csg

TOGETHER, YOU WIN.

CSG ILLEGAL BYPASS FRAUD PROTECTION

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

- **Direct revenue loss**
  - In many cases, operators lose hundreds of thousands of dollars per month
- **Indirect revenue loss**
  - 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 operators

- 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 FRAUD PROTECTION

CSG provides hundreds of operators from around the world with OSS and BSS solutions, designed with unique insight to create a comprehensive and fully integrated CSG Illegal Bypass Fraud Protection solution.

The solution allows in the first instance to pinpoint a SIM box number in a single call. This test call-based approach has the distinct advantage of speed, which is critical to identify fraudulent activity in the network. As soon as SIM box numbers are identified the CSG Illegal Bypass Fraud Protection solution allows for auto-blocking of the discovered on-net numbers and for blocking of off-net calls from identified SIM box numbers.

End-to-end integration is key part of the solution design to allow the auto blocking functionality to outpace the speed the fraudulently used SIM cards are replaced with. CSG believe that a manual approach to SIM card blocking is not relevant and won't be effective enough against highly sophisticated fraudulent operations.

High-level features of the solution include:

- World-class service for detecting active SIM boxes
- Call flow control at software level as opposed to probe-based solutions that are vulnerable to internal fraud and entail significant hardware maintenance
- Near real-time blocking of detected on-net SIM box numbers
- Near real-time blocking of calls from detected off-net numbers
- Ability to manually block numbers at granular level (per IP address, port, SIP/TDM etc.)
- Ability to manually unblock numbers
- Reporting-enabled solution
- Project designed to deliver value as soon as possible