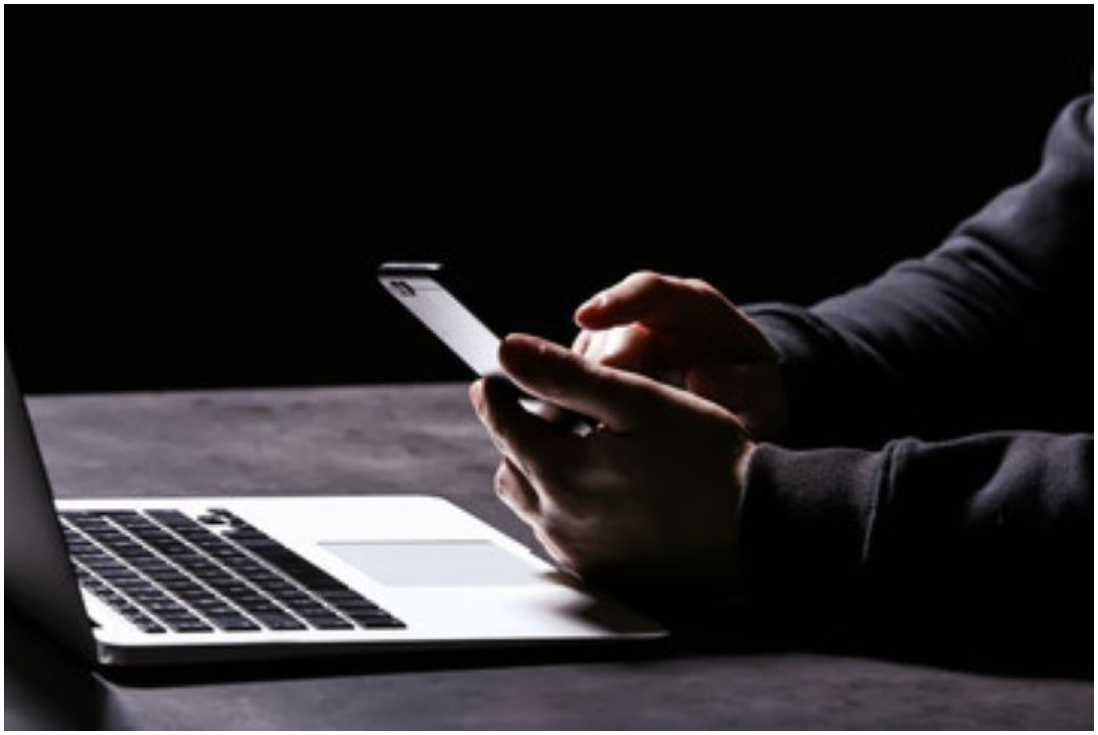
NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

Fraud losses are down for the telecommunications sector, but attacks are not

Nuance Communications

June 8, 2020



The Federal Trade Commission's latest fraud report estimates over 36,000 fraud reports in the U.S. and losses of over $25M – in the current COVID-19 environment, that number is growing by the day. Although there are surges in fraud attacks, the trend looks different for the telecommunications vertical. Telcos are seeing a momentary downturn in fraud, but it's critical to understand the full picture of risks.

In the telecommunications segment, subscription fraud is where most financial losses are seen. Each account successfully opened by a fraudster has an average loss of ~$1500, and virtually 1% of all account activations are fraud incidents for telcos. Subscription fraud occurs when a fraudster uses a stolen or synthetic identity to obtain mobile devices and services with no intention to pay for them. Given the high price of devices, there is an active grey market that exploits consumers seeking to obtain devices for lower resale prices, making subscription fraud lucrative for fraudsters.

Today, fraudsters are doing what most organizations are – adapting to the new normal. At present, the conditions make it less profitable to set up accounts in an attempt to obtain devices, and many carriers are seeing a dip in subscription fraud as a result.

Account takeovers (ATO)/SIM Swap attacks are poised to explode

An account takeover (ATO) is when a fraudster uses stolen information to take control of a victim's account. Credit card fraud is rampant when it comes to ATO; but in addition to seizing control of a credit card or bank account, ATO is commonly used to gain control of phone accounts. This kind of telco-specific ATO can also be known as "SIM swapping."

By changing the SIM card associated with the phone, a fraudster can intercept calls and SMS messages sent to that phone number. SIM Swapping is more and more common as fraudsters take advantage of many enterprises relying on over the top players (OTPs) to use SMS to protect customer information – think of when a special code is sent to you via SMS for authentication. Once a fraudster has your personal information and phone number, they can get these codes, call your phone company and ask to have your number transferred to a new phone. The fraudster then has access to all of your accounts on their device. With so much tied to our phone today – from bank accounts to personal files and work emails – SIM swapping fraud impacts are incredible and can be devastating. In most cases, the consumer is left *holding the bag*; however, there are several pending lawsuits against top telcos for not protecting the customer against SIM Swaps and ATO.

While subscription fraud might be down, SIM swapping is likely to see a considerable increase as a result of fraudsters taking advantage of the government stimulus and relief money being sent to consumers. While on the surface fraudsters may be trying to attack financial institutions to gain access to these monies, the telco is the path for those fraudsters to get into victims' bank accounts successfully. They need to intercept OTPs, meaning SMS messages that have details on consumer information, confirmation codes, and even timing of relief payments.

How telcos can prepare

Carriers have much more at stake than money; in most cases, their reputations are also on the line. With customer acquisition costs in the telecom space upwards of $500, protecting subscribers is even more critical than ever.

Fighting fraud is like playing "whack-a-mole," just when you figure out one technique and thwart it; another pops up in its place. Two-factor authentication (2FA) using SMS represents a considerable vulnerability for all organizations, with fraudsters leveraging SMS protection as a Trojan Horse to gain access to everything from mortgage deeds to bank accounts. The good news is, this does not have to be a losing battle.

Organizations all around the world have overcome this vulnerability and decreased the risk of SIM swapping attacks by leveraging the power of biometrics to provide a secure 2FA method. Push notifications combined with biometrics gives a safe and reliable way allowing for an easy and seamless authentication process.

Subscription fraud is also likely to see an uptick after its initial downturn when fraudsters start to leverage the data they obtained via phishing operations during the start of the pandemic. We expect to see subscription fraud return to normal levels, if not exceed those levels due to the increase in data fraudsters have likely gathered in the past months. Telcos should be ready for that surge, and biometrics provides the most efficient tools to prevent identity fraud, including subscription fraud.

For more information on Nuance biometrics and how its AI solutions can help telcos battle fraud click here.

Simon Marchand, Nuance Chief Fraud Prevention Officer, also contributed to this post.

Tags: Voice biometrics, Fraud prevention, Telco, SIM fraud

More Information

Learn more