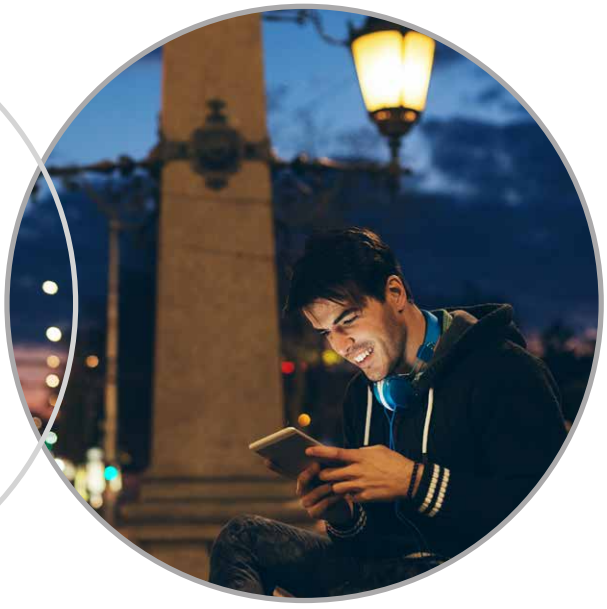
winning against the telecom fraudsters

the cost of interconnect bypass fraud

The telecom industry loses about $6 billion annually due to interconnect bypass fraud, or SIM box fraud, according to the Communications Fraud Control Association (CFCA)[1]. Despite having deployed sophisticated fraud management systems, SIM box fraud continues to cost an average service provider more than $2 million per year based on a survey by ROCCO[2].

Fraudsters avoid call charges by bypassing the legal interconnection routes and terminating their traffic directly to the mobile networks, using SIM boxes and low-quality Internet connections.

Not only are the financial losses significant but there is also an immeasurable impact on subscriber satisfaction that cannot be underestimated, including degraded voice quality, incorrect caller ID and increased SMS spam.



the need for a new comprehensive approach

iconectiv is an industry expert in telecom registries and solutions that minimize interconnection-related revenue leakage. As a frequent contributor to the GSM Association (GSMA) and CFCA fraud prevention activities, we believe that only a comprehensive approach based on the following key components can deliver long-term success in the fight against interconnection-related fraud:

- Minimizing the overall fraud opportunity
- Enforcing fair-use policies
- Enabling massive network information gathering, processing and sharing

The above approach targets the root causes of the fraud and its underlying mechanisms along with detection and enforcement.

a framework for controlling bypass fraud

minimizing the overall fraud opportunity

The first pillar of a comprehensive strategy to reduce fraud in your network is to introduce measures that make it less profitable and less attractive for the fraudsters in the first place.

the driver of bypass fraud

Bypass fraud is driven by the opportunity for arbitrage where fraudsters exploit the cost difference between terminating relatively expensive off-net calls (where interconnection rates apply) and the less expensive on-net calls (where interconnection rates do not apply).

In illegally bypassing the established interconnection routes, fraudsters can offer very competitive rates for international calls and SMS termination. They send international traffic over cheap Internet connections and use SIM box equipment to make it look like it is local, on-net traffic. In this way, the fraudsters can generate revenues from international traffic, take advantage of the very low on-net termination rates and pocket the difference. Besides causing significant economic loss, SIM boxes degrade voice quality and may cause cell overload, resulting in customer dissatisfaction.

increasing the cost and effort of committing fraud

The key in deterring the fraud is to raise the costs for the fraudsters to do their business, and make their criminal activities less profitable.

The fraudsters' expenses include the cost and effort of replacing blocked SIM cards, purchasing more advanced SIM box equipment, constantly modifying algorithms to evade detection, and spending additional airtime to camouflage fraudulent calls so that they appear to be dialed by ordinary subscribers.

For example, tightening the thresholds on allowable call patterns, such as ratios of incoming to outgoing calls and on-network to off-network calls, especially during an initial vetting period, will raise the costs for the fraudsters and delay their fraudulent revenues until after the vetting period. Also, imposing requirements on a minimum SIM card balance and a higher minimum refill amount, which get forfeited if the SIM card is blocked due to abuse, further increases the expenses for the fraudsters.

A fraudster might invest thousands of dollars in obtaining new SIM cards and use them for several weeks to generate inconspicuous traffic during an assumed vetting period (which cannot be fully known by the fraudster), only to realize that the SIM cards have suddenly been blocked and their entire balances forfeited just when the fraudulent operations started after the vetting period.

As their illegal activities gradually become more time-consuming, frustrating, and less profitable, the fraudsters may eventually realize that the time, cost and risk is not worth the return.

enforcing fair-use policies

The second pillar in deterring fraud is centered on preventing the abuse of unlimited or high-volume plans that bundle voice and SMS. These service plans are very attractive to the fraudsters since they offer very low on-net termination fees and allow them to profit from their illegal traffic schemes.

Consequently, limiting the abuse and fraudulent use of high-volume plans by automatically monitoring them against the fair use policy of the service provider becomes critical in fighting the fraud.

The fair-use policy monitoring needs to be done in real-time or in near real-time and be based on configurable thresholds, as any delay in detecting breaches can be exploited by the fraudster.

winning against the telecom fraudsters

policy-based action and enforcement

Focusing on monitoring and detection of fraud alone is not enough. Once a breach is detected, a wide range of automatic and policy-based responses should be possible. These include notifying the internal fraud prevention team, sending an SMS to the subscriber that the fair use policy has been violated, automatically returning to standard billing rates for voice and SMS, and eventually blocking the non-complying SIM card. Another option is to send an SMS notifying the subscriber that the number has been temporarily suspended due to possible fraudulent activity, and directing the person to contact customer care.

Enforcing proper use of unlimited and high-volume plans, including Mobile Virtual Network Operator (MVNO) plans, complicates the abuse and makes the SIM box fraud less profitable. This, again, discourages the fraudsters.

Monitoring traffic, detecting fraudulent activity in real-time and executing automatic and policy-based responses require close integration with a wide range of internal systems including Operations and Business Support Systems (OSS and BSS).

SMSC
SMS: "You have exceeded the fair-use policy, service is blocked"

BSS
Block or change service plan: Prevent SIM from abusing high-volume plan

E-mail
Fraud Manager notification: MSISDN over threshold

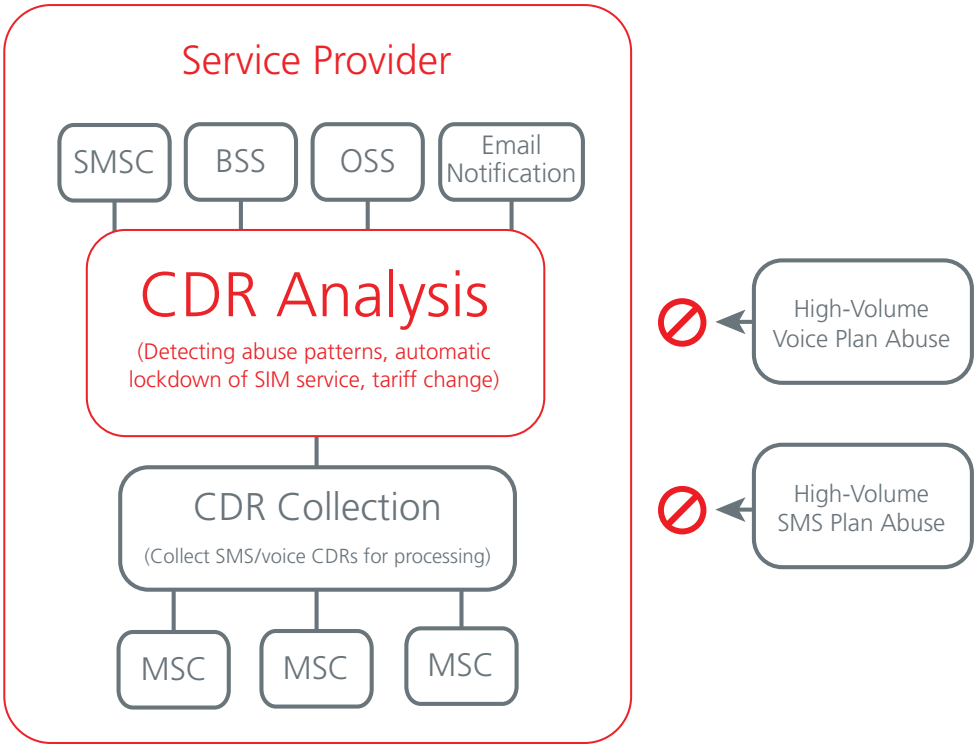


Figure 1: Comprehensive interconnect fraud detection and blocking offered as a managed service with close integration to internal systems including SMS Center (SMSC), OSS and BSS

massive network information gathering, processing, and sharing

The third pillar of a comprehensive approach to address the complex problem of interconnect bypass fraud and interconnection-related fraud in general is the ability to gather and leverage network information from many sources. This involves analyzing traffic patterns, dialed numbers, device identities, such as International Mobile Equipment Identity (IMEI) and subscriber behavior. It also involves establishing risk profiles including white lists and grey lists of suspect users.

the need for close OSS and BSS integration

The above tasks require close integration with a service provider's internal systems including OSS and BSS, as well as advanced reporting capabilities. Integration with national device and SIM registries and sharing of information with other service providers can also help identify illegal SIM box equipment based on IMEI values and detect duplicate IMEIs caused by SIM box spoofing.

In addition, access to detailed global number range information enables the service provider to proactively prevent other types of interconnection-related fraud, such as International Revenue Share Fraud (IRSF) and fraudulent use of corporate phone systems (also known as PBX hacking). This is possible by first identifying and then blocking fraudulent calls to high-risk numbers in real-time.

simplifying operations with a managed service

A managed service approach is an attractive model, due to the highly complex operations, the vast amount of information that needs to be analyzed including billions of Charging Detail Records (CDRs) and the need for constant updates of algorithms, threshold values and policy rules for detecting and blocking the fraud.

This approach enables the service provider to successfully fight interconnect fraud and minimize service abuse without having to allocate valuable resources on implementation details and day-to-day operations.

lets talk about your fraud prevention needs

As a frequent contributor to the GSMA Fraud and Security Group, GSMA Wholesale Agreements and Solutions Group, and the CFCA, iconectiv is committed to fighting telecom fraud. iconectiv does this by leveraging its vast experience in interconnection solutions, revenue-leakage prevention and OSS/BSS integration in multi-vendor networks.

Please contact us to learn more about how you can become more proactive in fighting interconnect bypass fraud, IRSF and PBX hacking fraud and win the battle against the fraudsters.

FOOTNOTES

[1] 2015 Global Fraud Loss Survey, CFCA

[2] SIM Box Losses Survey 2015, The Roaming Consulting Company (ROCCO)

about iconectiv

At iconectiv, we envision a world without boundaries, where the ability to access and exchange information is simple, secure and seamless. Our network and operations management, numbering, registry, fraud and revenue assurance, and messaging solutions enable the interconnection of networks, devices and applications for more than 1,000 customers globally and one billion people every day.

make the connection.

For more information about iconectiv, contact your local account executive, or you can reach us at:

+1 732.699.6800
info@iconectiv.com
www.iconectiv.com

iCOL-WP-AP-E-LT-001, September 2016