Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Identity Fraudsters Stole over $16 Billion from US Consumers in 2017. How can CSPs Reduce the Risks?

By: Bernardo Lucas

While we have emerged from the first quarter of 2018, consumers are still feeling the hangover effects of 2017. Sobering statistics and stories of how consumers around the world are being targeted by fraudsters continue to surface. A new study by Javelin Strategy and Research found that in the U.S. alone, identity fraud victims increased by 8%, resulting in $16.8 billion being stolen from 16.7 million U.S. consumers in just one year. The survey found that e-commerce shoppers experienced the highest prevalence of fraud, and consumers who are digitally connected were exposed to a 30% higher risk of fraud than those who are not. As the world, including fraudsters, embraces the digital transformation, how can communication service providers reduce the risks of identity fraud for their customers?

In today’s mobile-centric world, the use of mobile phones as a token for subscriber identification has become standard practice for most people. However, SIM-swap fraud, where scammers cancel and re-activate new SIM cards to hack services such as bank accounts, has been on the rise. Currently SIM-swap fraud is quite difficult to detect. Since it is a fairly new type of scam, telcos and banks are still trying to find effective ways of identifying when a customer’s mobile number has been fraudulently swapped and ported onto a new device. With fraudsters continuing to exploit this weakness, better authentication processes must be put into place.

In response to this need, new advances and technologies are rapidly being developed. 2018 is widely expected to be a breakthrough year for biometrics. In biometrics, body measurements such as finger prints, iris or retina recognition are used as a customary form of authentication. In fact, video identification is becoming a secure and user-friendly approach to enable mobile network operators (MNOs) to offer online mobile contracts with ID verification. While the *Mission: Impossible* movies have been showcasing this technology for decades, it is finally moving beyond science fiction to become part of our daily lives. Major moves are being made across the financial, consumer tech and automotive industries, to name a few, to get this technology into the hands of consumers.

For example, the auto industry’s adoption of biometrics is expected to grow 38% during 2016-2025. Market research firm Acuity estimates that by 2020, 100% of smart phones will include embedded biometric sensors as a standard feature – demonstrating the acceptance by both consumers and enterprises of biometrics as a credible and trusted form of authentication. While this technology is exciting, used in isolation it can still be thwarted by determined fraudsters. You may remember that it only took a matter of days for Apple’s Touch ID fingerprint scanner, iPhone X Face ID and Galaxy S8’s facial recognition and iris scanners to be tricked with fingerprints copied by a high-end printer. To make matters worse, biometric data has been named as one of the hottest targets for hackers to steal in 2018 – making it more difficult for CSPs to trust who is really on the other side of a transaction.

It is for this reason that Identity and Access Management (IAM) and other security leaders must ensure that, in addition to biometrics, one or more additional methods are implemented to provide a second layer of security.

The growing adoption of eSIMs will provide greater protection than traditional SIM cards. Instead of storing user authentication details on physical SIM chips, which can be swapped out and put into other devices to avoid detection, each eSIM is permanently embedded into the handset, along with its user’s unique biometrics and security passcodes. This way, only the owner can access a phone.

In addition, eSIMs will provide CSPs with greater control and will be able to prevent malicious apps from being downloaded onto a handset through initiatives such as the GSMA Security Accreditation Scheme.

However, even with multi-factor identification, if the initial profile is spoofed using a synthetic identity (Synthetic ID), and false accounts are created to support these fake identities, these prevention methods will still fall short. The rise of synthetic identities, or IDs created using either real, stolen or fake identity data, is estimated to have cost banks at least $6 billion in 2016. Synthetic IDs are being used by fraudsters to subscribe to new services without the intention to pay for them. In fact, these phony IDs can be made with just a few bits of stolen information, such as a social security number and birth date, to construct a whole new persona. The issue is becoming more pervasive by the day – and harder to identify. In social media, this problem has come to the fore: 48 million Twitter accounts were found to be run by bots instead of real people.

One of the areas that has exposed consumers to identity fraud through their social media accounts is the growing adoption of single sign-on and the use of social media accounts (like Facebook) to log in to other third-party sites. This has quickly become popular with consumers because in one click, you are immediately signed up or logged in. It's the perfect way to bypass the cumbersome, time-consuming process of entering in your information or remembering countless passwords. It is estimated that, when given the option, 65% of consumers will choose a social login vs. typing in an email address.

Enterprises are also quick to get on board and are currently seeing registration rates increase by 50% when they offer social logins. Today, 80% of the top 100 U.S.-grossing iOS and Android apps allow users to log in using their Facebook credentials. While consumers see this convenience as highly beneficial, in an era of enormous data breaches, social logins also provide an opportunity for fraudsters to utilize fake social media accounts to sign up for all sorts of services.

The good news is that while social media may be at the heart of the issue, it can also be used in the fight against synthetic IDs. Social media platforms have become a valuable open source of data that enables the passive acquisition of information about people, cultures, places and events around the world. Valuable new insights can be gained just by scrolling down a user's timeline. However, when we understand the sheer volume of social media activity in a given 'internet second' (e.g. 7,599 Facebook posts sent, 1,779 Instagram photos posted, 69,100 YouTube videos viewed) it would seem an overwhelming task for a fraud department to take this on single-handedly.

However, using new technologies, CSPs can now take publicly available online social data, along with other records collected in their OSS/BSS systems, to create a Digital Profile of every user, to help determine a person's risk profile. Using AI and Machine Learning capabilities, this analysis enables CSPs to establish an effective way to identify potential synthetic IDs, flagging high-risk individuals or businesses before they even become customers, and better understand the structure, hierarchy and methods of criminal, terrorist and fraudulent networks.

This is where an integrated approach to security and fraud management is required. With this approach, information can be constantly monitored across an organization, noting unusual trends and identifying fraud before it happens. That way, when security is breached, the fraud management system will be able to follow its path and identify patterns that reveal hidden relationships and suspicious movements and minimize any potential damage.

Marketing, sales, customer care, billing and charging, and network operations all have a part to play in protecting your network. Additionally, they hold data within their systems that can provide intelligence to identify the occurrence of potential fraud. For example, charging teams can provide valuable data from their Policy and Charging Rules Function (PCRF) solutions. CSPs can identify fraud by monitoring charging rules, then correlating this data with the information coming from the deep packet inspection (DPI) system to ensure traffic is being assigned and charged for appropriately. In addition, your security information and event management (SIEM) logs can be used to support active fraud detection by helping to identify when fraudulent apps have been installed. By defining which events are of interest, and how they should be responded to, the SIEM security logs can be used to temporarily adjust your thresholds to impose channel limitations or enforce caps, helping to prevent fraud and abuse.

In this environment, CSPs can go beyond traditional rule-based fraud detection. Rule-based detection is effective for identifying simple, recognized patterns, such as validating black lists of fraudsters. But in today’s high-stakes environment, we need to take it to the next level. Artificial intelligence is required to create actionable insights in this age of big data. Machine learning technologies can quickly identify abnormal patterns and correlations from disparate data sources, making fraud detection faster and more efficient. In addition, machine learning algorithms can also be used to target more complex risks, including those which haven’t even been identified. This will enable CSPs to rapidly spot and react to different threats as they arise.

The lines are becoming increasingly blurred between telecom fraud and cyber-security. The ability to stop this type of fraud at the front door, so to speak, will help reduce the incidence of all types of cybercrime and should be a critical component of every service provider’s fraud management toolkit. What’s more, as IoT grows and newly connected devices come onto the market by the billions, the ability to ensure that people are real, that identities are not compromised, and that businesses and consumers are being protected is imperative. Without these protections in place, consumer trust will erode, and the promise of the digital transformation could be compromised.