Analysis, Detection & Control of Telecom Fraud: Voice Bypass (SIM Box)
Rusham Monsoor
MBA (Merit, Sunderland-UK)
PMP
CPA
ACMA (UK)
ACMA (SL)
Six Sigma Yellow Belt Certified - APO
Certified Master of Telecoms Revenue Assurance Management
Certified Telecommunications Fraud Analyst
Introduction to Telecom Fraud
Revenue Assurance
Revenue Assurance

A basic Revenue Assurance definition used by many is: “All products & services delivered as expected; all products & services correctly and completely charged, including expected margin, in a timely manner”

There are many variations to this basic definition, and some derivatives that different organizations will elect to include or exclude from Revenue Assurance scope. There is no absolute right or wrong - each business must define scope to suit specific needs.
Revenue Assurance...

Revenue Assurance (RA) is a niche business activity most commonly undertaken within businesses that provide telecommunication services. The activity is the use of data quality and process improvement methods that improve profits, revenues and cash flows without influencing demand.

In summary Revenue Assurance is Keeping What is yours and only what is yours
fraud
Fraud Management

In law, fraud is deliberate deception to secure unfair or unlawful gain, or to deprive a victim of a legal right. Fraud itself can be:

- A civil offence (i.e., a fraud victim may sue the fraud perpetrator to avoid the fraud and/or recover monetary compensation),

- A criminal offence (i.e., a fraud perpetrator may be prosecuted and imprisoned by governmental authorities)
or it may cause no loss of money, property or legal right but still be an element of another civil or criminal wrong. The purpose of fraud may be monetary gain or other benefits, such as obtaining a driver's license or qualifying for mortgage by way of false statements.

A hoax is a distinct concept that involves deliberate deception without the intention of gain or of materially damaging or depriving a victim.
Watch Out!
Telecom Fraud
Telecom Fraud

Telecommunication fraud is defined as the theft of telecommunication services or the use of telecommunication service to commit other forms of fraud. This type of fraud happens on a daily basis, sometimes without anyone knowing until the damage has already been done.

- Fraud primarily occurs to a Company with a weak defense system. Billing systems and network vulnerabilities are easily exploited to gain access and if proper procedures were put in place it could have easily been prevented.
Telecom Fraud...

- With new voice technologies becoming more attractive, improperly installed systems can be infiltrated easily and put a small Company out of business in mere minutes.

- For example, a technology such as Voice over Internet Protocol (VoIP) uses the Internet to make and receive phone calls, and not infrastructure owned by the traditional telephone networks. Because of it’s affordability, some businesses try to install their own PBX (Private Branch Exchange) systems using an under qualified individual which can result in security leaks and cracks that can be easily exploited.
Key Fraud Types
Other Key Fraud Types

- PBX/Voice mail systems
- Subscription/Identity (ID) Theft
- International Revenue Share Fraud (IRSF)
- Credit Card Fraud
- Many more.....
Introduction to SIM box
By-Pass Fraud

- By-Pass Fraud occurs when in-bound off-net (gateway) traffic is disguised as on-net traffic (By-Pass) to avoid high costs of terminating traffic.

- Most By-Pass operations are performed on a large scale utilizing advanced SIM-Boxes that can be managed from anywhere. Content Service Providers attacked can experience significant losses in their in-bound interconnect revenues.

- Service providers should constantly monitor in-bound and on-net traffic in order to detect any indications associated with By-Pass Fraud, such as suspected calling numbers or suspicious call pattern tendencies.
What is a Sim Box?

- SIM box (also called SIM bank) – is one of hardware modules for GSM termination business.

- SIM box (SIMbox) device holds a bundle of SIM cards separately from VoIP/GSM gateway in order to minimize the maintenance expenses and solve the SIM blocking problem.
How to Buy a SIMbox?

- Ekaterina: Hello, welcome to Antrax. How can I help you today?

- Rusham: Hello

- Rusham: I need to have a quotation for SIMboxes

- Rusham: What are the choices available, large scale?

- Rusham: I am just stepping out

- Rusham: can you mail me on rusham@gmail.com
Ekaterina: In a few words I will tell you how this business works. We offer equipment, which is called GSM gateway.

You insert SIM cards of local operator inside of it and we send some amount of international telephone calls to your equipment with the help of internet connection theses international telephone calls are being transferred into local calls.

So that you pay for local calls made through your equipment, but get payed for international calls being sent to your equipment.
How to Buy a SIMbox?...

- Let me tell you that our equipment is one of the best and safest solutions for GSM termination all over international market.

- Price of the solution includes hardware, software, business plan, your personal manager to deal with all of your inquiries and also traffic manager to provide your gateway with a voice traffic for you to earn money.

- So the price for our solution starts from 7000$. Is this price OK for you?
How to Buy a SIMbox?...

- Rusham: How many SIMs?

- Rusham: and is there anything which is low priced for start up?

- Ekaterina: So price starts from 7000$.

- Ekaterina: we have many different packages as well.
Legitimate use for A SIMbox

- SIMbox per se is **not illegal**.

- It is freely available without any under the table deals as discussed above on ebay.
SIMbox Equipment

New LCD Fixed Wireless Terminal-GSM Dual Gateway Band 900/1800Mhz Worldwide

$31.75
Buy It Now
+$3.56 shipping

80 sold

From Hong Kong

Top-rated seller

32 port Sim Bank remote manage GOIP-4, GOIP-8, GOIP-16, GOIP-32 GSM voip gateway

$318.00
or Best Offer
Free international shipping

47 sold

From Hong Kong

Top-rated seller
SIMbox Equipment

HYPERMEDIA HG4000 VOIP GSM GATEWAY 128 SIM
$4,758.82
or Best Offer
From Germany

2N SIM Star Server + 8 Boards & 8 VoiceBlue Next GSM Gateway & Full Software
$11,500.00
or Best Offer
Free international shipping
From United States
How a Simbox call is established
How does it work
How does the whole Operation work?

- SIMbox or Interconnect Bypass Fraud is one of the most prevalent frauds today, costing the industry more than USD 3Bn.

- Fraudsters effectively bypass the interconnect toll charging points to exploit the difference between the high interconnect rates and the low retail price for on-network calls, thus avoiding payment of the official call termination fee of an Operator or MVNO.

- International Termination Charge $0.136, cost of the local calls $0.02. Available for Fraudster $0.116
How does Fraudster Camouflage

- Fraudsters are smart, technology aware and know how to outfox local operators.

- Experts at masking themselves, they host their equipment where their calls can reach multiple cell sites and get widely dispersed and they send out artificial SMS messages or accept a few incoming calls.

- They are known to use moving vehicles to mask their true intent.
- **LOCAL COST** (Orange), 0.01$ MIN
- **ROUTE COST** (to Kenya), 0.04$ MIN
- **GROSS MARGIN** (difference between local cost and rate of route), 0.03$ MIN
- **INCOME** (average turnover), **MONTHLY up to 8 000$**
- **INITIAL INVESTMENT** (for whole business launching) starts from 10 000$
- LOCAL COST (Mobile Smart, Philippines), 0.02$ MIN
- ROUTE COST (to Philippines), 0.07$ MIN
- GROSS MARGIN (difference between local cost and rate of route), 0.05$ MIN
- INCOME (average turnover), **MONTHLY up to 12 000$**
- INITIAL INVESTMENT (for whole business launching) starts from 10 000$
- LOCAL COST (Beeline), 0.05$ MIN
- ROUTE COST (to Armenia), 0.11$ MIN
- GROSS MARGIN (difference between local cost and rate of route), 0.06$ MIN
- INCOME (average turnover), **MONTHLY up to 12 000$**
- INITIAL INVESTMENT (for whole business launching) starts from 10 000$
- LOCAL COST (Uganda, Orange), 0.05$ MIN
- ROUTE COST (to Uganda), 0.16$ MIN
- GROSS MARGIN (difference between local cost and rate of route), 0.11$ MIN
- INCOME (average turnover), **MONTHLY up to 26 000$**
- INITIAL INVESTMENT (for whole business launching) starts from 10 000$
How much can a fraudster earn?

https://en.antrax.mobi/request-pricing/
# Termination rates to Jordan

<table>
<thead>
<tr>
<th>Country</th>
<th>Destination</th>
<th>Country Code</th>
<th>City Codes</th>
<th>Price ($)</th>
<th>Prime Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jordan</td>
<td>Orange Mobile</td>
<td>962</td>
<td>77</td>
<td>0.136</td>
<td>CLI Assured</td>
</tr>
<tr>
<td>Jordan</td>
<td>Other</td>
<td>962</td>
<td></td>
<td>0.126</td>
<td>Direct Assured</td>
</tr>
<tr>
<td>Jordan</td>
<td>Umniah Mobile</td>
<td>962</td>
<td>78</td>
<td>0.136</td>
<td>Direct Assured</td>
</tr>
<tr>
<td>Jordan</td>
<td>Zain Mobile</td>
<td>962</td>
<td>75, 79</td>
<td>0.136</td>
<td>CLI Assured</td>
</tr>
</tbody>
</table>
Adversities
Adversities (Difficulties)

- The obvious loss is the financial loss to the operators and intern to the regulator and the government.

- There are more externalities to this, this has a major impact on business communication, as the call qualities are very low when routed through SIMbox International Business dealings are impacted.

- When calls are routed to FAS, the called party would not know of such an event.

- If calls are missed, chances of knowing who called is very minimal, and hence it can not be returned.
Simboxes in Jordan
Simboxes confiscated in Jordan
Sim Box Countermeasures

- Fraud Management System
- Test Call Generators
- Call Detailed Record Analysis
- Control ISPs
- Consumer Feedback
- Limit the number connection
- Biometric Activations
- Negotiate Termination Rates
- Revise Termination Rate
- Locate and Bust
- Special Price Plan
- Hot List Monitoring
Fraud Management System

- Built-in statistical functions for detecting SIMboxes
- Special algorithms to identify bypassed calls
- Tools to define and test SIMbox profiles
- White-listing of trusted corporate SIMboxes
- CDR data browsing and case management
- 100% coverage of the customer network data
Fraud Management System...

- It detects SIMboxes efficiently with minimum administration
- It documents bypassed calls and measures the associated revenue losses
- Low cost of ownership (no 3rd party software fees)
- It provides FMS tools (case management, CDR storage, etc)
- User-friendly Web interface for real-time access and control
There are many FMS providers, who have embedded algorithms to capture SIM box based on past behavioral patterns.

Hence the reliability of such information is not very high, hence it is recommended to automate termination, but may suspend the line immediately.

Get the Fraud Management team to investigate the usage pattern and act upon it.
Test Call Generation Solution for Detecting & Stopping International Bypass
Test Call Generators

- Monitoring your incoming traffic to detect your SIM cards in SIM boxes bypassing your interconnect gateways and leading to wholesale termination revenue losses:
  - Detection calls generation from a unique portfolio of 2,800+ routes (including all types of operators/routes worldwide) towards your network.
  - Use at least 3 TCGs from different parts of the world.
Test Call Generators

- Identification of your fraudulent SIM cards used in SIM boxes together with:
  - Systematic material proofs of bypass
  - ‘Real’ Real time alerts notification sent

- Maximization of the probability to detect bypass with specific call campaign

- Analysis and presentation of actionable findings with formal proofs of fraud and detailed technical trace.
<table>
<thead>
<tr>
<th>Probe ID</th>
<th>Call ID</th>
<th>Orig</th>
<th>Calling</th>
<th>Called</th>
<th>Start</th>
<th>Released</th>
<th>Duration</th>
<th>Rel Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTCARD1</td>
<td>11111611506-3</td>
<td>New York(#2.2)</td>
<td>3016243333</td>
<td>3019243333</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:05</td>
<td>00:00:41</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-24</td>
<td>New York(#2.2)</td>
<td>3017242222</td>
<td>3019242229</td>
<td>11/16/2011 11:15:29</td>
<td>11/16/2011 11:16:11</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-2</td>
<td>New York(#2.1)</td>
<td>3016042222</td>
<td>3019242222</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:07</td>
<td>00:00:43</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-19</td>
<td>New York(#2.18)</td>
<td>3017242218</td>
<td>3019242218</td>
<td>11/16/2011 11:15:25</td>
<td>11/16/2011 11:16:08</td>
<td>00:00:43</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-16</td>
<td>New York(#2.15)</td>
<td>3015242215</td>
<td>3019242215</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-17</td>
<td>New York(#2.16)</td>
<td>3016242216</td>
<td>3019242216</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-14</td>
<td>New York(#2.13)</td>
<td>3016242213</td>
<td>3019242213</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:07</td>
<td>00:00:43</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-12</td>
<td>New York(#2.11)</td>
<td>3016241011</td>
<td>3019242211</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-11</td>
<td>New York(#2.10)</td>
<td>3016241010</td>
<td>3019241010</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-9</td>
<td>New York(#2.9)</td>
<td>3019242889</td>
<td>3017242239</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-8</td>
<td>New York(#2.7)</td>
<td>3019242237</td>
<td>3016242237</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:07</td>
<td>00:00:43</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-7</td>
<td>New York(#2.6)</td>
<td>3019242236</td>
<td>3016242236</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-6</td>
<td>New York(#2.5)</td>
<td>3019242235</td>
<td>3016242235</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-5</td>
<td>New York(#2.4)</td>
<td>3019242234</td>
<td>3016242234</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-4</td>
<td>New York(#2.3)</td>
<td>3019242233</td>
<td>3016242233</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:05</td>
<td>00:00:41</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>11111611506-22</td>
<td>New York(#2.21)</td>
<td>3019242221</td>
<td>3016242220</td>
<td>11/16/2011 11:15:25</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:41</td>
<td>Normal</td>
</tr>
</tbody>
</table>
CDR Analysis

- Arguably the best detection mechanism, but has a number of constraints in achieving satisfactory results.

- Operators who are totally dependent on 3rd parties for bypass fraud detection are at a risk of not knowing and understanding the intensity of this fraud plus missing out on valuable learning that they could gain.

- On the other hand, 3rd party companies are necessary for Test call generation and actual probing & identification of fraudster’s physical locations for raids to be carried out.
C DR Analysis

- One of the key skills an operator could acquire in identifying SIM Box numbers is CDR Analysis.

- Data is powerful and it speaks a lot if carefully studied and analyzed. Most solution providers use standard SIM Box detection algorithm to filter the MSISDNs such as:
  - High Volume of calls from same MSISDNs
  - High volume of calls from same CELL ID
  - Outgoing and incoming call ratio
  - Local and international call ratio
  - Numbers having same running sequence
CDR Analysis

First extract CDRs of known cases of the bypass fraud and study in detail the patterns.

• Some key figures to consider while performing CDR analysis:

  • Number of calls within a fixed period (1 or 2 hours)
  • Number of calls to different unique B-party
  • Number of calls in a sequence within a period
  • Number of minutes between each call in the sequence
  • Number of calls with same Cell ID within a period
  • Number of B-Party random numbers
  • Number of days since the A-Party number was activated (1st call flagged)
Control Internet Service Providers

- Fraudsters are able to continue the way they wish just because they have the services from ISPs

- If ISPs are regulated and heavy fines are imposed on them for providing services for fraudsters, this will disable the freewill operations of the SIMboxers

- Introduce KYC / Stricter controls for Lease lines and high capacity broadband connections
Consumer Feedback

- Regulator could introduce a toll free short-code service where consumers can text the local numbers they received an International call from.

- All such MSISDNs should be sent to the respective operators for further investigation, as it could contain false reporting.
Limit the number of connections

- Regulate activation process, and limit the number of connection per identification document.
- Re-register all active lines with Biometrics, provide deadlines to MNOs to complete the registration process, and terminate all unregistered SIMs.
- Create a centralized server in which all connections held with all operators are logged, and avoid duplication by checking the central server before allowing new connections.
- Activation authorization could be controlled by the server.
Activation on Biometrics

- Post creation of the server, Activation authorization should be obtained from the server, based on the Biometric information.

- This will limit drastically drop the false or fraudulent activations
Operators or the Regulator should negotiate termination rates with the carriers and arrive at an optimal rate, where ILD Carriers will be able to collect white route calls, with minimal impact on Termination Revenue.
Narrow the Gap

- This may not be the best of options, but is one of the most successful methods to eradicate SIMbox.

- Regulator should try to minimize the gap between the local termination rates and International termination rates, hence the benefit to the fraudster shrinks, and ultimately it becomes a market not worth operating in.
Narrow the Gap...

- A good example is Malaysia where the International Termination rates has been revised from 0.0325 (MYR 0.144) to 0.0126 (MYR 0.056)

- Where in the case local termination rates the lowest is 6 Sen and some networks charge an exorbitant 12 Sen.

- As the gap has narrowed or crossed, SIMbox does not exists in Malaysia anymore.
Locate and Bust

- Experts providing this service in the region is *Latro Services Inc.*
Locate and Bust...

- Analyze

- Provide analysis using CDRs and Test Call detections.
  - Gather data
  - Look for patterns
  - Calculate location estimate
  - LATRO provides optional data collection
Locate and Bust...

- Locate

- Search algorithms provide location estimates and a complete picture of the bypass fraud.
  - RF Test
  - On-site service
  - Portable RF Measurement System to pinpoint and isolate the location of the bypass operations
Locate and Bust...

IMSI and IMEI catcher

GSM IMSI/IMEI catcher is a device used to detect mobile phones active in specific area as well as to precisely detect their location with accuracy less than 1 meter.

This unit has been designed primarily for law enforcement and police forces increasing the effectiveness of target cell phones tracking and localization.

Other applications of this equipment may include detection of active cellular handsets at border check points, airport luggage check-in areas, conference rooms, SIMBox Localization etc.

Locate and Bust...

- Eliminate

- Provide findings to authorities to support takedown.
  - Investigation report
  - Authority consultation
  - Authorities shutdown fraud operations location of the bypass fraud operations
Special Price Plan

- If you can't fight them join them
- What is the net loss for a minute
- Create a special SIMbox plan
- Migrate all detected numbers to it
Hotlist Monitoring for Frauds

• **GSMA Hotlist**
  This is a list of IRSF numbers built up by GSMA using inputs from member operators worldwide. The list is split into multiple sheets, which contains the top most occurrence, recent updates and removed on request.

• **Unallocated Number Ranges**
  Fraudsters are keen on masking their A numbers, and at times CLI provided could be from an un allocated number range in called party’s country. So by creating an alert for it, could give a heads up.
Hotlist Monitoring for Frauds...

• Premium Number Prefixes
  This is more of GSMA hot list, but usually built up by the company itself.

• High Termination Cost Destinations
  International Revenue Share Fraud
### GSMA Hot List

<table>
<thead>
<tr>
<th>Number</th>
<th>Range (CC4 digits)</th>
<th>Country</th>
<th>Fraud Type</th>
<th>Source TADIG code (most recent)</th>
<th>Source Organisation</th>
<th>Source Country</th>
<th>Date Added (most recent)</th>
<th>Number of Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>447418420001</td>
<td>447418 United Kingdom</td>
<td>IRSF</td>
<td>SWEIQ</td>
<td>Tele 2 AB</td>
<td>SWEDEN</td>
<td>11/11/2016</td>
<td>369</td>
<td></td>
</tr>
<tr>
<td>38599980007</td>
<td>3859998 Croatia</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>04/05/2016</td>
<td>367</td>
<td></td>
</tr>
<tr>
<td>447589034313</td>
<td>447589 United Kingdom</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>04/05/2016</td>
<td>186</td>
<td></td>
</tr>
<tr>
<td>242016570004</td>
<td>2420165 Republic of the Congo (Br)</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>29/07/2016</td>
<td>185</td>
<td></td>
</tr>
<tr>
<td>231332512146</td>
<td>2313325 Liberia</td>
<td>IRSF</td>
<td>IRLME Limited</td>
<td>IRELAND</td>
<td>31/05/2016</td>
<td>174</td>
<td></td>
<td></td>
</tr>
<tr>
<td>385910210031</td>
<td>3859102 Croatia</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>29/07/2016</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>447021001400</td>
<td>447021 United Kingdom</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>23/12/2016</td>
<td>145</td>
<td></td>
</tr>
<tr>
<td>85021811111</td>
<td>8502181 Korea (North)</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>10/04/2015</td>
<td>127</td>
<td></td>
</tr>
<tr>
<td>18672925445</td>
<td>18672925 Canadian Arctic Territories</td>
<td>IRSF</td>
<td>RUSNW</td>
<td>MegaFon, Open Joint Stock Company</td>
<td>RUSSIA</td>
<td>01/02/2016</td>
<td>116</td>
<td></td>
</tr>
<tr>
<td>242011580002</td>
<td>2420115 Republic of the Congo (Br)</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>29/07/2016</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>
Mahmoud Kamel
Email: Mkamel@Tfkeir.com
Cell: +962 791548440
Fixed: +962 65544 664

Rusham Monsoor
Email: rusham@gmail.com
Cell: +94 77 7874266
+94 77 RushamM
How does the whole Operation work?

- SIMbox or Interconnect Bypass Fraud is one of the most prevalent frauds today, costing the industry more than USD 3Bn.

- Fraudsters effectively bypass the interconnect toll charging points to exploit the difference between the high interconnect rates and the low retail price for on-network calls, thus avoiding payment of the official call termination fee of an Operator or MVNO.
How does the whole Operation work?...

- There are two unavoidable reasons for the surge and persistence of this type of fraud.

- The **first** is the use of pre-paid SIM cards. Most commonly used by fraudsters, their ownership and address are much harder to trace compared to the easily traceable post-paid SIMs.

- Problem is serious in countries where the incoming international traffic rates are high and controls are lax in terms of availability of SIMs and law enforcement.
How does the whole Operation work?...

- The **second** issue is the subscriber churn (mix) rate between Operators in the market. The telecommunications industry operates in a low customer loyalty environment.

- Fraudsters usually take advantage of cheap packages including bundled offers, which earn lower per-minute revenue to the operator than the interconnect rate they can earn from the international carriers.
How does the whole Operation work?...

- Due to this highly competitive market and the low customer loyalty phenomenon, the cost of all-inclusive bundles is driven down.

- And disposing of bundle offers and cheap packages is not an option.
How does the whole Operation work?...

- Fraudsters are smart, technology aware and know how to outfox local operators.

- Experts at masking themselves, they host their equipment where their calls can reach multiple cell sites and get widely dispersed and they send out artificial SMS messages or accept a few incoming calls.

- They are known to use moving vehicles to mask their true intent.
- LOCAL COST (Orange), 0.01$ MIN
- ROUTE COST (to Kenya), 0.04$ MIN
- GROSS MARGIN (difference between local cost and rate of route), 0.03$ MIN
- INCOME (average turnover), **MONTHLY up to 8 000$**
- INITIAL INVESTMENT (for whole business launching) starts from 10 000$
- LOCAL COST (Mobile Smart, Philippines), 0.02$ MIN
- ROUTE COST (to Philippines), 0.07$ MIN
- GROSS MARGIN (difference between local cost and rate of route), 0.05$ MIN
- INCOME (average turnover), **MONTHLY up to 12 000$**
- INITIAL INVESTMENT (for whole business launching) starts from 10 000$
- LOCAL COST (Beeline), 0.05$ MIN
- ROUTE COST (to Armenia), 0.11$ MIN
- GROSS MARGIN (difference between local cost and rate of route), 0.06$ MIN
- INCOME (average turnover), **MONTHLY up to 12 000$**
- INITIAL INVESTMENT (for whole business launching) starts from 10 000$
- LOCAL COST (Uganda, Orange), 0.05$ MIN
- ROUTE COST (to Uganda), 0.16$ MIN
- GROSS MARGIN (difference between local cost and rate of route), 0.11$ MIN
- INCOME (average turnover), **MONTHLY up to 26 000$**
- INITIAL INVESTMENT (for whole business launching) starts from 10 000$
How much can a fraudster earn?

https://en.antrax.mobi/request-pricing/
Termination rates to Jordan

<table>
<thead>
<tr>
<th>Country</th>
<th>Destination</th>
<th>Country Code</th>
<th>City Code(s)</th>
<th>Price($)</th>
<th>Prime Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jordan</td>
<td>Orange Mobile</td>
<td>962</td>
<td>77</td>
<td>0.136</td>
<td>CLI Assured</td>
</tr>
<tr>
<td>Jordan</td>
<td>Other</td>
<td>962</td>
<td></td>
<td>0.126</td>
<td>Direct Assured</td>
</tr>
<tr>
<td>Jordan</td>
<td>Umniah Mobile</td>
<td>962</td>
<td>78</td>
<td>0.136</td>
<td>Direct Assured</td>
</tr>
<tr>
<td>Jordan</td>
<td>Zain Mobile</td>
<td>962</td>
<td>75, 79</td>
<td>0.136</td>
<td>CLI Assured</td>
</tr>
</tbody>
</table>
Adversities (Difficulties)

- The obvious loss is the financial loss to the operators and intern to the regulator and the government.

- There are more externalities to this, this has a major impact on business communication, as the call qualities are very low when routed through SIMbox International. Business dealings are impacted.

- When calls are routed to FAS, the called party would not know of such an event.

- If calls are missed, chances of knowing who called is very minimal, and hence it can not be returned.
Simboxes confiscated in Jordan
Sim Box Countermeasures
Sim Box Countermeasures

- Fraud Management System
- Test Call Generators
- Call Detailed Record Analysis
- Control ISPs
- Consumer Feedback
- Limit the number connection
- Biometric Activations
- Negotiate Termination Rates

- Revise Termination Rate
- Locate and Bust
- Special Price Plan
- Hot List Monitoring
Fraud Management System

- Built-in statistical functions for detecting SIMboxes
- Special algorithms to identify bypassed calls
- Tools to define and test SIMbox profiles
- White-listing of trusted corporate SIMboxes
- CDR data browsing and case management
- 100% coverage of the customer network data
Fraud Management System...

- It detects SIMboxes efficiently with minimum administration

- It documents bypassed calls and measures the associated revenue losses

- Low cost of ownership (no 3rd party software fees)

- It provides FMS tools (case management, CDR storage, etc)

- User-friendly Web interface for real-time access and control
Fraud Management System...

- There are many FMS providers, who have embedded algorithms to capture SIM box based on past behavioral patterns.

- Hence the reliability of such information is not very high, hence it is recommended to automate termination, but may suspend the line immediately.

- Get the Fraud Management team to investigate the usage pattern and act upon it.
Test Call Generation Solution for Detecting & Stopping International Bypass
Test Call Generators

- Monitoring your incoming traffic to detect your SIM cards in SIM boxes bypassing your interconnect gateways and leading to wholesale termination revenue losses:

- Detection calls generation from a unique portfolio of 2,800+ routes (including all types of operators/routes worldwide) towards your network.

- Use at least 3 TCGs from different parts of the world
Test Call Generators

- Identification of your fraudulent SIM cards used in SIM boxes together with:
  - Systematic material proofs of bypass
  - ‘Real’ Real time alerts notification sent

- Maximization of the probability to detect bypass with specific call campaign

- Analysis and presentation of actionable findings with formal proofs of fraud and detailed technical trace.
<table>
<thead>
<tr>
<th>Probe ID</th>
<th>Call ID</th>
<th>Orig</th>
<th>Calling</th>
<th>Called</th>
<th>Start</th>
<th>Released</th>
<th>Duration</th>
<th>Rel Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTCARD1</td>
<td>111116111506-3</td>
<td>New York(#2.2)</td>
<td>3016243333</td>
<td>3019243333</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:05</td>
<td>00:00:41</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-24</td>
<td>New York(#2.22)</td>
<td>3017242222</td>
<td>3019242229</td>
<td>11/16/2011 11:15:29</td>
<td>11/16/2011 11:16:11</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-2</td>
<td>New York(#2.1)</td>
<td>3016042222</td>
<td>3019242222</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:07</td>
<td>00:00:43</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-21</td>
<td>New York(#2.20)</td>
<td>3012242220</td>
<td>3019242220</td>
<td>11/16/2011 11:15:25</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:41</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-19</td>
<td>New York(#2.18)</td>
<td>3017242182</td>
<td>3019242182</td>
<td>11/16/2011 11:15:25</td>
<td>11/16/2011 11:16:08</td>
<td>00:00:43</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-16</td>
<td>New York(#2.15)</td>
<td>3016242161</td>
<td>3019242161</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-15</td>
<td>New York(#2.14)</td>
<td>3016242144</td>
<td>3019242144</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-14</td>
<td>New York(#2.13)</td>
<td>3016242133</td>
<td>3019242133</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:07</td>
<td>00:00:43</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-13</td>
<td>New York(#2.12)</td>
<td>3016242121</td>
<td>3019242121</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-12</td>
<td>New York(#2.11)</td>
<td>3016242111</td>
<td>3019242111</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-11</td>
<td>New York(#2.10)</td>
<td>3016241010</td>
<td>3019241010</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-10</td>
<td>New York(#2.9)</td>
<td>3019242899</td>
<td>3017242399</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-9</td>
<td>New York(#2.8)</td>
<td>3019242888</td>
<td>3017242388</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-8</td>
<td>New York(#2.7)</td>
<td>3019242373</td>
<td>3016242373</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:07</td>
<td>00:00:43</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-7</td>
<td>New York(#2.6)</td>
<td>3019242236</td>
<td>3016242236</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-5</td>
<td>New York(#2.4)</td>
<td>3019242234</td>
<td>3016242234</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-4</td>
<td>New York(#2.5)</td>
<td>3019242235</td>
<td>3016242235</td>
<td>11/16/2011 11:15:24</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:42</td>
<td>Normal</td>
</tr>
<tr>
<td>ATTCARD1</td>
<td>111116111506-22</td>
<td>New York(#2.21)</td>
<td>3019242221</td>
<td>3016242220</td>
<td>11/16/2011 11:15:25</td>
<td>11/16/2011 11:16:06</td>
<td>00:00:41</td>
<td>Normal</td>
</tr>
</tbody>
</table>
CDR Analysis

- Arguably the best detection mechanism, but has a number of constraints in achieving satisfactory results.

- Operators who are totally dependent on 3rd parties for bypass fraud detection are at a risk of not knowing and understanding the intensity of this fraud plus missing out on valuable learning that they could gain.

- On the other hand, 3rd party companies are necessary for Test call generation and actual probing & identification of fraudster’s physical locations for raids to be carried out.
CDR Analysis

- One of the key skills an operator could acquire in identifying SIM Box numbers is CDR Analysis.

- Data is powerful and it speaks a lot if carefully studied and analyzed. Most solution providers use standard SIM Box detection algorithm to filter the MSISDNs such as:
  - High Volume of calls from same MSISDNs
  - High volume of calls from same CELL ID
  - Outgoing and incoming call ratio
  - Local and international call ratio
  - Numbers having same running sequence
CDR Analysis

First extract CDRs of known cases of the bypass fraud and study in detail the patterns.

• Some key figures to consider while performing CDR analysis:
  
  • Number of calls within a fixed period (1 or 2 hours)
  • Number of calls to different unique B-party
  • Number of calls in a sequence within a period
  • Number of minutes between each call in the sequence
  • Number of calls with same Cell ID within a period
  • Number of B-Party random numbers
  • Number of days since the A-Party number was activated (1st call flagged)
Control Internet Service Providers
Control Internet Service Providers

- Fraudsters are able to continue the way they wish just because they have the services from ISPs

- If ISPs are regulated and heavy fines are imposed on them for providing services for fraudsters, this will disable the freewill operations of the SIMboxers

- Introduce KYC / Stricter controls for Lease lines and high capacity broadband connections
Consumer Feedback

- Regulator could introduce a toll free short-code service where consumers can text the local numbers they received an International call from

- All such MSISDNs should be sent to the respective operators for further investigation, as it could contain false reporting
Limit the number of connections

- Regulate activation process, and limit the number of connection per identification document.

- Re-register all active lines with Biometrics, provide deadlines to MNOs to complete the registration process, and terminate all unregistered SIMs.

- Create a centralized server in which all connections held with all operators are logged, and avoid duplication by checking the central server before allowing new connections.

- Activation authorization could be controlled by the server.
Activation on Biometrics

- Post creation of the server, Activation authorization should be obtained from the server, based on the Biometric information.

- This will limit drastically drop the false or fraudulent activations
Negotiate Rates

- Operators or the Regulator should negotiate termination rates with the carriers and arrive at an optimal rate, where ILD Carriers will be able to collect white route calls, with minimal impact on Termination Revenue.
Narrow the Gap

- This may not be the best of options, but is one of the most successful methods to eradicate SIMbox.

- Regulator should try to minimize the gap between the local termination rates and International termination rates, hence the benefit to the fraudster shrinks, and ultimately it becomes a market not worth operating in.
Narrow the Gap...

- A good example is Malaysia where the International Termination rates has been revised from 0.0325 (MYR 0.144) to 0.0126 (MYR 0.056)

- Where in the case local termination rates the lowest is 6 Sen and some networks charge an exorbitant 12 Sen.

- As the gap has narrowed or crossed, SIMbox does not exists in Malaysia anymore.
Locate and Bust
Locate and Bust

- Experts providing this service in the region is *Latro Services Inc.*
Locate and Bust...

- Analyze

- Provide analysis using CDRs and Test Call detections.
  - Gather data
  - Look for patterns
  - Calculate location estimate
  - LATRO provides optional data collection
Locate and Bust...

- Locate

- Search algorithms provide location estimates and a complete picture of the bypass fraud.
  - RF Test
  - On-site service
  - Portable RF Measurement System to pinpoint and isolate the location of the bypass operations
Locate and Bust...

IMSI and IMEI catcher

GSM IMSI/IMEI catcher is a device used to detect mobile phones active in specific area as well as to precisely detect their location with accuracy less than 1 meter.

This unit has been designed primarily for law enforcement and police forces increasing the effectiveness of target cell phones tracking and localization.

Other applications of this equipment may include detection of active cellular handsets at border check points, airport luggage check-in areas, conference rooms, SIMBox Localization etc.

Locate and Bust...

- Eliminate

- Provide findings to authorities to support takedown.
  - Investigation report
  - Authority consultation
  - Authorities shutdown fraud operations location of the bypass fraud operations
Special Price Plan

- If you can't fight them join them
- What is the net loss for a minute
- Create a special SIMbox plan
- Migrate all detected numbers to it
THE HOT LIST
Hotlist Monitoring for Frauds

• GSMA Hotlist
This is a list of IRSF numbers built up by GSMA using inputs from member operators worldwide. The list is split into multiple sheets, which contains the top most occurrence, recent updates and removed on request

• Unallocated Number Ranges
Fraudsters are keen on masking their A numbers, and at times CLI provided could be from an un allocated number range in called party’s country. So by creating an alert for it, could give a heads up
Hotlist Monitoring for Frauds...

- **Premium Number Prefixes**
  This is more of GSMA hot list, but usually built up by the company itself.

- **High Termination Cost Destinations**
  International Revenue Share Fraud
## GSMA Hot List

<table>
<thead>
<tr>
<th>Number</th>
<th>Range (CC+4 digits)</th>
<th>Country</th>
<th>Fraud Type</th>
<th>Source TADIG code (most recent)</th>
<th>Source Organisation</th>
<th>Source Country</th>
<th>Date Added (most recent)</th>
<th>Number of Occurrences</th>
</tr>
</thead>
<tbody>
<tr>
<td>447418420001</td>
<td>447418</td>
<td>United Kingdom</td>
<td>IRSF</td>
<td>SWEIQ</td>
<td>Tele 2 AB</td>
<td>SWEDEN</td>
<td>11/11/2016</td>
<td>369</td>
</tr>
<tr>
<td>385999800007</td>
<td>3859998</td>
<td>Croatia</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>04/05/2016</td>
<td>367</td>
</tr>
<tr>
<td>447589034313</td>
<td>447589</td>
<td>United Kingdom</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>04/05/2016</td>
<td>186</td>
</tr>
<tr>
<td>242016570004</td>
<td>2420165</td>
<td>Republic of the Congo (Br)</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>29/07/2016</td>
<td>185</td>
</tr>
<tr>
<td>231332512146</td>
<td>2313325</td>
<td>Liberia</td>
<td>IRSF</td>
<td>IRLME Limited</td>
<td></td>
<td>IRELAND</td>
<td>31/05/2016</td>
<td>174</td>
</tr>
<tr>
<td>385910210031</td>
<td>3859102</td>
<td>Croatia</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>29/07/2016</td>
<td>172</td>
</tr>
<tr>
<td>447021001400</td>
<td>447021</td>
<td>United Kingdom</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>23/12/2016</td>
<td>145</td>
</tr>
<tr>
<td>85021811111</td>
<td>8502181</td>
<td>Korea (North)</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>10/04/2015</td>
<td>127</td>
</tr>
<tr>
<td>18672925445</td>
<td>18672925</td>
<td>Canadian Arctic Territorie</td>
<td>IRSF</td>
<td>RUSNW</td>
<td>MegaFon, Open Joint Stock Company</td>
<td>RUSSIA</td>
<td>01/02/2016</td>
<td>116</td>
</tr>
<tr>
<td>242011580002</td>
<td>2420115</td>
<td>Republic of the Congo (Br)</td>
<td>IRSF</td>
<td>USAAT</td>
<td>AT&amp;T Mobility</td>
<td>UNITED STATES</td>
<td>29/07/2016</td>
<td>100</td>
</tr>
</tbody>
</table>
Mahmoud Kamel
Email: Mkamel@Tfkeir.com
Cell : +962 791548440
Fixed: +962 65544 664

Rusham Monsoor
Email: rusham@gmail.com
Cell : +94 77 7874266
+94 77 RushamM