csg

TOGETHER, YOU WIN.

CSG ILLEGAL BYPASS DETECTION WITH AUTO BLOCKING

IDENTIFY AND ERADICATE FRAUD

Fraud presents a huge problem for mobile network operators (MNOs) around the world, costing over US$38 billion annually. But of all the different interconnect fraud issues, illegal bypass termination is by far the largest. In many countries, the international termination rate (ITR) is considerably higher than the local (retail) termination rate to a mobile number in the country. This makes it profitable for fraudsters to bypass the licensed international operator when terminating calls in the country. They pay the lower local rate instead of the ITR. This practice is illegal in most countries, and a huge problem for many operators due to lost revenues.

HOW ILLEGAL BYPASS FRAUD WORKS

The simplest way of committing illegal bypass fraud involves setting up a SIM box (GSM gateway); standard equipment can be easily acquired over the internet and equipped with a rack of SIM cards. The calls are typically routed via an internet connection to the SIM box residing in the terminating country. The SIM box then converts the call into a local mobile call to the receiving party on the mobile network.

Another variant of illegal bypass is when fixed line equipment—a "leaky PBX"—is used to convert the call to a local call. This is less common than SIM boxes but also poses a significant problem for operators.

THE EXTENT OF SIM BOX FRAUD

Fraudulent "SIM box termination" of international incoming calls, also referred to as "carrier bypass fraud," is a major challenge for MNOs and licensed international gateway operators (IGW). It results in poor customer experience and consequent churn, as well as lost revenue.

In some countries, as much as 70 percent of all incoming international calls are terminated fraudulently. The Communications Fraud Control Association (CFCA) estimates that US$6 billion are lost yearly due to interconnect bypass fraud alone. This not only impacts operators, but also the tax authorities of the affected countries, as taxes due on international traffic cannot be collected.

THE CONSEQUENCES OF ILLEGAL BYPASS FRAUD

Beyond direct revenue loss, other consequences of illegal bypass fraud include:

- Missing or incorrect Calling Line Identifier (CLI), which means that many calls are declined by the called party (B subscriber) and missed calls are not returned. This results in further revenue loss for the licensed operator

- Degraded voice quality due to latency issues, highly-compressed IP connections, and longer call set up time. This impacts the customer experience and the reputations of both carriers. Customer experience has a direct impact on loyalty, lifetime value and revenue

CSG ILLEGAL BYPASS DETECTION WITH AUTO BLOCKING

CSG Illegal Bypass Detection with Auto Blocking is a test call-based that can pinpoint a SIM box number in a single call. With this active testing on-net and off-net SIM box numbers are identified. However, the MNOs only deal with blocking on-net SIM box numbers. This solution also tackles the challenge of blocking off-net SIM box numbers.

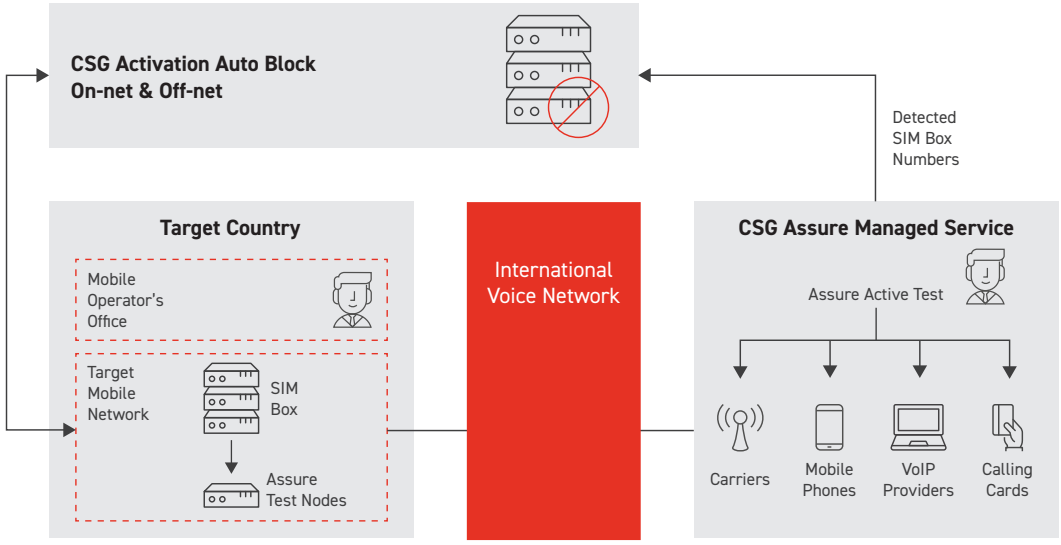
This test call-based approach has the distinct advantage of speed, which is critical as rapid removal of illegal bypass from the network will eliminate the profit for the SIM box operator. By continuously and quickly blocking the on-net and off-net fraudulent SIM boxes, the fraudulent SIM box operator will lose money and discontinue operations.

CSG Illegal Bypass Detection with Auto Blocking allows operators to proactively identify and eradicate illegal SIM box numbers and shut it down. The solution generates end-to-end controlled test calls from abroad into the target mobile networks where test nodes are placed. The CLI is inspected; a local CLI normally indicates a SIM box number and can be acted upon accordingly.

CSG provides its Illegal Bypass Detection with Auto Blocking solution as a managed service, allowing fast setup and minimal involvement from the operator to ensure a fast return on investment. The flexible alerting and reporting features of CSG Illegal Bypass Detection with Auto Blocking enable the delivery of instant SIM box alerts, as well as aggregated and detailed test reports for the customer. The network-facing aspects of the solution can be provided as SaaS or on-premise.

CSG Illegal Bypass Detection with Auto Blocking helps operators with:

- **Multiple call origination/route alternatives:** Since only some of the traffic coming into the country will be subject to illegal bypass, it is important to be able to simulate a large variety of traffic streams into the target network
- **Intelligent call generation:** Since every test call is associated with cost/network resource consumption, it is important to achieve a high ratio of found SIM box numbers per test call
- **Avoiding detection:** If the SIM box operator finds out that test calls are being made and their SIMs blocked, they can try to destroy the testing (e.g. block test calls)
- **Powerful alerts and reporting:** Since speed is important, the responsible person/system at the customer level should be instantly alerted when a SIM box number is found. Monitoring the progress of successful SIM box elimination over time requires good reporting
- **Calling line identification:** The SIM box operator might try to hide the CLI when terminating the calls, making it impossible to identify the SIM to be blocked. Specially configured SIM cards with CLIR override (CLIRO) can help eliminate this problem
- **Blocking of on-net and off-net SIM box numbers:** Integral to the solution is the integrated fraud detection and SIM box number blocking. The automated, end-to-end process creates operational efficiencies, as well reducing revenue leakage and significantly improving the MNO's EBITDA



One of the key attributes of a successful illegal bypass detection solution is the ability to generate calls from a large number of sources. Only a certain percentage of the traffic into the country will be subject to illegal bypass, making it important to simulate a variety of traffic streams into the target network.

The CSG Illegal Bypass Detection with Auto Blocking solution offers over 1,000 alternatives to originate the calls, including:

- Via international carrier routes
- Via VoIP (OTT) providers
- From international mobile subscriptions
- From calling cards

A GLOBAL PRESENCE

CSG is currently working with operators in Asia, Africa, Eastern Europe, Latin America and the Caribbean to eradicate illegal bypass fraud. In each case, we collaborate with the respective fraud departments to establish the best procedures for reporting any SIM box numbers.

ABOUT CSG

CSG simplifies the complexity of business transformation in the digital age for the most respected communications, media and entertainment service providers worldwide. With over 35 years of experience, CSG delivers revenue management, customer experience and digital monetization solutions for every stage of the customer lifecycle. The company is the trusted partner driving digital transformation for leading global brands, including Arrow, AT&T, Bharti Airtel, Charter Communications, Comcast, DISH, Eastlink, iFlix, MTN, TalkTalk, Telefonica, Telstra and Verizon.

At CSG, we have one vision: flexible, seamless, limitless communications, information and content services for everyone. For more information, visit our website at csgi.com and follow us on LinkedIn, Twitter and Facebook.