

# Active Fraud Eliminator

THE CHALLENGE

## Minimize fraud from sources such as illegal SIM Boxes (GSM Gateways)

Fraud is a significant problem that costs carriers billions annually. Additionally, it consumes a substantial amount of signaling and voice bandwidth as well as the resources of the individual network elements (i.e. STPs, switches, databases) that have to process each fraudulent call.

Illegal SIM Boxes alone (also known as illegal GSM Gateways) impact carriers financially on the order of billions annually while accounting for as much as 20% of a provider's terminating traffic. In addition to illegal SIM Boxes, the table to the right highlights some of the other more pervasive types of fraud that are harming carriers today.

Particularly difficult to control is fraud that originates on another network and enters the destination carrier's network through its SS7 carrier-to-carrier interconnect links. A good example of this "off-net" fraud is inbound calls that have been generated by illegal SIM Boxes that reside on another carrier's network. Stopping off-net fraud is problematic because carriers typically do not have an active control mechanism in place that can readily stop or deter the fraud before it can establish a connection and consume network resources. As a result, carriers are often forced to rely on the originating carrier to intervene, an approach that provides no direct control and is often unreliable.

Type of Fraud	What Happens	Risk to the Operator
Illegal SIM Boxes	SIM Boxes (GSM Gateways) are used illegally to bypass standard network interconnections in order to make traffic appear as local mobile calls	Carriers lose the difference between the international/national termination rate and the mobile-rate, causes inefficient overuse of network resources
Roaming	Fraudulently obtained subscriptions are used in a roaming region, usually to perform "high value" activities such as the sale of outbound international minutes of use	One of most expensive types of fraud, irritates customers whose identity has been stolen and can cause billing nightmares
Premium Service (Phishing)	Subscribers are duped into placing calls to high-cost premium services	Customer irritation resulting in churn, increased customer care costs and operator refunds
Subscription	Customers sign up for service with no intent to pay, building large multi-month bills	Projected revenue will never be earned plus the cost of trying to collect on unpaid bills
SMS*	Unwanted and fraudulent (i.e. someone impersonating valid customers or SMSCs) messages are delivered to subscribers	Increased churn due to customer irritation, lost termination fees, increased operational costs, damages adoption of emerging advertising and m-commerce opportunities

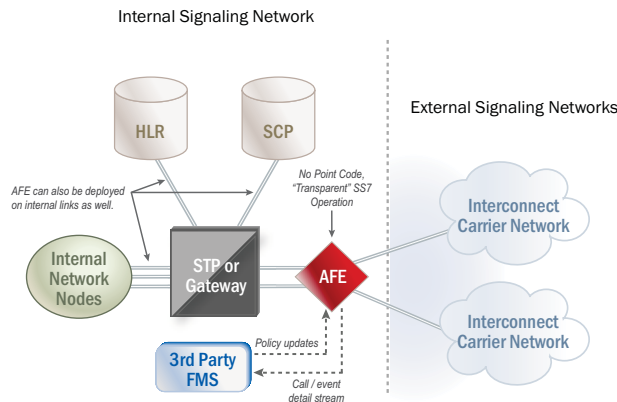
\* Due to the nature of SMS fraud, it is best controlled using Sevis' SMS Defense; however, both SMS Defense and Active Fraud Eliminator utilize Sevis' Signaling ASE® System, so they can be deployed using the same platform.

THE SOLUTION

## Enhance your ability to control fraud with Active Fraud Eliminator

Sevis' **Active Fraud Eliminator (AFE)** enhances a carrier's ability to control fraud through the use of Active Probe Technology. Active Probe Technology enables **AFE** to reside "transparently" (i.e. without a point code) on any SS7 signaling link and intercept fraudulent calls or messages in near-real-time based on a carrier's customized fraud control policies. Once intercepted, **AFE** can stop the message or perform advanced control functions to include message thresholding, re-routing, modification or response.

With **AFE**, a carrier can enhance their ability to control "off-net" fraud at their network perimeter (such as calls from illegal SIM Boxes that reside on another network) as well as "on-net" fraud that originates within their own network.



Active Fraud Eliminator Example Interconnect Deployment

### Active Fraud Eliminator's Key Capabilities

**Utilizes Active Probe Technology:** Can reside transparently, without a point code, on any signaling link and requires no SS7 network reconfiguration to install.

**Can Intercept "Off-Net" and "On-Net" Fraud:** Can be situated on a carrier's SS7 interconnect links or any internal signaling link to ensure that fraud originating on another network (like from an "off-net" illegal SIM Box) or within a carrier's own network is intercepted.

**Advanced Call Control:** Can stop messages (i.e. block "blacklisted" numbers) as well as perform message thresholding, re-routing, modification or response, enabling carriers to manage fraud in unique ways (for example, a carrier can degrade a fraudster's QoS to minimize damage until the culprit is apprehended by law enforcement).

**Decision Support Tools:** Provides visibility into potentially fraudulent message traffic to include calls generated by suspected "off-net" illegal SIM Boxes.

**Built-in Fraud Management System (FMS) API:** An existing FMS can send automated policy updates to AFE so that policy changes can be implemented in near-real-time. Additionally, AFE is capable of providing the FMS with a call/event detail stream if desired.

**Centralized Policy Management:** Carriers can centralize fraud control policy creation and management using the system's scaleable EMS which allows multiple platforms and physical sites to be managed with one user interface.



## The Architecture:

### One platform, no point code, many solutions

Each Sevis solution utilizes Sevis' patented **Signaling ASE<sup>®</sup> System**, a proven, carrier-grade system that enables both Sevis and partner-developed applications to be deployed without an SS7 point code, thus eliminating the need for operators to re-engineer their signaling network upon installation and allowing any ASE-enabled solution to operate independent of a carrier's existing vendor infrastructure.

The ASE System is comprised of the *ASE Platform* (the "transparent" SS7 network element) and the *ASE Manager*. The ASE System is the cornerstone of all of Sevis solutions, and once deployed it can be the foundation to help you address other needs in addition to enhancing your fraud control capabilities to include improving SS7 network security and risk mitigation (*Signaling Defense*), controlling SMS spam (*SMS Defense*) and resolving network interoperability issues (*Network Mediator*).



The ASE platform and ASE architecture

## Technical Specifications: Carrier-grade, high availability, flexible

### Protocols

#### ANSI

- T1.111 MTP
- T1.113 ISUP
- T1.112 SCCP
- T1.114 TCAP
- AIN 0.1/0.2
- IN
- ANSI-41 D
- WIN

#### ITU/ETSI/3GPP

- Q.701 – Q.705, Q.707 MTP
- Q.761 – Q.764 ISUP
- Q.711 – Q.714 SCCP
- Q.771 – Q.774 TCAP
- Q.721 – Q.724 TUP
- INAP CS-1/CS-2
- GSM MAP
- CAMEL

#### Sigtran

- M3UA
- M2PA

#### Application

- SMPP
- SS7oIP

### Platform Specifications

#### Chassis

- 2 U high, rack-mountable chassis
- 19" (482.6 mm ) or 23" (584.2 mm) rack mount
- Packet switching backplane
- 3 trunk interface module slots
- Up to 12 T1/E1s per platform
- Up to 48 transparent low speed SS7 links per chassis
- Up to 3 transparent ATM high speed links per chassis
- Chassis clustering
- Alarm status display module
- Telco alarm interface (dry/wet contact relay)

- 5 10/100 Base-T Ethernet ports
- Hardware/software status reporting

#### Power Supplies and Fans

- N+1 redundancy
- Hot swappable
- DC (-48V)
- A and B DC power feed

#### Trunk Interface Module

- Up to four T1/E1s
- Up to 16 transparent low speed SS7 links
- Up to 1 transparent ATM high speed link
- A, B, C, D, E, F links
- Channel associated signaling
- T1/E1, RJ-48C
- Hot swappable
- 3 10/100 Base-T Ethernet ports
- Drop and insert grooming
- Automatic link protection
- LED status indicators
- Rear transition module

#### Regulatory Compliance

- NEBS Level III certified
- ETSI 300 019 2-1 to 2-4
- CE
- FCC Part 15, Class A (CSA)

#### Temperature Range

- Operating: -5 °C to +55 °C (23 °F to 131 °F)
- Storage: -40 °C to +70 °C (-40 °F to +158 °F)

### Management Server

#### Architecture

- Centralized client/server
- Dual processor
- RAID 5
- Hot-plug hard drives
- Hot-plug redundant power supplies
- Java-based GUI client

#### Event Management

- Event filtering with audible event notification
- Hardware/software status reporting

#### Performance Management

- CPU and memory utilization monitoring
- Link status monitoring
- Detailed platform/server statistics

#### Security Management

- User-configurable multi-level security access
- User authentication and activity timeout
- Encrypted management interfaces

## The Company: Helping carriers protect their revenue, subscribers and network

Sevis Systems helps communications service providers protect their revenue, subscribers and network through innovative signaling solutions. Founded in 1999, Sevis is an employee owned and operated company that is headquartered in Plano, Texas. Sevis' solutions have been purchased by some of the largest service providers in the world and are resold by globally-recognized equipment suppliers including Alcatel-Lucent. To find out more about Sevis and our unique solutions, please call us at **877.517.3847** or visit our website at **www.sevis.com**. We look forward to working with you.