cataleya

FIGHTING VOICE FRAUD WITH BIG DATA ANALYTICS

BUILDING IDENTIFICATION AND MITIGATION INTO GLOBAL NETWORKS

UPDATE: FEBRUARY 2016

CONTENTS

OVERVIEW

Declining traditional voice revenues and increasing market competition post challenges to service providers in growing their profitability. As profit margins are extremely challenging, it is critical that profits are protected from fraud and minutes are monetised.

For some service providers, fraud losses might just be a small percentage of revenue. However for some others, it can lead to stagnating profits and even company insolvency.

The Communications Fraud Control Association (CFCA) estimates global telecom fraud losses at $38.1 billion in 2015 or approximately 1.69% of global telecom revenue. No matter the size of the service provider, any loss from voice fraud is unnecessary. Tackling fraud in a service provider's business will lead directly to increased profitability and a healthier, sustainable business overall.

The CFCA 2015 Global Telecom Fraud Survey notes that 89% of operators surveyed said fraud losses had increased or stayed the same within their own companies. While there has been progress in the fight against fraud, a large percentage of service providers have yet to see it in their businesses. Fraud losses remain steady or have increased while the market has become more challenging year-on-year. While service providers cannot change the market conditions they face, they can prioritise the fight against fraud by looking for new ways to combat these external threats.

“

The Communications Fraud Control Association (CFCA) estimates global telecom fraud

losses at $38.1 billion

in 2015 or approximately 1.69% of global telecom revenue.

THE FULL IMPACT OF VOICE FRAUD

The financial implications of fraud run deep in an organisation. In reviewing quarterly results, it is simple to see where fraud has impacted a service provider's bottom line. It directly takes away from short term gains in profitability and reduces a business's chances of success in the near term.

At the same time, fraud can damage a service provider's reputation and long term trust in the industry. Depending on the type of fraud that has occurred, customers or partners may be affected and see their losses related to doing business with the service provider. This compounds the initial loss from fraud and challenges the service provider to find partners and win new customers.

Customers find it difficult to select a service provider that they cannot trust and reputation damage caused by fraud can have a lot to do with that. In this way, fraud can cause a service provider to lose customers, partners, and profits. That is a formula that accelerates insolvency and guarantees an uphill battle to be successful in the voice market.

Similarly, fraud inhibits a service provider's ability to invest in its business and deliver next-generation services. If profitability gains are continually under threat, service providers will be challenged to make the necessary investments in their business to adopt new services and trust these next-gen services to support profitability.

Fraud losses can lead to a spiral of inaction that ultimately leaves a service provider unable to move forward in its business and deliver new services. This is why combating fraud is so important to developing sustainable businesses that are trusted across the industry.

AN EVOLVING THREAT

Fraud is a truly global phenomenon. The top 10 countries for originating fraudulent calls is spread evenly across developed and developing markets in Asia, Europe, Africa and the Americas. Criminals that commit fraud are clever enough to use a variety of destinations and not rely on one place of origin. Fraud calls are terminated in a similarly random set of countries like Cuba, Latvia, Taiwan, the United Kingdom, and Somalia.

There's no one market or destination that can be identified as a hub or home to fraud. It is also a constantly changing threat. There are many types of fraud like roaming, premium rate, PBX, IMEI reprogramming, interconnect bypass, and international revenue share fraud, and under each category there are also variations and differing shades of each type.

Fraudsters innovate like in any other businesses and that makes it very challenging to identify and mitigate voice fraud.

"The CFCA 2015 Global Telecom Fraud Survey notes that **89%** of operators surveyed said fraud losses had increased or stayed the same within their own companies.

COMMON TYPES OF FRAUD

1. FALSE ANSWER SUPERVISION: EARLY ANSWER / CALL DIVERSION SCENARIO

Early Answer is caused by one of the interconnect parties sending a false answer signal. This causes all the previous switches to start billing even when the called party has not answered the call. Call Diversion Scenario is a form of call hijacking to an automatic recording machine that emulates a ringing tone and afterwards tries to keep the caller in the call by playing recorded messages. The caller is unable to reach the desired calling party and it is charged for the call duration.

FIGURE 1: FALSE ANSWER SUPERVISION – EARLY ANSWER

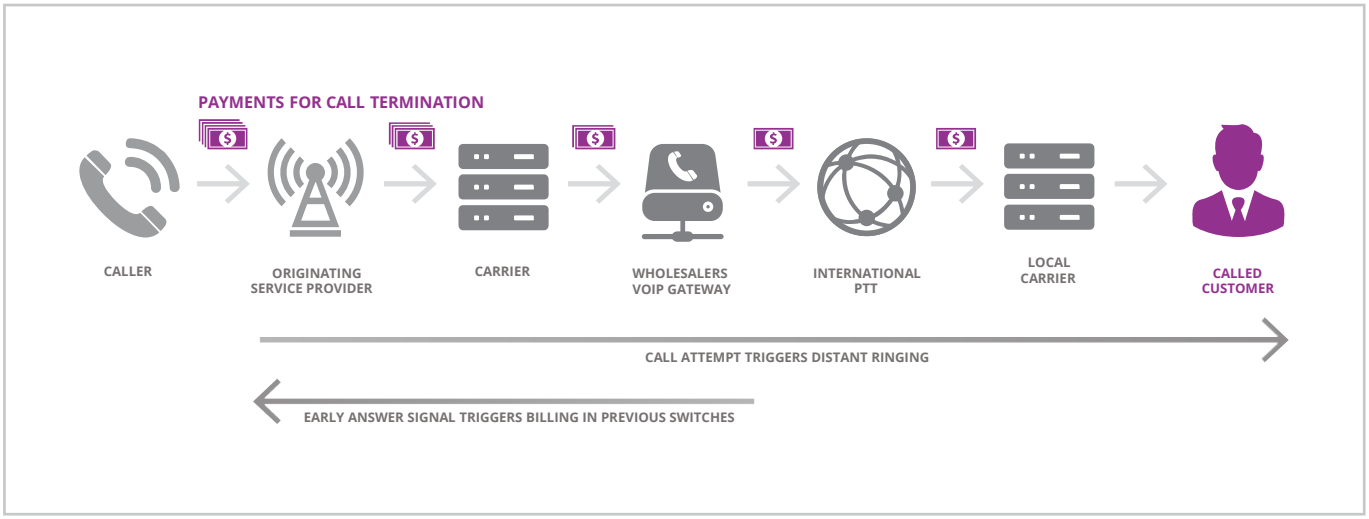
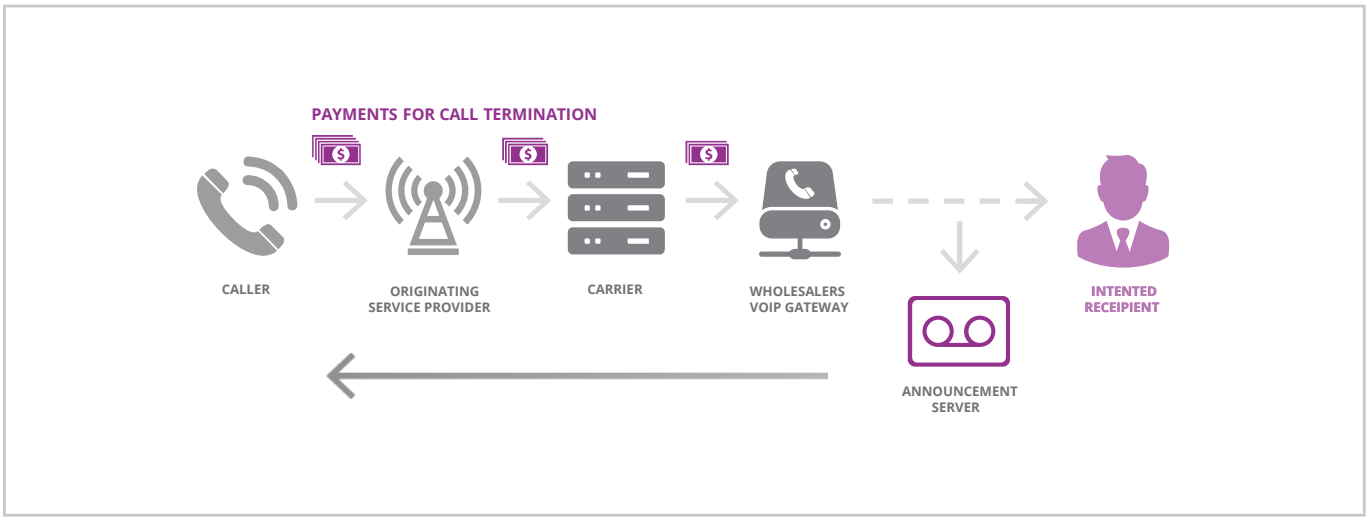


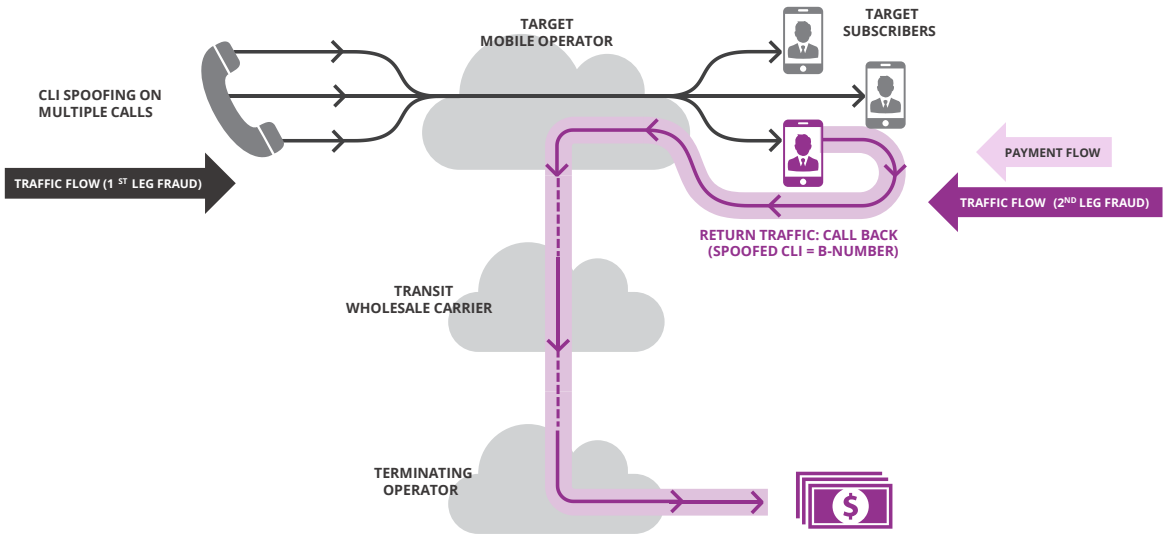
FIGURE 2: FALSE ANSWER SUPERVISION – CALL DIVERSION SCENARIO



2. WANGIRI FRAUD

This fraud is also known as "robot dialing + callback". The objective of the fraudster is to call thousands of users and hang up after one ring. The number that originated the call will be a Premium Number, unsuspecting mobile users will return the call paying a premium rate per minute. The premium number will many times be disguised as a local number.

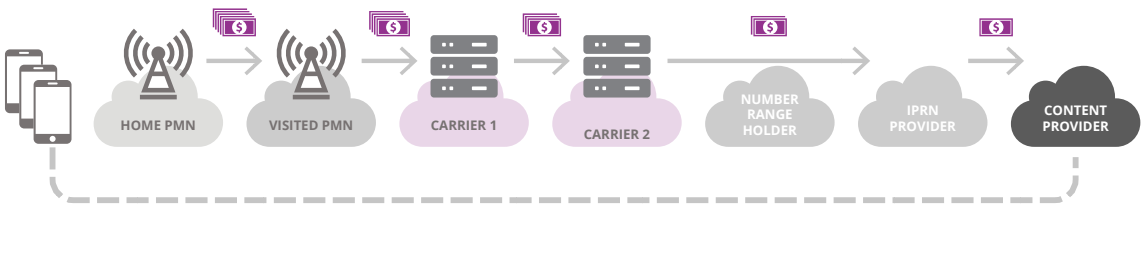
FIGURE 3: WANGIRI FRAUD



3. INTERNATIONAL REVENUE SHARE (IRSF)

Fraudsters take advantage of certain premium rate country terminations such as Somalia, Sudan, Pacific Island, and inflate traffic into these countries. The fraudsters can plan a role in the origination side by getting access to a fraudulent SIM or hijacking a PBX system, or on the termination side by colluding with content or IVR providers in the countries with premium termination rates.

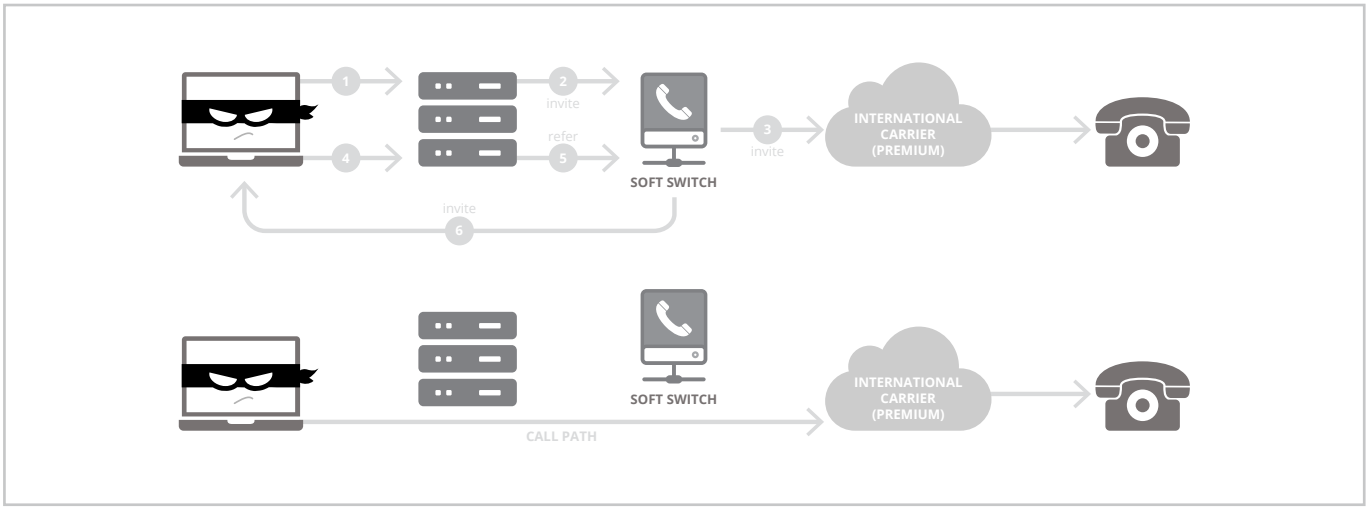
FIGURE 4: INTERNATIONAL REVENUE SHARE (IRSF)



4. PBX HACKING

Fraudsters hack into a PBX of an enterprise and once the PBX is hijacked, this results in several types of Fraud including IRSF etc. Typically, the hackers get into the PBX after office hours including weekends to drive up the traffic to premium destinations and take part in the revenue share fraud.

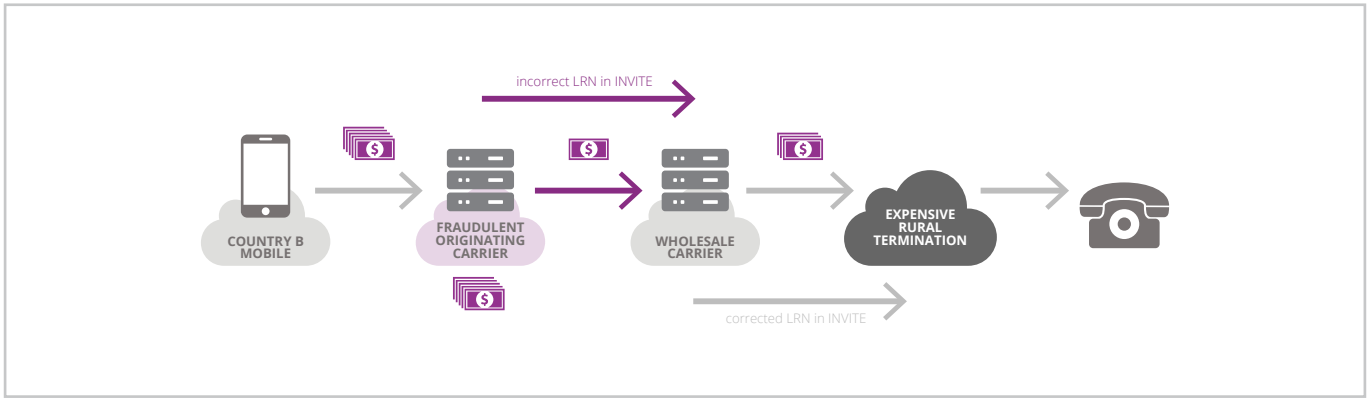
FIGURE 5: PBX HACKING



5. BYPASS FRAUD

Bypass fraud cases are generic and involve the bypass of a legitimate carrier in the delivery path of the call which SIMBox fraud case is one of the typical case. The Location Routing Number (LRN) fraud is one of the other case where the fraudulent operator sneaks in a LRN via a low cost route and send it to the wholesale provider where it tries to terminate the call to the indicated network, but the call does not go through and a „re-dip“ has to be done to the LNP server which provides the correct termination network on the high cost route and the wholesale operator will bear all the costs for termination.

FIGURE 6: LRN FRAUD USED FOR BYPASS FRAUD



6. SUBSCRIBER IDENTITY THEFT (SIMBOX FRAUD)

This fraud is particularly rampant in countries with high numbers of incoming international traffic and are loose in terms of availability of SIMs and law enforcement help. The fraudsters mainly use pre-paid SIMs where the ownership and address is hard to be detected. There are many variations of SIMBox fraud and thus, methods of detecting them vary as well.

FIGURE 7: SIMBOX FRAUD – INTERNATIONAL BYPASS

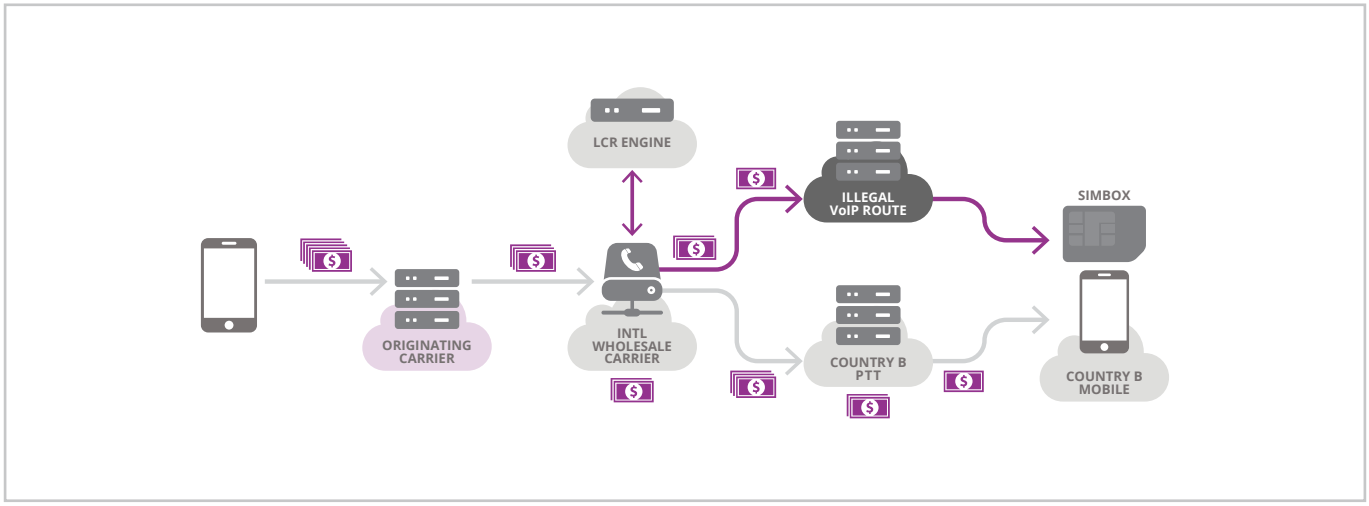
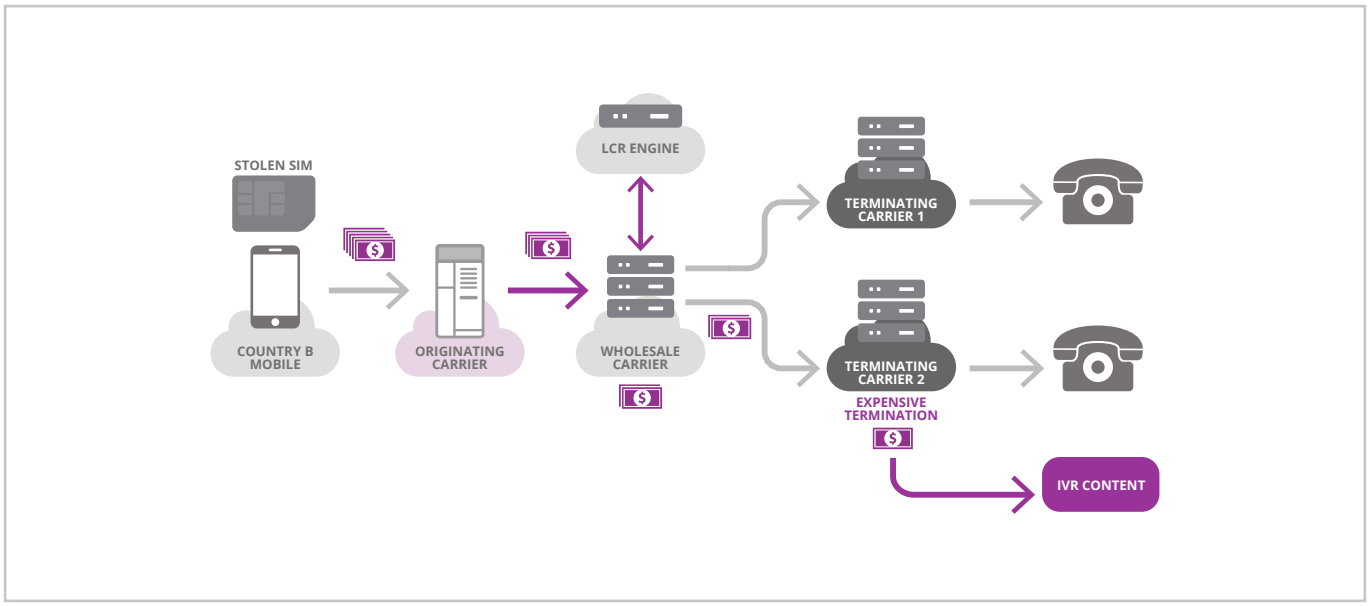


FIGURE 8: SIMBOX FRAUD – STOLEN SIM



NEW INTELLIGENCE

The challenge for most service providers is to find an effective fraud mitigation solution that can deliver the return on investments. The common practice for service providers is using rule-based fraud mitigation mechanisms by creating rules in its network to recognise specific fraud conditions.

While this is one way to mitigate threats, it only covers one aspect of fraud and fraudsters can easily identify when these rules are in place. It is not enough to protect an organisation when fraud is constantly changing and evolving.

Service providers need a proactive and data-driven approach to fight fraud. Network data and analytics supported with machine learning algorithms give service providers an evolving tool that can keep pace with changes in methods and types of fraud. Network data and analytics captured by a next generation session border controller (SBC) can be positioned to work to not just optimise network performance, but also to identify and mitigate fraud.

Sitting directly in the call path, the SBC has the ability to capture data in real time and alert the service provider of any abnormal behaviours on the network and in individual sessions. Voice quality (MOS, R-Factor), Real Time Protocol Analysis (One-Way & Two-Way RTP, Set-up & Disconnect Time Stamping) and call behaviour (automatic speech recognition, call distribution, post dial delay) can all be examined to determine fraud in real time.

Due of the role they play in the network, next generation SBCs offer deep analysis of signalling and media and offer unparalleled visibility. Compared to third party solutions or a solution that sits outside of the network, the SBC offers an immediate response with the added efficiency of using data that is available in the network.

The network data and analytics can be processed using machine learning algorithms that learn based on real fraud scenarios. These machine learning algorithms evolve and develop a database of behaviours that can be used to identify new types of fraud in addition to recognised methods of fraud. It works to recognise variations and suspicious call behaviours. Machine learning requires minimal user input while offering global scalability as it flexes and evolves to combat fraud.

Compared to the rule-based approach, machine learning offers immediate warnings about suspected fraudulent behaviour on a call. The call behaviour is immediately compared with averages and samples from the service provider and correlated with past behaviour. The service provider can then be alerted in real time and the issue investigated. With the rule-based approach, an alert may never be triggered and the service provider may only see the revenue leakage when examining invoices months after the event.

Real time call data streamed to ML algorithm

ML algorithm checks active all pattern and compares to historical data

Data is processed and broken into separate clusters for visual presentation

RULE BASED	MACHINE LEARNING (ML)
Call starts - 200 OK	Call start - 200 OK
Media starts flowing 9 seconds later	Media starts flowing 9 seconds later
Run media delay against fule implemented for >10 seconds	Log media delay, compare with averages and samples from same carrier. Correlate with Past Behavior
No Fraud Alarm triggered	Unusual excess of media delay, carrier is warned to investigate
Carrier is being charged extra for every call with up to 9 seconds media delay. Carrier does not know about this revenue leakage until the delay is higher than 10s	Carrier is being charge extra for every call with media delay. Carrier has been notified in real time about the occurence to confirm it.

If suspicious patterns are detected by ML, operator is immediately flagged

Visual representation of data will allow the operator to detect unusual events in the call flow

Based on the data collected and operator interaction, ML acquires new knowledge for future events

VISIBILITY AND PREDICTABILITY

The most powerful approach to fighting voice fraud combines historic data and call data records (CDRs) with real time analytics to deliver both visibility and predictability. This is about capturing network data and using it to evaluate what is happening on the network in real time. The benefit of this approach is the ability to quickly identify potential fraud and take action without delay.

According to the i3 Forum, it can take between 30 to 180 days to identify and mitigate fraud using a traditional approach. It can take 30 days to analyse the CDRs and possibly another six months of dispute resolution with partners. During that time, payments can be withheld and fraud may still be occurring as the dispute is being resolved. The cost to the business can continue to grow as minutes continue to flow.

When historic network data and analytics are combined with real time analysis, this scenario can be reduced to a less than 24-hour cycle. A next generation SBC can provide notification and graphical insights which makes it simple for the service provider to identify possible fraud and block it. The service provider can then notify the interconnect about the situation.

This minimises revenue leakage with added value of having hard data from the network to support the decision to block the fraud. If there is a dispute, the service provider can share a business intelligence report to prove where the suspected fraud occurred and minimise disputes with partners.

FUTURE OF FRAUD

Just as voice fraud is evolving, the SBC-based and machine learning-enabled fight against fraud is not standing still. As more service providers adopt this approach and deploy next generation SBCs, the stronger their capabilities will be in identifying fraud. Global databases of fraud patterns and behaviours will grow, strengthening a service provider's ability to fight fraud.

There are also opportunities to incorporate new data sets into machine learning algorithms to better identify threats. As Big Data grows in acceptance, there will be new opportunities to cross reference network data with other external factors. Assessing risk and identifying threats will become even more precise and in turn service providers will see thier revenue leakage decline.

The role of next generation SBCs in the fight against fraud is growing as network data and analytics are captured in real time and put to work for service providers. Real time data and analytics is critical to fighting voice fraud and its value will only grow as more next generation SBCs are deployed globally. Service providers cannot afford to play a reactive role in fighting fraud and must look at how they can use network data and analytics to minimise the impact of fraud on their businesses.

ABOUT CATALEYA

Cataleya is a leader in IP networking innovation, with a strong track record in developing and deploying next generation carrier grade switching systems, pushing the envelope in an all IP paradigm. Cataleya is headquartered in Singapore with its own technology development team in Silicon Valley and a wholly-owned subsidiary of Epsilon Global Communications Cataleya is another outstanding result of Epsilon's innovation DNA and reflects a strong service provider influence in the design and functionality of its technology. A new approach to new challenges has led to a product of unparalleled performance, simplicity to operate and reduced cost of ownership.

www.cataleya.com

www.cataleya.com

GENERAL CONTACTS

Europe: +44 207 096 9600 | **Asia:** +65 3016 4020 | **USA:** +1 408 571 2200 | **Email:** info@cataleya.com