SANDVINE

# Interconnect Bypass Fraud

## Protect revenue against fraudulent voice services

## INTERCONNECT BYPASS FRAUD DELIVERS:

### OTT Bypass and SIMbox Fraud

Detects and mitigates two most prevalent bypass frauds in the telecom industry

### Advanced Fraud Detection

Detects and prevents attempted fraud with Sandvine's extensive library of standard and custom-built application signatures and closed-loop correlation and analysis of subscribers, connections, and traffic patterns focused on fraud detection

### Preservation of Legitimate Voice Revenue

Ensures operators receive revenue for the voice services provided to users including roaming services

### Active Testing and Short SLAs

Resolves issues swiftly with a team of experts dedicated to new fraud techniques and anomaly detection as well as policy enforcement

### MARKET OVERVIEW

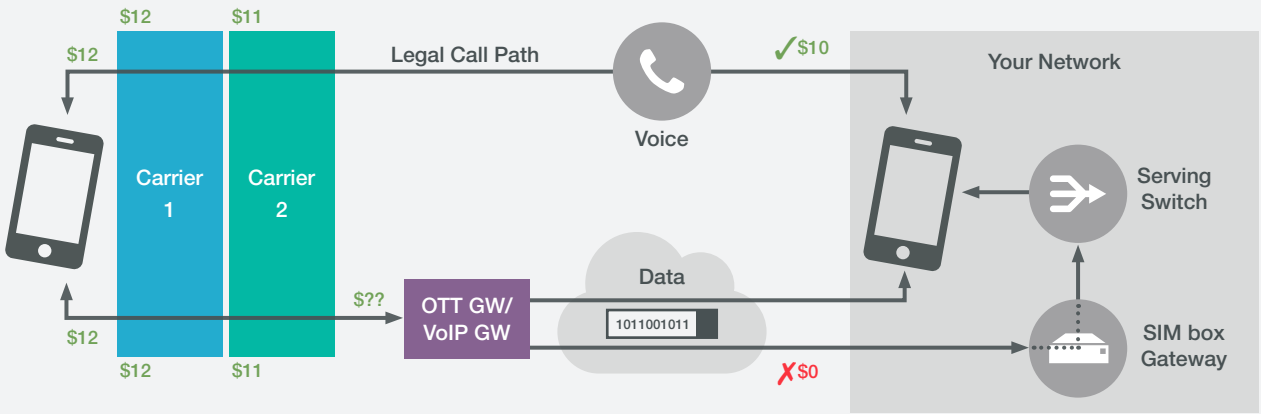
**Before the explosion of mobile data traffic and OTT applications, voice and SMS were the majority of operator revenue. Today, users rely heavily on OTT VoIP and instant messaging applications to communicate, which has reduced the service-related revenue for operators year-over-year. This increasing demand for alternative communication services also attracts fraudulent actors on the voice market – using evolving techniques to bypass regular Public Switch Telephone Network (PSTN) voice routing and OTT VoIP applications.**

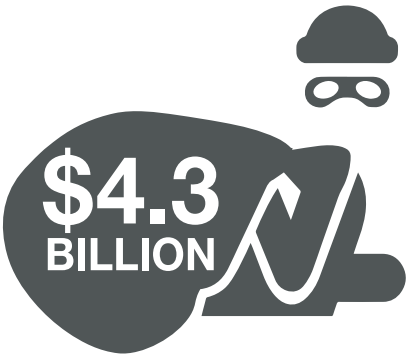
This new age of voice applications attracts fraudsters, resulting in a high rate of interconnect bypass fraud. Fraudsters "hijack the signal" between the end network, as the majority of the fixed interconnection fee goes to the operator that terminates the call, and unfairly profit from the legitimate means of routing the call. This is particularly worrying for the operator as both callers are unaware that their calls are not being completed through the PSTN and any poor experiences are attributed to the carrier.

(See **Figure 1**) For example, a call originating in the United States but destined for Brazil could travel through networks in Mexico and Colombia before reaching the end user. In this instance, a portion of the per minute fee paid by the user would go to each of the networks the call passed through – in the case of interconnect bypass fraud the revenue is received by the fraudsters instead of the operator in Brazil.

**Figure 1**

**Operators have their calls hijacked and revenues threatened by voice bypass fraud, with both callers being unaware that their calls are being hijacked**






**Interconnect bypass fraud is one of the largest sources of lost revenue and costs network operators across the globe an estimated $4.3 billion (USD) annually.**
**Source: 2017 CFCA Global Fraud Loss Survey**

Historically, interconnect bypass fraud was attributed to "SIMbox fraud," which involved installing a piece of hardware – SIM box – within PSTN to bypass traditional voice call routing by terminating the interconnect calls. A SIM box contains many locally purchased SIM cards from multiple operators, allowing fraudulent actors to intercept calls and collect the majority of the interconnect fees as their SIM box makes these calls over a lower-quality mobile connection.

With the explosion of mobile VoIP applications available, the legacy interconnect telecom frauds have evolved and advanced to cover OTT applications as well. In the scenarios of OTT bypass fraud, a normal phone call is diverted over IP to a mobile VoIP application on a smartphone, instead of being terminated over the normal telecom infrastructure. Many VoIP applications are polymorphic in nature and tend to be especially aggressive to adapt to bypass network control and policies. Therefore, operators need a solution to identify both types of interconnect bypass fraud as well as enforce suitable policies that minimize circumvention.

Unauthorized voice traffic poses a threat not only to operator revenue, but also for telecom regulatory agencies whose goal is to keep citizens and infrastructure safe. Bypassing techniques and unregulated VoIP applications are popular to use in illegal communication since the calls made cannot be intercepted or tracked by law enforcement agencies. Operators are therefore responsible for adhering to the regulations and minimizing the footprint of illegal voice traffic in their networks.

## SOLUTION OVERVIEW

**Interconnect Bypass Fraud leverages Sandvine's Active Network Intelligence (ANI) Classification Engine to correctly classify OTT VoIP traffic, even when it is encrypted, as well as identify users and devices involved in SIMbox fraud.**

The ANI Classification Engine uses machine learning capabilities, along with heuristics and an extensive, frequently updated signature library to deliver the most accurate classification of all traffic. Additionally, this solution differentiates authorized OTT VoIP traffic from fraudulent VoIP applications, whereas other solutions require manual mining from large amounts of metadata. Polymorphic applications can be correctly classified by the ANI Classification Engine by leveraging machine learning algorithms, and the bypassing of blocking policies can be minimized.

This solution is not limited to only identifying fraud on the network, it also offers operators a comprehensive way to mitigate voice-related fraud through appropriate actions. When fraud is detected, operators can enforce necessary policies for that specific traffic type. The most effective action is to block or reject the call, which will terminate it and the call will be rerouted through the carrier switched path – instantly recovering revenue for the operator.

For SIMbox fraud, operators can identify users and the devices involved with a closed-loop analysis of traffic patterns and behavior, detecting the fraudulent IP addresses and subnets. The identified servers and IPs can be monitored in isolation to prevent activity and detected VoIP gateways used in SIMbox fraud.

**With this understanding of varying call types and multiple fraud techniques, Sandvine uses Active Network Intelligence to minimize the impact of voice-related fraud with flexible policies to protect operator revenue and ensure compliance with telecom regulations.**

## ABOUT SANDVINE

Sandvine helps organizations run world-class networks with Active Network Intelligence, leveraging machine learning analytics and closed-loop automation to identify and adapt to network behavior in real-time. With Sandvine, organizations have the power of a highly automated platform from a single vendor that delivers a deep understanding of their network data to drive faster, better decisions. For more information, visit **sandvine.com** or follow Sandvine on Twitter at **@Sandvine.**

SANDVINE

**EUROPE**
Svärdfiskgatan 4
432 40 Varberg,
Halland
Sweden
T. +46 340.48 38 00

**CANADA**
408 Albert Street,
Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

**ASIA**
RMZ Ecoworld,
Building-1, Ground Floor,
East Wing Devarabeesanahalli,
Bellandur, Outer Ring Road,
Bangalore 560103, India
T. +91 80677.43333