SANDVINE

Interconnect Bypass Fraud Management

Protect revenue against fraudulent voice services

INTERCONNECT BYPASS FRAUD BENEFITS:

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 service providers 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 service provider revenue. Today, users rely heavily on OTT VoIP and instant messaging applications to communicate, which has reduced the service-related revenue for service providers 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 service provider that terminates the call, and unfairly profit from the legitimate means of routing the call. This is particularly worrying for the service provider 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 service provider in Brazil.

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 service providers, 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, service providers 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 service provider 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.

Interconnect Bypass Fraud Management

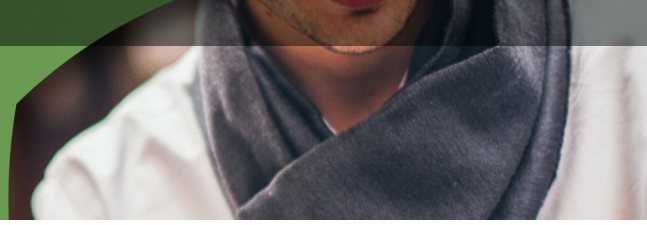
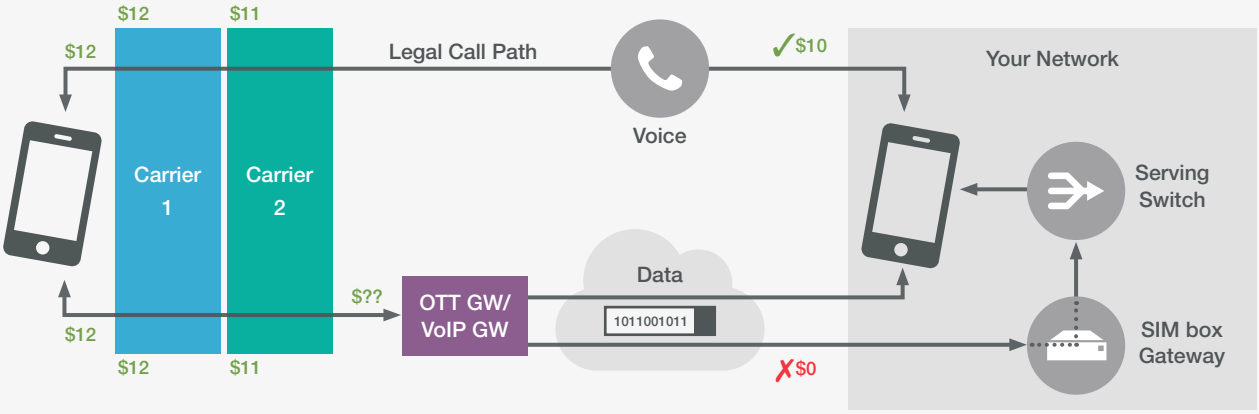
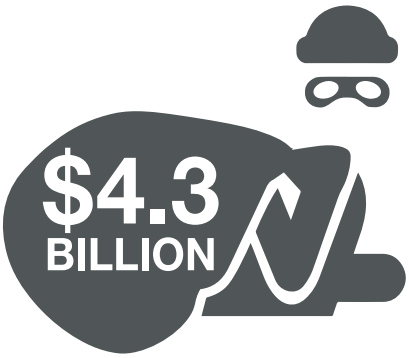


Figure 1

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



Service providers are therefore responsible for adhering to the regulations and minimizing the footprint of illegal voice traffic in their networks.



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

USE CASE 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.

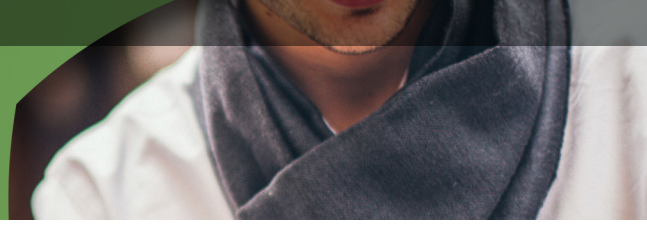
The ANI Classification Engine uses machine learning capabilities, along with heuristics and an extensive, frequently updated signature library to deliver the most accurate classification of all traffic. Additionally, this use case differentiates authorized OTT VoIP traffic from fraudulent VoIP applications, 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 use case is not limited to only identifying fraud on the network, it also offers service providers a comprehensive way to mitigate voice-related fraud through appropriate actions. When fraud is detected, service providers 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 service provider.

For SIMbox fraud, service providers 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 service provider revenue and ensure compliance with telecom regulations.

Interconnect Bypass Fraud Management



ABOUT SANDVINE

Sandvine's cloud-based Application and Network Intelligence portfolio helps customers deliver high quality, optimized experiences to consumers and enterprises. Customers use our solutions to analyze, optimize, and monetize application experiences using contextual machine learning-based insights and real-time actions. Market-leading classification of more than 95% of traffic across mobile and fixed networks by user, application, device, and location creates uniquely rich, real-time data that significantly enhances interactions between users and applications and drives revenues. For more information visit **http://www.sandvine.com** or follow Sandvine on Twitter **@Sandvine**.

SANDVINE

The App QoE Company

USA
5800 Granite Parkway
Suite 170
Plano, TX 75024
USA

EUROPE
Neptunigatan 1
211 20, Malmö
Skåne
Sweden
T. +46 340.48 38 00

CANADA
410 Albert Street,
Suite 201, Waterloo,
Ontario N2L 3V3,
Canada
T. +1 519.880.2600

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