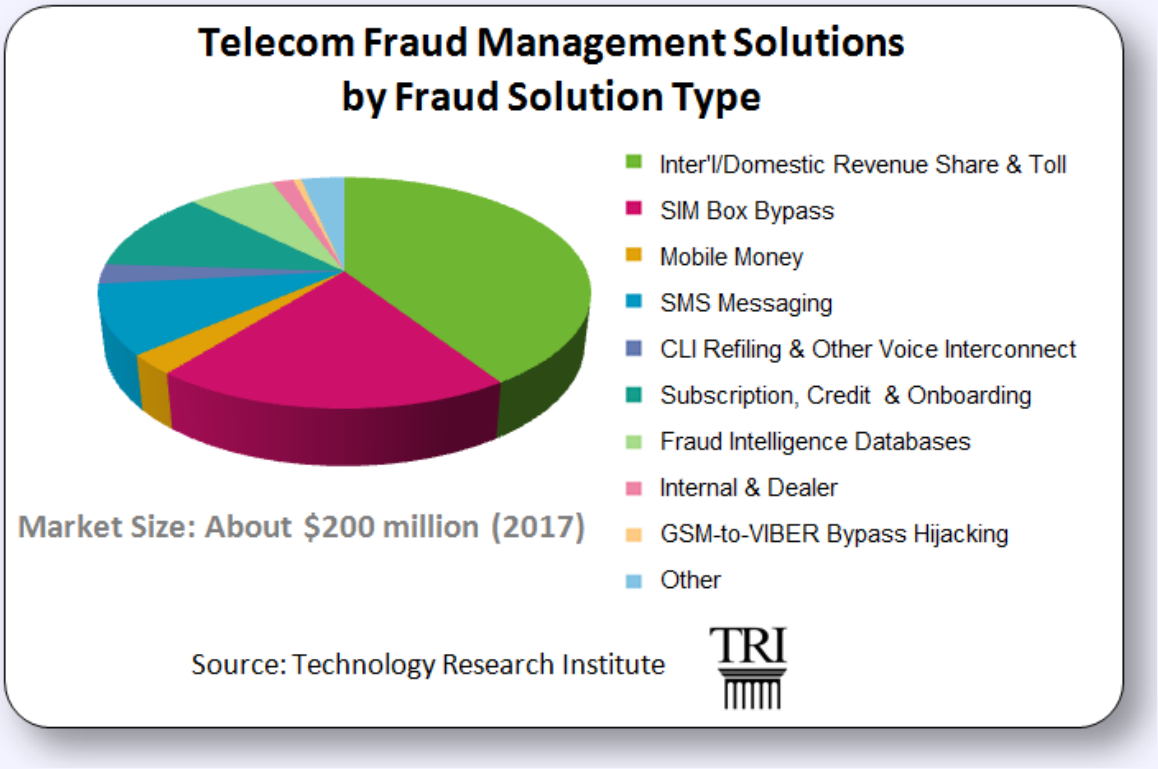
This Executive Summary is freely available to the public and the full report may be purchased by any telecom operator, fraud solution firm, or government regulator.

In thanks for their financial support of this research, TRI has written vendor profiles on the fraud management (FM) activities of several solutions firms. What's more, we covered solution vendors in the body of the report regardless of whether they chose to purchase this research report or not.

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

2. Telecom Fraud Management Solutions Market Forecast

TRI estimates the global market for telecom fraud management solutions – including FM software, test call generation services, and managed services – to be about $200 million in calendar year 2017. See the chart below.



B. Research Highlights

1. International & Domestic Revenue Share Fraud

As it was in 2015, international and domestic revenue share fraud continues to be the fraud threat driving the greatest investment in fraud control. According to the CFCA, revenue share is the fraud segment that accounts for the greatest telecom industry losses.

Here's our perspective and trend analysis on the Revenue Share fraud sector:

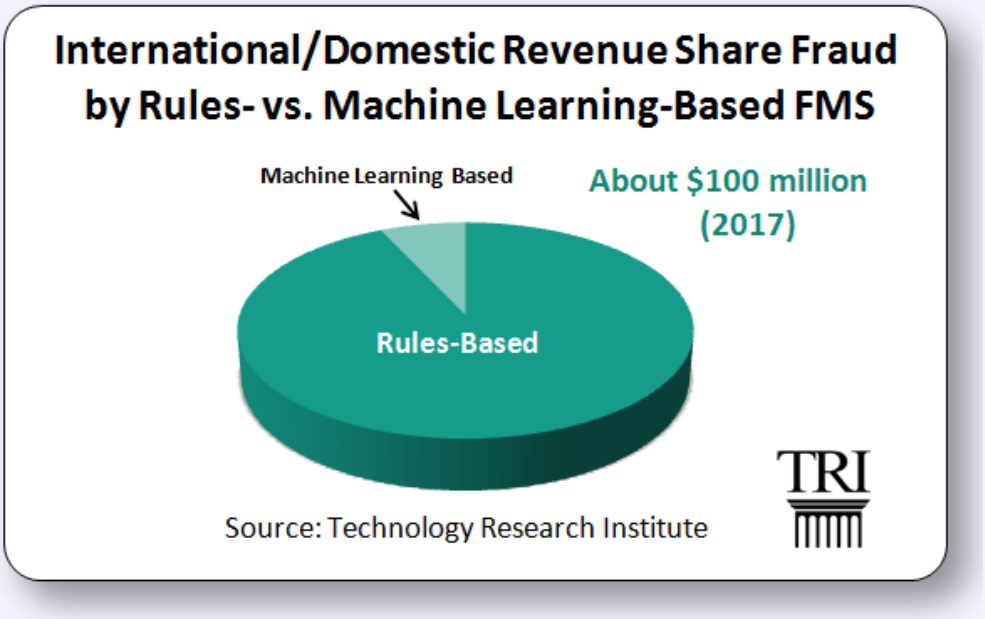
- **Improving machine learning/analytics capability is a winner at the high end.** Mobileum has successfully delivered a machine-learning/analytics-driven Revenue Share solution to a major North American operator.

  A machine learning FMS gives operators a much finer grainer detail on call activity so they can better segment calls into groups that receive tailored real-time treatment depending on a wide range of factors: likelihood of the call being fraud, fraud type,

customer affected, originating phone number, destination number, etc.

Essentially the system allows an operator to deliver a more customer-experience-sensitive fraud program. One treatment policy can be set for VIP customers and another for low value customers, for example.

Thus far, machine-learning/analytics systems represent a small percent of the Revenue Share Fraud solutions market, but we predict excellent growth in this sector for certain types of operator.



- **Cloud will Eventually Lower the Cost of FM Solutions** – In Chapter 3, we hear from PacketFabric, a company who is revolutionizing networking by operating a private network connected to all major data centers in the US (and later the world). By connecting to PacketFabric at only one location, an enterprise can have a presence in all data centers PacketFabric operates in, and by extension, it can reach every application or network that is ported to PacketFabric from any location. Equipped with rapid provisioning and no long term connection commitments, PacketFabric will help drive very cost effective connection – and faster adoption of cloud services.

  Recognizing that cloud is the wave of the future, **WeDo Technologies** recently introduced the first FMS solution across the cloud. Now while most fraud management departments don't yet consider a move to the cloud to be urgent. Cost savings and convenience will in a few years make it highly attractive for combating fraud threats such as Revenue Share.

- **Leading international wholesalers are stepping up their protection of retail partners**. Leading wholesalers realize it's in their best self-interests to help their retail operators block fraudulent traffic. For instance, comprehensive fraud prevention programs are underway at **Tata Communications**; **BICS** has initiated a program enabling its retail operator partners to collaboration with each other; and **iBasis** has developed a systems to actual stop of traffic (as opposed to merely redirecting it) when

fraud is detected and in full policy alignment with the needs of each individual operator. See Chapter 4 for details on what large wholesalers are doing in fraud fighting.

- **Direct International Interconnects to Tier 1 Retail Operators.** In a bid to grow its Tier 2 international wholesaler business, the **Bankai Group** has created a carrier program (with on-line portal ordering) to enable small retail operators and OTTs to connect to international Tier 1 retailers. In this way, OTTs can avoid the need to inefficiently pass through multiple transit carriers to reach international destinations. Bankai merely adds a margin on top of what the destination Tier 1 retailer charges to connect.

  If Bankai succeeds, this may prove an effective way to skirt around tier 3 carriers whose margins are tight and therefore inclined to turn a blind eye to proper fraud controls. So Bankai's program could serve as an effective way to reduce number hijacking IRSF and SIM Box bypass in the market as a whole.

- **Partner Management Solutions on the Rise. Subex,** one of the FMS market leaders **is** carving out a new category in the revenue assurance sector: advanced partner management and settlement. Subex xpands the category beyond traditional cost management to include: Partner/Deal Analysis & Monitoring, Advanced Roaming settlement, Global Services for Travelers, and complex IoT Partner Management.

- **Help is on the Way for Small & Island Countries Who are IRSF Targets –** To get around the issue of blocked international premium rate numbers, fraudsters tend to pick on countries that have high interconnect or termination rates.

  Cook Island is like many countries in the Pacific: its international termination rate is a high 60 cents a minute, a price designed to cover the infrastructure costs of providing service to a very small population. Well, this high termination fee is a magnet to fraudsters. And through schemes such as **Number Misappropriation** or **Number Hijacking,** fraudsters in the transit chain redirect IRSF calls destined for these countries to an IVR machine at an entirely different location. The end result is that operators around the world put Cook Island on their fraud black lists, even though the calls are never landing on Cook Island's numbers.

  Much of the answer to this problem is educating operators on how to best help these small island operators. In Chapters 2 and 4 of this report, consultants **Colin Yates** and **Jan Dingenouts** give solid advice on what needs to be done to correct this unfair treatment of vulnerable small operators.

- **Providing Solutions to Help the Enterprise** – Solution providers are missing the opportunity to extend their Revenue Share Fraud protection to enterprise customers who are vulnerable to PBX attacks and other frauds. **Oculeus** is innovating here by providing its large telecom clients with a way to protect their enterprise clients with a less-than-$50-a-month service the carrier can charge the enterprise for basic fraud protection.

- **Combining CDR and SIP-Based Systems in an FMS.** Today, two very different kinds of FMS systems are vying for attention in revenue share fraud control: CDR-based and SIP based solutions. As you know, CDR-based systems are the veteran systems who dominate the Revenue Share Fraud fight. SIP-based fraud blocking systems are much

simpler and are designed to block VoIP calls in the pre-call phase by dipping into a blacklist database of known fraudulent numbers and number ranges.

There are advantages to both systems and in this Report we examine the strength and weakness of both FMS varieties in depth. On the development front, **Equinox Information Systems** and Oculeus are leading the solution vendors in the race to combine these capabilities on a single platform and we think – with certain exceptions -- it's the wave of the future.

- **Defense-in-Depth Approach to Fraud & IP Security Control**. One of the more interesting research interviews we held was with "cloud play provider" **Evolve IP**, a greater Philadelphia-based OTT who offers a very broad range of data and voice services. Rather than choose one fraud solution, Evolve IP works with multiple vendors in a layered approach.

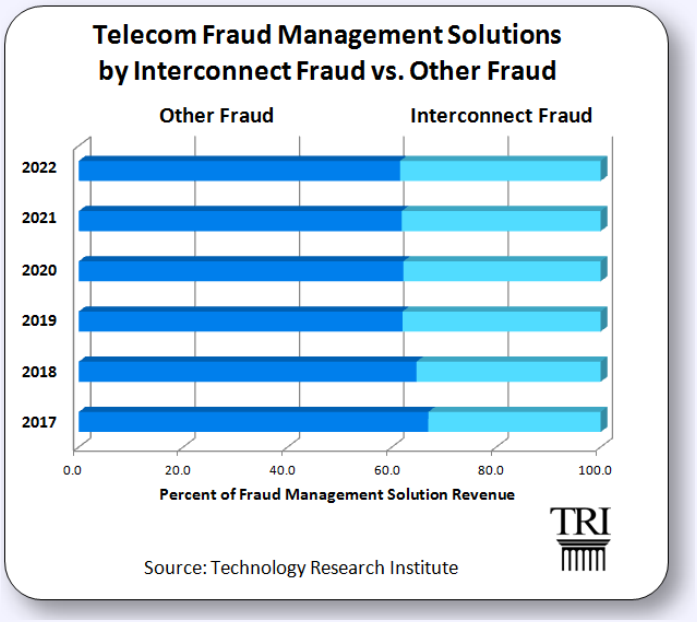
2. Interconnect Fraud

Operators have been fighting interconnect fraud, especially SIM box fraud, for a long time, and yet solution vendors and operators have not succeeded in effectively controlling the fraud.

In many cases, through insider fraud, it's made to appear that SIM Box bypass is a minor issue until a test call company comes in and discovers that significant revenue is being lost.

In recent years, fraudsters have stepped up their game in SIM Box Fraud. Many have transformed their local in-country SIM Box operations to global deployments from a remote command and control location where than can launch SIM Box bypass in several countries simultaneously. The technology that makes this possible is the SIM Server. With a SIM Server, a fraudster can rotate thousands of SIM cards across multiple markets so the usage footprint becomes very, very small. It has made detection a much greater challenge.

And now, other interconnect frauds are appearing or gaining to the point where more serious attention must be paid to the interconnect problem.



If you compare the market for interconnect fraud solutions versus other fraud solutions, we think interconnect fraud will grow from one-third of the market today to about 40% in five years.

Here are some interconnect fraud trends we think are significant:

- **Regulators are stepping up to Lead the SIM Box Bypass Fight in their Countries.** Country regulators want to see SIM box fraud blocked on a national level. But the problem is even if one operator does an excellent job of cleaning its network of bypass, the fraudsters will simply step up their attacks on other operators in the country. So the net effect is that the losses and economic harm still occurs in the country.

  But now, regulators of certain countries are stepping up to fully manage the SIM box bypass problem in their countries. And in Chapter 7 of this Report we hear from the **Regulator in Jordan** who explains how they have succeeded in controlling SIM Box fraud in the country by enacting tough policies and working with vendor partners such as **LATRO Services**.

- **Stealth Test Calls in SIM Box Fraud**. A patented invention by SIGOS (discussed in Chapter 6) may soon become a game changer in stopping SIM Box bypass. SIGOS's technique basically opens up a pool of potential test call numbers in the millions, and in this way makes it nearly impossible for the fraudsters to identify which phone numbers are a test call's path.

- **Managed Services Growth** – Araxxe has succeeded in providing anti-bypass programs as a managed service. Araxxe builds no TCGs itself, but is a big customer of the TCGs manufactured by other firms. Araxxe's success proves that the wise use, deployment, and route selection is the key to getting the most from TCGs.

- **SMS A2P Fraud** is growing as the use of A2P messages ramps up as companies increasingly seek to notify and send marketing messages to mobile users. SMS aggregators such **HAUD Systems** sells an SMS blocking capability. **iconectiv**, a big aggregator itself, goes one step further in a revenue assurance direction: it not only blocks the fraudulent routing, but they also redirects the operator to clean, high quality routes that continue to make money for them. (Details in Chapter 8.)

- **CLI- Refiling** is a pesky problem that got much worse when EU operators recently raised the rates of incoming calls coming from non-EU states. They did this to compensate for the stiff price controls imposed on them for intra-EU calls by the EU regulator. One wholesaler executive told us flat out: "There are no good solutions for this problem yet, and the fraudsters are making barrels of money from this fraud."

- **Outgoing SIM Box Fraud –** In this case, fraudsters exploit the different rates of calls made through a so-called "World Plan" that offers flat rate calling into multiple countries. The fraudsters essentially pump calls into high termination rate countries killing the home operator's profit margin.

- **A Hybrid TCG and FMS System** – SIM Box fraud defense requires speedy coordination between an FMS and the companies making test calls via grey routes to identify the fraudulent SIMs. The quicker you can shut down the illegal SIM, the faster you can prevent a fraudster from making a profit. Trouble is, there's a time lag between

in getting FMS data back to take action.

To cure this delay, solutions are coming that combine test calls with an FMS specifically tuned to the needs of interconnect fraud operations.

- **GSM-to-VIBER Bypass Hijacking** is very deadly to international revenue for mobile operators on the receiving end of international calls because a wholesale transit operator takes the call out of the normal GSM billing schemes to land the call directly a VIBER (or other OTT) app on a mobile phone, thereby bypassing the terminating carrier and any taxes.

  The market has been crying for a technical solution to OTT bypass, and one company, **Revector**, has developed a telco-grade, real-time detector and blocker for GSM-to-VIBER hijacking. TRI conducted an in-depth interview with Revector in Chapter 9.

- **US Regulations are Beginning to Swing toward Protecting Facilities-Based Operators.** The **FCC** (US Federal Communications Commission), now controlled by a Republican administration, has recently ruled to remove certain favorable treatment and price breaks enjoyed by non-facilities competitive operators and OTTs in serving up enterprise services. The net effect of this action is that licensed telecom and cable operators will be strengthened as they compete against OTTs. If these kinds of national policies spread worldwide, then they could help boost governments' ability to police interconnect fraud such as SIM Box bypass and OTT bypass.

3. Customer Onboarding, Subscription Fraud & Credit

Know thy customer. Those words are the spearhead of the massive cross-industry movement to block criminals from penetrating customer accounts or gaining access to services that can absolutely kill a telecom business.

The implications of stopping subscription fraud are enormous: the majority of telecom fraud and bad debts can be stopped if a telecom is vigilant as it onboards customers for services. After all, a fraudster can only abuse your service if you let them have access in the first place.

Here are some of the dramatic developments in one of the hottest sectors of fraud control:

- **Cross-Industry Identity via Biometrics** is getting big attention by the banking industry and is set to revolutionize the way identity is verifying through biometrics and nationally maintained databases. One telecom fraud expert developing these solutions for banks is **FRS Labs** who we interviewed in Chapter 10.

- **A Secure & Simple Mobile App to Block Credit Card Fraud** – While there's a big emphasis today on biometric fraud prevention, start-up **Raptor Labs** offers a secure easy-to-execute-and-use system that uses a mobile app to approve purchases, and requires no exchange of sensitive user or account information.

- **Internal Onboard Systems are a Good Way to Save on Credit Bureau Costs**. **Neural Technologies** delivers solutions that turn an operator's scattered internal intelligence on

prospective customers into a valuable internal onboarding and credit clearance system. In cases where intelligence is lacking, then – and only then – is the decision turned over to a service bureau.

- **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 "unbanked" people around the world. While most of the opportunity is in developing countries, even a developed country like the US has many millions of unbanked consumers.

- **Money Laundering and National Identity Laws** are moving toward safer national global commerce. For example, India has established a national identity database that is holds biometric data on 1 billion people already. And the US government has issued new laws to ensure compliance with anti-money-laundering policies – and this policy is being enforced across all global trading partners of the US.