How Regulators Can Lead the Fight Against International Bypass Fraud

Six Proactive Steps Regulators Can Take to Better Manage the Problem and Protect Their Nations from Huge Revenue Losses & Infrastructure Damage

By Dan Baker, Technology Research Institute (TRI)

TRI

No one can give you an accurate worldwide figure on the taxes lost and national infrastructure damaged due to international bypass fraud via illegal SIM Box activity.

In fact, no international or watchdog organization — ITU, United Nations, etc. — has released authoritative figures on national losses from bypass.

Yet, to nations infected by International Bypass, the symptoms are very obvious: tax revenues from international voice traffic are in decline; the quality of voice service is getting worse; and licensed telecom operator profits are being hurt.

So, as a regulator, policy maker or law enforcement expert in an infected country, what can you do to improve the situation?

What steps can and should you take – at the national government level – to better protect your country's tax revenue, quality of communications, and national infrastructure?

Well, answering that question is the purpose of this white paper.

Our aim is to offer some perspective and advice on national regulatory strategies to cure the bypass disease.

For the past few years, my organization, Technology Research Institute (TRI), has interviewed dozens of telecoms, consultants, and fraud management (FM) experts around the globe to get a handle on how telecom fraud is being detected and stopped. That research led us to publish a comprehensive 239-page report entitled, Telecom Fraud Management Services, Software & Strategies.

Our research concluded that SIM Box bypass is one of the toughest fraud problems telecom operators face. Globally, operators spend about $51 million a year on bypass fraud management solutions each year. Operators actually detect and block fairly large volumes of SIM Boxes on a daily basis, yet sadly the problem very often doesn't go away.

In short, the fraudsters succeed despite the anti-fraud efforts of the operators. They simply replace the blocked SIM cards with fresh supplies of SIMs and continue their bypass!

At the national level, the problem goes even deeper. If one operator does an excellent job of cleaning its network of bypass, then the fraudsters will simply step up their attacks on the other operators in the country. So the net effect is that the losses and economic harm still occurs in the country.

Clearly then, it's time for national regulators to consider new options. For if they don't successfully manage and monitor bypass fraud on a national basis, the problem may never go away.

And if you agree that regulators need to proactively manage the bypass problem, how should they do that? What strategies make sense? And what are the lessons learned from regulators in other countries who struggle with the same fraud problem?

To help answer these questions, we'll cover the following topics to:

- Show the damage to financial and national infrastructure which is caused by bypass fraud;
- Explain the deceive, divide and conquer strategies fraudsters use to maximize the money they steal;
- Discuss why regulators should lead the national bypass FM effort rather than defer the problem to the licensed telecom operators.
- Recommend specific steps regulators should take to better manage and coordinate the national bypass fraud problem; and,
- Review the successful case of a regulator in the Middle East who took a leadership role in bypass control.

Let's begin.

Overview of Financial & National Infrastructure Damage

The damage caused by international voice bypass is substantial and goes far beyond the loss of national tax revenue. Here's a quick rundown on its impact:

Financial & Revenue Loss

- Tax Revenue Loss — As you well know, bypass causes huge losses in the international voice call taxes used to fund national infrastructure and other government programs.

- Operator Revenue Loss — Unlicensed SIM Box operators rob the licensed telecom operators of their livelihood, jeopardizing their ability to compete and serve customers well.

National Infrastructure & Service Quality Damage

- Damage to National Infrastructure – When bypass fraudsters destroy the incentive for licensed operator to invest in their networks, the whole nation feels the impact of degraded comms infrastructure.

- Quality of Service Declines — Fraudsters lower the average QoS of a nation's voice service because they use cheap, low quality equipment to cut their costs.

Security & Privacy Damage

- Lawful intercept systems are bypassed — Illegal SIM Box terminated calls sidestep the lawful surveillance systems that police and intelligence agencies use to track criminals and terrorists.

- Voice Privacy and Security Protections -- Public networks have security, privacy, and encryption built in, but bypass networks are often sent in the clear allowing criminals or hackers to listen in on conversations.

- SMS messages are compromised — SMS messages are also compromised by bypass. This is especially troubling since SMS has become a major communication channel for confidential and personal data. Application-to-Person (A2P) SMS termination is a huge growth area fueled by automated notification systems such as those within the banking, airline, and consumer retail markets.

The Fraudster's Strategy: Deceive, Divide & Conquer

The battle to stop SIM Box bypass fraud has evolved into full scale electronic warfare as fraudsters constantly evolve their bypass techniques to avoid detection.

The fraudster's strategy is nationally focused: fraudsters purchase SIM cards from every mobile operator in a country, then, using antennas and SIM Boxes

located in highly populated regions, launch their bypass fraud across multiple networks.

a. Deception: Flying under the Radar of Detection

Managing and controlling SIM Box bypass requires great FM sophistication. Control techniques -- such as test call generation and usage pattern analysis -- that worked well only a few years ago have been largely neutralized by the fraudsters.

Perhaps the most powerful deception tool in use by fraudsters today is the SIM Server, which enables fraudsters to control bypass operations from a central location. A SIM server -- in a country like Monaco, Jamaica, or anywhere else – can control device Gateways in the infected country.

With SIM Servers, SIM cards no longer need to be physically in the local infected network, only the antennas that dump the fraudulent traffic onto the local mobile network.

Most importantly, the SIM Server allows the fraudster to "fly below the radar" of detection by lowering the usage of each SIM card to an absolute minimum. Large storage banks of SIM cards allow the fraudster to rapidly and automatically rotate a SIM card's usage so it doesn't alert FM systems.

In addition to their smart use of SIM Servers, fraudsters have also learned how to better foil the test calls operators and governments use to discover which SIM card IDs are actually being used for fraud traffic.

b. Divide & Conquer: How Fraudsters Play Operators Against Each Other

Fraudsters use a national strategy that cuts across all the operators in a country. Their strategy is very simple: choose the routes of least resistance.

Let's say there are three mobile operators in a country. Big Mobile and Medium Mobile are the largest mobile operators in the country and they each have very good SIM Box defenses in place. However the third and smallest operator, Small Mobile, has minimal FM detection capability.

Well, in that case, fraudsters can push more traffic onto Small Mobile's SIM cards. Yet notice what happens: even though Big Mobile and Medium Mobile do a good job of bypass blocking on their own networks, the amount of bypass on a national level remains the same because fraudsters diverted traffic to Small Mobile's SIM cards. Bottom line: the nation loses the same amount of tax revenue and the harm to the national infrastructure still occurs.

The other issue is that Small Mobile stands to gain financially from the fraudster's bypass activity. Normally, Small Mobile would receive a small share of domestic voice traffic, but if fraudsters are redirecting traffic through its SIM cards, it's making money and there may be no incentive for it to block SIM Box bypass traffic at all.

Why Regulators Should Lead the Fight to Stop Bypass in a Nation

When you understand how fraudsters are experts at flying under the detection radar and at shifting their traffic to operators with weakest fraud controls, I think the rational choice is for regulators to step up and coordinate the SIM Box bypass problem directly.

Let's face it: the regulator in each country is best positioned to facilitate collaboration of the fraud management activities across operators, direct a national strategy, and audit the operators to ensure their programs are effective.

Now it's true that taking the lead in fraud control operations is a new role for many regulators. SIM Box fraud management is usually considered the responsibility of the mobile operators themselves since it requires deep technical and network expertise.

However, mobile operator themselves generally do not have deep enough expertise in SIM Box FM, so they frequently hire FM vendors to do this work on a contract or managed service basis anyway.

Regulators, likewise, can also engage these SIM Box FM vendors to implement and manage the technical details of their bypass blocking strategy.

Six Steps Regulators Should Take to Control SIM Box Fraud

So if regulators should facilitate and coordinate SIM Box FM at a national level, what specifically should they do? Well, here are six key strategies to consider.

1. Write Laws that Make Bypass Fraud a Costly Crime to Commit -- In many nations, there are no laws that specifically prohibit SIM Box bypass. In other nations, the penalties for committing the fraud and breaking the laws are too light. For example, in one country, SIM Box operators are fined $10,000 for a violation. However, they can easily earn that amount back within a few days of operating SIM Boxes. Such light penalties do not deter fraudsters from continuing their operations.

2. Gain National Visibility over SIM Box Fraud Activity – Advanced data analytics systems are available that can detect every SIM Box as it's activated on a particular network, though such systems may not be installed on all networks. Another technique is to run test call campaigns that analyze how international calls are being routed through the fraudsters.

The beauty of monitoring across telecom operators is that a regulator gains a macro level understanding of the SIM Box fraud occurring across the country. Once the activity of fraudsters is understood, the regulator can then develop a strategy to prioritize the defensive measures, zero in on hot spots, and conduct "drive-by" antenna location in specific neighborhoods to determine the precise location of antennas, bust operations, and make arrests.

3. Coordinate the Use of Vendor SIM Box FM Systems & Services – Here's one of the ironies battling SIM Box fraud: while the fraudsters play divide-and-conquer against the operators, the operators themselves often fail to share FM intelligence, systems, and services with each other.

It's a great reason why regulators should take the lead in coordinating national and mobile operator efforts. For example, FM vendors sell test call services individually to mobile operators today. However, if test call services were a shared resource, detecting fraudulent interconnect routes would be more easily achieved for the benefit of all operators in a country.

The same goes for the advanced detection of illegal SIM Boxes using sophisticated data analytics systems. Advanced systems such as Protocol Signaling based analytic nodes are relatively expensive to deploy, yet probe systems dedicated to one operator's network at a time are less effective because the fraudster simply redirects its traffic to mobile networks not protected by the advanced systems. So sharing and coordinating the deployment of analytic resources across networks will surely pay dividends.

In summary, regulators should encourage shared FM resources whenever possible.

4. Audit the FM Performance of Mobile Operators – Regulators must walk a fine line between managing SIM Box FM at a national level, and interfering with a mobile operator's own business operations.

Yet tension between regulator and the operator is natural when operators have not succeeded in controlling SIM Box fraud themselves. After all, a regulator must step in to protect its own tax revenue and maintain a healthy and high quality communications infrastructure.

Certainly, advanced systems that discover illegal SIM Boxes on the network are an excellent tool for running performance audits on mobile operators. Regulators should also run their own test call campaigns to validate how well the operators in their market are applying control systems. What's more, regulators can also collect and analyze Call Detail Records (CDR) supplied by the mobile operators to gain even deeper knowledge of the fraud patterns while appropriately guarding the privacy and trade secret nature of the CDR data owned by each operator.

5. Reward & Penalize Operators to Ensure Policy Compliance – SIM Box fraud cannot be stopped if one or two operators in a country are cheating by encouraging or turning a blind eye to fraudsters terminating bypass traffic through their SIM cards.

By ensuring that each and every mobile operator maintains a high standard of SIM Box FM, national tax revenues are bound to increase since fraudsters can no longer play one operator against another. Not only that, operators can

safely invest in growth knowing that licensed operators are competing on a level playing field. Tighter control over SIM card sales, rewards for compliance, and penalties for poor FM performance are potent tools a regulator has at its disposal.

6. Bust Up SIM Box Operations & Make Arrests – The enforcement side of SIM Box defense is crucial because it frustrates and scares the fraudsters. When enforcement is weak or non-existent, fraudsters are emboldened to invest more in a country because their risks are much lower.

The regulator should coordinate the neighborhood deployment of specialized RF measurement equipment that pinpoints the actual location of the SIM Boxes and antennas. The police can then quickly go in to confiscate equipment and make arrests in one fell swoop.

Jordan: A Successful Case in Regulator-Driven Fraud Management

As fraudsters continue to steal money and wreck infrastructure damage on countries around the world, regulators in many countries have begun to take a more active role in managing the national voice bypass fraud problem.

Jordan's Telecommunications Regulatory Commission (TRC) conducted a full-scale government-led program that has significantly reduced the amount of SIM Box fraud in the country.

Dr. Ghazi AL-Jobor, Chairman of the Board of Commissioners at TRC, said,

"As a regional leader, we have achieved tremendous success in Jordan by taking a centralized approach in eliminating bypass fraud. TRC has used its resources as a regulator to manage a well-orchestrated effort between operators, law enforcement, and LATRO to locate and eliminate illegal bypass fraud. Bypass fraud violates the Telecommunications Law in establishing, operating, or managing a Public Telecommunications Network for the purpose of providing Public Telecommunications Services without having the required licenses from TRC and connecting his network with another Telecommunications network without having the right to do so in order to terminate international call to the national telecom operators in Jordan illegally. TRC's actions have helped restore revenue to the operators, increase tariff receipts for the government, preserve the Privacy and Quality of Service for the citizens of Jordan, and protect the National Security."

In TRC's successful SIM Box mitigation program, critical data was combined from the Jordanian operators' fraud management systems in addition to TRC's own test and analysis, allowing TRC to successfully locate and arrest SIM Box operations and prevent further financial loss to the operators and the national government. More than 20 fraud operations representing more than 240 million annual minutes of bypass termination capacity were prosecuted to date.

Details on the program follow:

- Laws: Strong Anti-SIM Box Laws were Enacted – The Jordanian government implemented stiff financial and criminal penalties around the operation of unlicensed telecom services in the country.

- Monitoring: Test Call Services Monitor Each Operator in the Country. TRC ran test call and audited the mobile networks to discover which networks were most infected.

- Visibility: The Fraudsters' SIM Box Activity & Strategies were Exposed — Running all the detection data through a central analysis platform, TRC gained a comprehensive view of fraud activities across the country of Jordan.

- Detection: SIM Box Equipment Locations were Precisely Pinpointed — Using network data on SIM Box activity as a starting point, the project team used LATRO's Versaradio™ Radio Frequency (RF) investigation tool to identify the exact location of the actual SIM Boxes.

- Enforcement: SIM Box Operations were Busted — TRC then mobilized its law enforcement resources to take action. In just a few months, authorities seized and confiscated SIM Box equipment with more than 500 gateway modems representing greater than 20M potential minutes of fraudulently terminated calls per month. This produced an estimated revenue savings of $2M for the Jordanian government.

Conclusion

International bypass fraud is a major unsolved problem that costs nations major tax losses and communications infrastructure damage each year.

For years, regulators have waited in the wings hoping mobile operators would solve the problem on their own. But operators have not succeeded, in part, because fraudsters have become more sophisticated and skilled at pitting the licensed operators of a country against each other.

It's now crucial for regulators to step up and assume a far more direct role in managing SIM Box FM at a national level. The case study from the Middle East shows that regulators can succeed with national management programs that combine six key strategies:

1) Write laws that make bypass fraud a costly crime;

2) Gain national visibility over SIM Box fraud;

3) Coordinate the use of vendor FM solutions;

4) Audit FM performance of mobile operators;

5) Reward & penalize operators to ensure policy compliance; and,

6) Bust up fraud operations & make arrests.

About Technology Research Institute

Since 1994, Technology Research Institute (TRI) has been writing and researching telecom software and systems markets. In 2015, TRI published Telecom Fraud Management Services, Software & Strategies, a 239-page market research report that analyses the struggles, challenges, successes, and failures of those fighting fraud in the telecom industry. Authored by Dan Baker, TRI's research director, the report draws on conversations with three dozen telecom fraud experts with major contributions by five top consultants in the field. 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.

About LATRO Services

LATRO conducts fraud control, revenue assurance, and technical services around the globe. The company's managed services have benefited mobile network operators and communications service providers in all major global regions. The LATRO team of dedicated experts and innovative software and hardware solutions enable network operators to identify and eradicate international bypass fraud in addition to other frauds on their networks.