Addressing Telecom Fraud to Plug Revenue Leakage

By Abhilash M, Architect, SunTec Business Solutions
Pranoy P, Analyst, SunTec Business Solutions
Sherin Leya Oommen, Analyst, SunTec Business Solutions

A customer of a leading telecom operator receives their monthly bill and is shocked to find it running into several thousand dollars. The call details reveal hundreds of calls to international locations that they never made. Yet the telecom company says that the bill is genuine and not an error at their end. Unfortunately, both the customer and the telecom service provider are victims of telecom fraud. Today DCS' are often connected with the corporate network but inadequately protected. This presents a weak spot for hackers to exploit, resulting in significant revenue leakage. Communication service providers usually ignore the threat as they consider the losses from individual incidents minimal, but over time, these leaks can have a significant impact on revenues. Over the last year, as the world grappled with the COVID 19 pandemic, incidents of fraud went up significantly, and raked up a considerable financial impact as well. Can organizations really afford such massive losses? And how can they improve their fraud management measures?

The Mechanics of Fraud

In the telecom sector, most fraudulent activities usually take place at the provider level. Hackers infiltrate the service provider and then install duplicitous systems that are not detected by the organization. This then generates large bills that the customer has to pay. Hackers can also attack the customer's phone network through their voicemails, improperly disposed of SIM cards and pre- paid calling cards. They then use the customer's phone network to make expensive unauthorized calls. Most service providers have established terms and conditions that make it the customer's responsibility to pay for calls made from their phone system even if they are fraudulent. But this is rarely implemented in practice, and most often service providers bear the cost of such calls. According to Europol's European Cybercrime Centre and Trend Micro, globally, fraud costs the telecom sector USD 32.7 billion every year.

Kinds of Fraud

Scams within the telecom sector can target different systems. It is important to understand the different kinds of fraud to better prevent them. Here are some of the most common kinds of illegitimate activity targeting key functional areas within the telecom sector.

- **VOIP Telephony** – Hackers access a customer's telephone system and then manipulate it to make unauthorized long-distance calls, creating an exorbitant bill. Alternatively, hackers can also access the telecom system and make calls to black-listed countries, also racking up massive bills. The fraud is uncovered only when the customer receives the bill. Service providers need to invest in intelligent security systems that can block calls to locations identified as high risk for toll fraud. The system should also be able to track the customer's usage patterns and be able to flag unusual call activity.

- **Data:**Cloning is the most significant threat in cable networks. In this, two modems have the same MAC address and appear to be one device. This means that the cloned device will receive the same service as the actual one without paying for it. The Communications Fraud Control Association (CFCA) estimated that service providers in North America incurred close to $1billion in lost revenue from cloning fraud. Telecom service providers need solutions that can map the network configuration to automatically detect and prevent cable modem fraud. With such a solution, service providers can stop revenue leakage and better manage QoS for actual subscribers.

- **Video Streaming** – As OTT platforms, Pay TV networks, and video streaming services continue to gain popularity, the sector is witnessing different kinds of scams. Identity theft, account fraud – sharing and takeover enabled by password sharing are emerging threats before this sector. Approximately USD 9.1 billion was lost due to account sharing and data piracy in 2019 alone and this number is expected to go up to USD 12.5 billion by 2024.[2] Players in this sector must implement effective solutions that can detect and prevent unauthorized users and bad actors.

Preventing Fraud

Service providers must focus on detecting and preventing fraud across their infrastructure to plug revenue leakage and maintain customer trust. The first step to prevention is to understand the system by documenting the different components, and comprehensive revenue processes. This end-to-end infrastructure mapping can help identify vulnerabilities and possible threats. The system must be monitored continuously to detect attacks in real time and analyze line loss factors. Whenever a new technology is introduced, service providers must ensure compliance to industry standards and monitor it closely, as they may introduce new opportunities for revenue leakage. The organizational strategy must include effective, state-of-the-art monitoring tools and performance indications, and solutions for carrying out root cause analysis to resolve problems. As with most things in the current digital era, fraud prevention too is heavily reliant on effective use of data. The system must be able to analyze data across key indications like subscription growth, transactions, conversions, and recurring billing to trace gaps in revenue flow. It should be able to monitor call activity, understand behavior patterns, and even review bills to flag aberrations.

Fighting Fraud Better

Service providers must invest in high performance platforms that have a service-oriented architecture and built-in support for big data storage. AI and ML capabilities will ensure a formidable defense against most threats. Some key features to look out for when investing in a fraud management solution include ML Engine, ML Service, Intelligent tagging, and dynamic rule-based decision services. Most good solutions come equipped with real case scenarios of possible scam activities and their solutions. And the organization can also address business specific threats thanks to its flexible and dynamic rules. Any technology platform designed to help service providers fight fraud will increase the lifetime value of their customer relationships through real time customer engagement and contextual product and technology innovation.

Fraud is everywhere in the 21st century business landscape, and organizations can no longer afford to continue with ineffective security solutions that cannot track, identify, and report suspicious activity in real time. But along with technology, it is important to remember that an organization's security posture is also dependent on awareness and a culture of secure behavior within its walls. Regular training sessions for employees and customers is a vital ingredient of an enterprise security strategy. The threat landscape is only going evolve further as hackers come up with increasingly sophisticated attack approaches. Enterprises must focus on a robust security strategy to stay one step ahead of bad actors.

Sources:

1Businesswire

2Cision PR Newswire