csg

TOGETHER, YOU WIN.

DETECTING AND STOPPING INTERNATIONAL TELECOM FRAUD

A WHITE PAPER

Phone fraud is a nuisance for millions of consumers, enterprises and service providers. The methods are plentiful—artificially generated traffic by hacking into corporate switches, missed call campaigns, false answers are examples of fraud that causes high costs for the victims.

But fraud costs communications service providers much more. According to the Global Telecom Fraud Survey by the Communications Fraud Control Association (CFCA), international telecom fraud cost communications service providers (CSPs) $28.3 billion in 2019, or 1.74 percent of their annual revenue.

CSPs have devised methods to combat fraud, but fraudsters are always coming up with new ways to turn a profit. For instance, CFCA reports that some newly emerging fraud methods are payment fraud and IP PBX fraud. Some of the top types of fraud are listed in the table below.

EXAMPLES OF TYPES OF INTERNATIONAL TELECOM FRAUD

TYPE OF FRAUD	DESCRIPTION
Illegal Bypass	→ Avoiding or reducing the termination cost through a SIM box, leaky PBX, OTT app or through A number manipulation (i.e. EU bypass)
International Revenue Share Fraud (IRSF)	→ Artificially inflated traffic to high-rate destinations/premium rate numbers by PBX hacking, stolen SIMs or other means
False Answer Supervision (FAS)	→ False answer (call hijacking, short-stopping), early answer (pre-charge) and late disconnect (post-charge) fraud
Wangiri (Japanese for “one ring and cut”)	→ Missed call campaign (callback scam) fraud: leave missed calls (premium rate number) on a huge number of phones

These types of fraud not only impact a CSP's bottom line—they also impact their relationships with their customers. Degraded voice quality and latency issues caused by fraudsters negatively impact the customer experience, which can eventually cause customers to lose faith in their CSP and even defect to another provider.

If CSPs don't have the right fraud management systems in place, they put their revenue and reputation at risk. Fortunately, 74 percent of service providers saying fraud is growing in importance in their organization. And as of now, they have two primary ways to combat it.

ACTIVE AND PASSIVE TESTING

CSPs have two options for fraud management systems: an active testing system or a live traffic analysis (passive testing) system. Each solution has its own unique strengths:

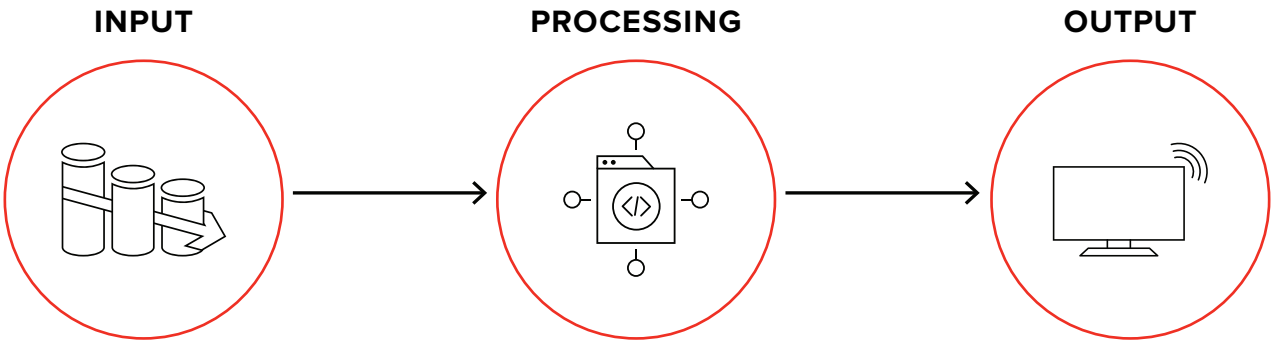
- **Active testing systems** are able to simulate a variety of traffic streams, and pinpoint fraud within a single test. Active testing also excels at detecting fraud applied on normal subscriber traffic, like FAS and illegal bypass fraud.
- **Live traffic analysis (passive testing)** collects live traffic CDRs, providing a true representation of the customer experience. Live traffic analysis excels at detecting artificially generated traffic, like IRSF and Wangiri fraud.

Most CSPs uses one of these approaches but not the other, missing out on the benefits each provide. By combining the two into one integrated system, active testing can make live traffic detection stronger and vice versa.

HOW THEY WORK TOGETHER

A fully integrated active and passive testing system allows for comprehensive and fast detection of fraud with higher certainty—and less impact on CSPs' bottom line. The combined system detects potential problems in live traffic, then triggers an active test to verify the problem. Active test results also help the live traffic analysis to detect more fraud.

ACTIVE TESTING ADVANTAGES	LIVE TRAFFIC ANALYSIS ADVANTAGES	COMBINED APPROACH ADDITIONAL ADVANTAGES
Accuracy—Pinpoint fraud within a single test	Scope—Covers all traffic in the mobile network	Accuracy—Use active test results to train the live traffic analysis; machine learning algorithms
Speed—Fraud conclusion and blocking can be done within minutes	Relevance—Assess the avoided loss based on real traffic flows	Speed—Increase the speed of life traffic analysis detections by using active test results
Not possible to fool by fraud equipment; human behavior call pattern	Not possible to fool by fraudster test; number whitelisting	Scope—Find more fraud by drawing conclusions from the combined data



A combined system can work along the following lines:

- **Input**
  - The system intakes live traffic measurements (voice, SMS, data, etc.) and active test measurements
  - These measurements are normalized and input into a fraud detection model
- **Processing**
  - The combined live traffic and active test results is profiled using advanced statistical methods and machine learning techniques
  - Additional active tests can be triggered to verify for example that the caller is a machine
  - All potential fraud events are given a fraud confidence level and events with a level above a threshold are concluded fraud cases
- **Output**
  - Fraud cases are reported, with visualizations and reports that let fraud teams drill down into and analyze the reported fraud cases
  - Other system actions are triggered, typically to automatically block the fraud

SUCCEEDING AT SCALE

Many CSPs can detect fraudulent traffic, but only after several hours or days. But by that time, it's too late to block—fraudsters like SIM box owners can start making a profit in 60 minutes from a SIM card is activated.

An integrated testing system needs scale and speed to detect traffic in near real-time and block it. Cloud SaaS deployments can lower operating costs and streamline operations by eliminating the setup and upgrades of server. SaaS is growing in popularity—over 20 percent of CSPs are already using a SaaS fraud management system.

The cloud scales to support unlimited traffic volumes and can provide very high data processing power. Data visualization helps fraud teams drill down into incident analytics and key KPIs, and communicate those results to management. Nearly 60 percent of CSPs say that integrating a business intelligence/data analytical tool is the best step they can take in the short term to improve fraud management performance.

FROM MANPOWER TO MANAGED SERVICES

Having the right system in place is just one piece of the fraud detection puzzle—CSPs also need staff to operate these systems. But the average fraud team is made up of only four to five people, leaving fraud departments stretched and vulnerable to attacks, especially during evenings and weekends.

Fraud departments need more manpower—or more specifically, managed services. According to TM Forum, managed services are becoming more popular in the fraud management space, with 60 percent of CSPs already having part of the process provided by a third party. Over 70 percent use managed services for detection and prevention, while 50 percent use managed services for prevention.

By buying fraud detection as a managed service, fraud detection logic is continuously updated by the anti-fraud service provider, ensuring detection methods are always up-to-date. Managed services also help mitigate internal fraud. By letting the anti-fraud service provider manage detection, the fraudsters have a more difficult time fooling the logic vs. an on-premise, CSP-operated system.

A combined active and passive testing system helps CSPs:

- Prevent revenue loss
- Decrease customer churn
- Increase revenue through improved partner relationships (fewer concerns about accidentally blocking legitimate traffic thanks to more accurate detection)
- Reduce cost for disputes
- Protect brand reputation
- Use less manpower with managed services

DETECT, THEN REACT

Just as active and passive testing work best together, so too do fraud detection systems with fraud elimination systems. Many operators are blocking fraudulent traffic manually, which is a time-consuming process that requires 24/7 maintenance.

Automation of the fraud detection and fraud elimination lets CSPs block fraudulent traffic in near real-time. Mediation systems connect the fraud detection system to the network to provision blocking requests for quick blocking, without any human intervention required.

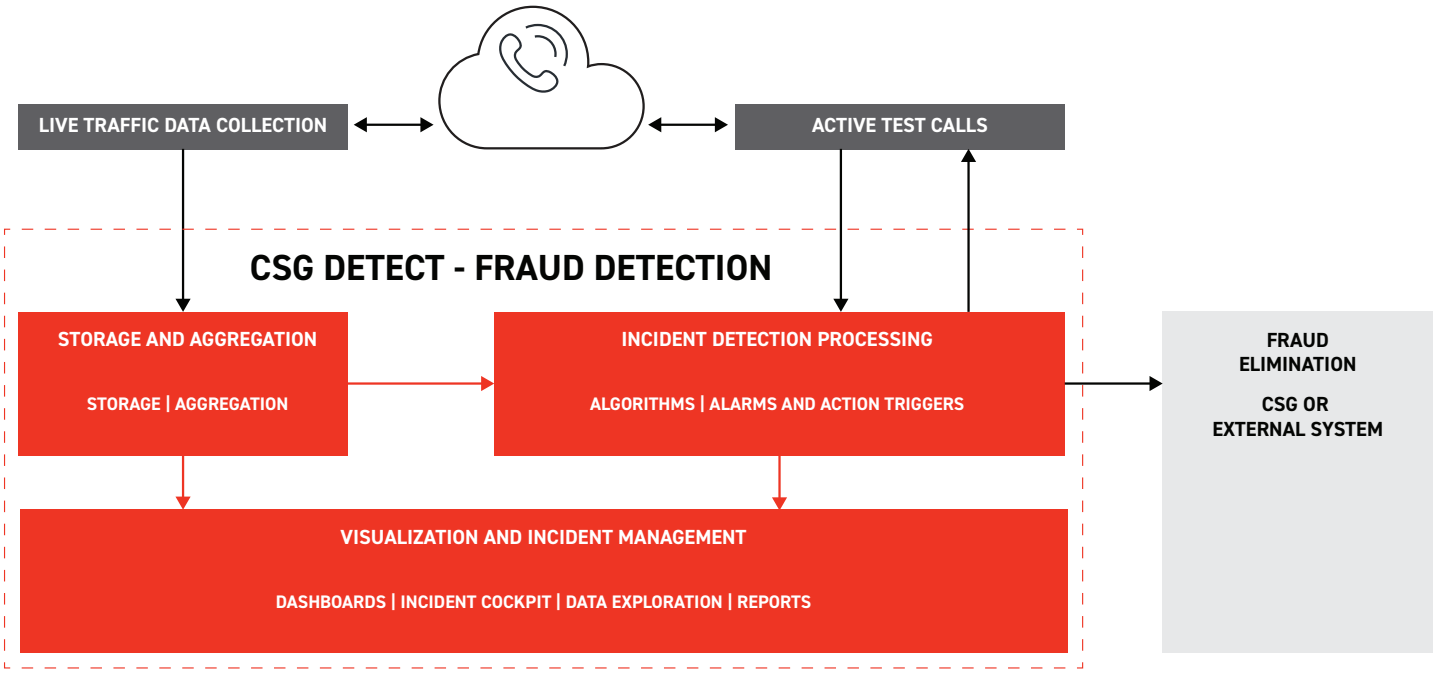
International telecom fraud costs CSPs billions every year, with a negative impact on millions of mobile customers. A robust fraud detection system, with the combined power of active and passive testing, provides CSPs with the tools they need to reduce revenue leakage and improve the customer experience.

THE CSG SOLUTION

CSG Comprehensive Fraud Detection solution, based on the CSG Detect combined live traffic analysis and active testing platform. is a high-speed event data processing, fraud incident detection and visualization solution. It can be configured for many different types of fraud detection.

Key characteristics include:

- Collection—Collect data from the customer network in near-real-time
- Detection—Understand the normal and detect anomalies in the live traffic and active test data by traffic profiling using advanced statistical methods and machine learning techniques



- Evaluation—Automatically conclude if anomaly is caused by fraud; integrated Active Testing and benchmarking features secure accuracy and avoid false positives
- Response—Trigger instant action at fraud case detection: Alarm, API call, blocking action

The solution resides in the cloud and run as a CSG managed service, providing the customer with continuous detection results.

ABOUT CSG

For more than 35 years, CSG has simplified the complexity of business, delivering innovative customer engagement solutions that help companies acquire, monetize, engage and retain customers. Operating across more than 120 countries worldwide, CSG manages billions of critical customer interactions annually, and its award-winning suite of software and services allow companies across dozens of industries to tackle their biggest business challenges and thrive in an ever-changing marketplace. CSG is the trusted partner for driving digital innovation for hundreds of leading global brands, including AT&T, Charter Communications, Comcast, DISH, Eastlink, Formula One, Maximus, MTN and Telstra.

To learn more, visit our website at csgi.com and connect with us on LinkedIn, Twitter and Facebook.