www.pipelinepub.com Volume 8, Issue 3

AI’s Role in Combating Next-Generation Fraud

By:

Fraud is a pervasive problem for Communication Service Providers (CSPs). When CSPs worldwide collectively lose $29 billion due to telecom fraud, they cannot afford to ignore potential solutions. AI and analytics hold tremendous potential: Gartner recently estimated that new implementations of Machine learning (ML) in fraud management have the potential to save CSPs millions of dollars, reducing fraud losses by as much as 10 percent by 2022.

So why are AI and analytics so critical in the fight against next-generation fraud?

Fraudsters are already experts in AI and automation

There is no doubt that fraudsters are leveraging automation and technology to commit crimes faster and more effectively today than ever before. Fraud scams such as Wangiri use an auto dialer to call multiple people simultaneously and immediately hang up before they answer. The aim of the scam is to entice those who see a missed call on their phone to call back. When they do, users are charged a premium fee for the call. This fee is then syphoned off to the fraudsters. Fraudsters are also capitalizing on the rise of bot technology to conduct the next generation of subscription fraud. Fraudsters can quickly launch a bot attack that randomly tests login credentials and common user passwords to look for ways to gain control of accounts, which are then used to order devices and costly services.

Fraudsters also target CSPs directly by using machine learning techniques to detect whether a carrier has a fraud management system in place—and then target those who don’t. In addition, they will sometimes create distractions or ‘honeypots’ by committing small, easily detectable types of fraud; and then, while the carrier is focused on stopping these efforts, go after more lucrative areas.

When fraudsters infiltrate your network, the challenge is to pinpoint them in a crowd, especially when they seek to deceive your controls by imitating the behavior of ordinary customers. With so much data and complexity in the network happening so fast, however, it becomes much more challenging for fraud managers to quickly zero in on the relevant information and focus on the real fraudsters.

This is where machine learning and artificial intelligence (AI) capabilities are required. Machine learning and automated contextual analysis expedite how to respond to suspicious behavior and provide helpful background information by combining data with context and repeatedly adding the latest new data to the accumulated history. Ultimately, these capabilities help fraud managers determine the right decisions exactly when they need it.

Rise of 5G will create new vulnerabilities for fraudsters to exploit

In the growing 5G and IoT ecosystem of partners, platforms and services, CSPs will experience increased complexity that raises many fraud management challenges that need to be addressed. IoT devices have become a welcome mat for hackers. Smart homes give fraudsters new opportunities to hack: a home security system, HVAC or smart speakers are a few easy ways for the fraudsters to obtain a customer's account details and make additional fraudulent charges. Consider this example: a smart washing machine should connect to the local grocery store to order detergent when supply is running low. Instead, if hacked, this same washing machine could now be making calls to premium phone numbers, with the charges being directed back to the customer. Yet it's not only the devices that CSPs need to guard against, it's also the system. The IoT's growing ecosystem of partners, platforms and services introduce added complexity that will increase the opportunity for bad actors to find new ways of breaking the system. For example, as IoT devices are equipped with eSIMs, they will welcome new opportunities for traditional types of telecom fraud to make a resurgence, such as subscription fraud, international revenue share fraud and traffic pumping.

The beauty of the IoT's connectedness is also its downfall. Once hackers have gained account takeover of one device, a smart home instantly becomes a plethora of devices and services to conduct subscription fraud at lightning speed. Machine learning capabilities can now be used to identify and stop new types of telecom fraud. While rules-based algorithms do a great job at spotting fraud we already know about, machine learning algorithms can quickly spot the 'outliers' or abnormal behavior that could signal new fraud and security schemes that we have never seen before. This is vitally important as we move into an era with new technologies, new devices and new services—and where risk can go beyond commercial terms, to even impacting the wellbeing of customers who are using new services like connected cars, e-health or home security.

As we enter the 5G era, it becomes more apparent that CSPs will require robust fraud management methodologies that utilize the power of machine learning and automation to turn data into powerful risk management insights and actions in order to predict, detect and safeguard against vulnerabilities.

AI and Analytics: Supercharging how CSPs

Prevent Next-Gen Fraud

To date, traditional rules-based fraud systems have been the primary tool for telecom fraud departments—and they still play a critical role in preventing abuse. Rules-based algorithms are very good at spotting and stopping the types of fraud they are designed to stop. But that's where the value ends. Machine learning takes fraud management to the next level. The technology relies on the same foundations behind 'suggestion engines' for companies like Spotify and Netflix. These services can predict what you might like to watch or listen to next, and they analyze your previous behavior to do so. The more data these systems ingest, the more accurate they become. With machine learning, the software gets better and 'learns' over time.

In fraud management, where the value of machine learning (ML) stands out is on the more complex fraud schemes, which are increasingly being designed to mimic human behaviors and fly under the radar of rule-based systems. IRSF, interconnect bypass and voice or wholesale fraud all share this characteristic and are prime use cases where ML can offer value by tracking anomalies more quickly.

Not only are advanced analytics, AI, machine learning and automation required to process and manage the sheer volume, velocity and variety of data that a 5G network will generate, these technologies will also improve the ability for CSPs to spot known fraud threats—as well as new, unknown ones. It is also important to reinforce the notion that fraudsters already have AI and automation in their arsenal of weapons, giving them the ability to organize their actions over a huge scale—and then essentially train a computer to keep repeating and optimizing the process as it searches for new opportunities to commit fraud. When one type of fraud—like subscription fraud—can lead to another more damaging kind of fraud—such as IRSF or something even more threatening—it becomes essential that operators have access to their own ML/AI tools as well.

While machine learning should be viewed as a critical part of a CSP's toolkit for minimizing telecom fraud, it is not a panacea. Legacy driven siloes between OSS/BSS, security, and fraud management must be broken down so that the different guises of fraud can be detected earlier. Every day the level of sophistication and organization among fraudsters increases. By relying on the traditional model of risk management governance, where the key auditing functionalities have been relegated to isolated selections of tactical technologies, management features, and operational procedures along the value chain, CSPs will simply fail in the 5G era. Gone are the days when a simple set of rules built on top of OSS/BSS data would be enough for CSPs to detect fraud and stop revenue leakage. This approach must change immediately if CSPs want to minimize their threats.