Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 13, Issue 8

Digital Transformation Has Opened New Doors to Telecom Fraud, and Machine Learning is Coming to the Rescue

By: Joao Resende

The digital transformation is creating tremendous opportunities for service providers, whether you are talking about traditional communication services or new digital services. New technologies, new devices and even new business models are reshaping the world service providers live in. But it also creates new opportunities for fraud and revenue leakage; hurting carriers' bottom lines - and their reputations. According to the 2015 CFCA Fraud Loss Survey, Telecom Fraud is a nearly US$4OB annual business. The reason fraudsters are so successful is that telecom networks and business systems are very complex – providing a veritable breeding ground for "points of failure" that can be leveraged to their advantage. But that number is only the tip of the iceberg. Most of the fraud types reported in this survey are still focused on old traditional services. The amount of new fraud that the industry is at risk of experiencing is staggering when compared to the figures reported today.

New risks caused by IoT and the big data revolution

With all-IP networks, the onset of network virtualization functions (NFV) and the Internet of Things bringing a new type of complexity to the table, suffice it to say that the future is looking good for fraudsters. Billions of potentially untested and unsecured newly connected chipsets, modules and devices are entering the market, along with an entire ecosystem of digital service provider partners, new digital services, complex revenue share plans, and B2B2X business models. The number of transactions (aka opportunities for fraud) are exploding – but service provider margins are shrinking. This makes even small losses painful.

While most Communication Service Providers (CSPs) are focused on launching new services and partnerships with Digital Service Providers (DSPs), our fear is that security and fraud are being sidelined as an afterthought – or that CSPs will believe that their old ways of managing fraud will suffice. Nothing could be further from the truth. And from a revenue assurance perspective, things aren't getting any easier either, when you take into consideration that most new business models and partnerships require real-time billing and settlement; linking connectivity to applications, SLAs, chargebacks and margin controls that go down to the level of assets provided to CSPs. Things are getting very complicated and messy – and there is a lot of money at stake. Yesterday's fraud and revenue assurance tools simply weren't built for today's connected world.

The IoT industry recently experienced hackers taking over millions of connected things like security cameras, DVRs and even refrigerators to initiate denial of service attacks (DDoS), bringing down websites like Spotify, Twitter and Netflix. With service providers making up a critical part of this new ecosystem, it's just a matter of time before new IP and IoT enabled fraud starts impacting the service providers' revenue chain. After all, fraudsters always tend to "follow the money". But fraud doesn't typically happen in plain sight. How will we be able to detect it if we don't know what we're looking for? The ability to predict the future – to know the unknown – is what service providers need.

How machine learning is being used to tackle fraud

Fortunately, as fraudsters are growing increasingly sophisticated, so are the tools for combatting them. Service providers are swimming in data – really, really, BIG data. And with today's new machine learning based analytics techniques, CSPs can now detect new fraud types practically in real-time, just as they are emerging.

Rules-based fraud systems have been the primary tool for telecom fraud departments for many years – 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 a whole new level. It's the technology behind "suggestion engines" for companies like Spotify and Netflix. It's how these services can predict what you might like to watch or listen to next, and it's all based on analyzing your previous behavior. The more data it ingests, the more accurate it becomes. With machine learning, the software gets better over time – it "learns" on its own.

The same types of machine learning techniques are now being 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 dollars and cents, to even impacting the health and safety of customers who are using new services like connected cars, e-health or security.

It appears service providers are beginning to recognize the benefits of machine learning. WeDo Technologies' conducted its own telco fraud survey in the fall of 2016. The survey collected responses from 14 North American communications service providers. Twenty-one percent stated that they are currently using some form of machine learning or artificial intelligence (AI) for fraud management, while nearly twenty-nine percent revealed that they have plans to do so in the future. Machine learning techniques are especially suited to stopping fraud, because they can be used to identify unusual patterns and correlations from disparate data sources. By combining modern distributed system architectures with the ability to ingest massive amounts of data from new data sources, service providers are opening a new window into fraud detection that never existed before.

Digital risk profiling - the latest weapon in the fight against fraud

Telecom fraud is increasing in complexity, and the types of information we gather – our fuel for fighting fraud - needs to change as well. With valuable external data sources at our fingertips, it would be foolish to ignore the benefits this information can provide. The use of both external and internal data sources allow service providers to gain a deeper understanding of suspicious activities, identify patterns, and detect unusual transactions. Service providers can now leverage Big Data, the latest data mining techniques, and the power of machine learning, to create instant digital risk profiles that can help combat the growing threat of different fraud types, especially subscription fraud. Subscription fraud is when a fraudster signs up for services with no intent to pay. It constitutes about 40% of all telecom fraud today, and it is seen as a "gateway" type of abuse because it is often the initial way fraudsters begin their broader attack on a network operator. Therefore, stopping subscription fraud has a carry-over effect of reducing other types of fraud as well.

By tapping into the hidden value of social media and other freely available information gathered from the web, data can be utilized to create or enhance a person's risk profile, establishing an effective way to flag high-risk individuals or businesses before they even become customers. There is a growing amount of publicly available digital data spread across various sources throughout the web on practically every individual. CSPs can leverage this information, but attempting to find and collate it all manually is inefficient and costly.

With the right fraud management tools and the latest advances in machine learning, pertinent information can be gathered and analyzed in near real-time to create a risk profile of a particular user or company in question. The main goal is to provide a statistically sound, probability-based view of the predicted risks they pose.

A Digital Risk Profile can be created by analyzing publicly available information, which can include social media activity, education, demographics, and more. Digital risk profiles can help flag suspected fraudsters by enabling fast, evidence-based decisions that dramatically increase the speed and efficiency of threat research and analysis. It allows CSPs to find hidden connections within new and emerging threats, and improve identity verification by spotting current and new customers who are actively manipulating their identities in the marketplace. Another benefit is that, with today's technology, it can all be done over the cloud, with practically zero implementation time.

Telecom fraud isn't what it used to be. Managing today's threats require the latest tools and the right partners. There is too much at stake to go it alone.