NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

Telcos and SIM swap fraud: protecting consumers and mitigating risk exposure

Brett Beranek | Vice President & General Manager, Security & Biometrics

July 16, 2021

As the number of high-profile SIM swap frauds rises, telcos, financial institutions, and other organizations must do more to protect their consumers and lead with security. Every product, service, and interaction must have a cross-channel security approach baked in.

Over the last several years, a number of high-profile SIM swap frauds have come to light: from Twitter's Jack Dorsey in 2019 to Stefan Thomas, who lost his entire cryptocurrency investment in a SIM swap scheme. And, although it's not a new type of fraud, there is so much more at stake now than before. The accelerated adoption of mobile banking and fintech applications means that people's financial resources could be at risk.

Many organizations have published guidance about how consumers can help protect themselves from SIM swap fraud, but the fact of the matter is this: Placing this responsibility on consumers' shoulders ignores the realities of how fraudsters truly operate. Moreover, when it comes to preventing identity fraud, enterprises have the most power—far more than consumers do. In short, telcos can – and should – do more to protect their customers and help mitigate their risk exposure.

Protecting consumers by leading with security

Security simply cannot be an afterthought. Consider the story about a parrot who learned to order goods, turn off lights, and otherwise command a digital home assistant. It's one of many examples that illustrate the ways in which security takes a back seat to product design, interface, and usability.

Instead, security needs to be built into every product, every service, every interaction. The good news is that solutions are available, and a growing number of telcos have begun to adopt them. High-risk transactions should be protected by additional verifications, such as two-factor authorization leveraging biometric factors such as voice. Doing so will help prevent unauthorized modifications to a subscriber's account—something that can lead to significantly more damaging attacks against bank accounts, cryptocurrency wallets, and so on.

As an example, multi-modal biometrics have helped one Brazilian telco identify fraudsters more efficiently and effectively, helping to reduce their losses due to fraud. As another example, Deutsche Telekom has adopted voice biometrics to create a quick and secure authentication process for its customers, something that's also had a positive impact on the company's frontline workforce.

As SIM swaps and other contact center frauds continue to plague organizations, telcos must recognize their responsibility in helping to prevent fraud. Focusing on the direct costs associated with account takeovers often means ignoring the indirect, yet monumental, costs of fraud that victims and other organizations must bear. A cross-channel security approach is a necessary first step toward protecting consumers and mitigating risk exposure. At the end of the day, multi-modal biometric fraud prevention solutions help telcos and other organizations find known and unknown fraudsters before they can commit their crimes.

To learn more about Nuance's security and biometrics solutions, please go here.

Tags: Fraud prevention, Telco, SIM fraud, Nuance Gatekeeper

More Information

About Brett Beranek

Brett Beranek is responsible for overseeing the security and biometric line of business at Nuance, a Microsoft company. In this role for the past 12 years, Beranek has brought Nuance to a leadership position in the biometric authentication and biometric fraud prevention space. A thought leader in the field of biometrics, Beranek is a frequent contributor in industry events and the media on the topic of AI technology and it's use by the fraud community, and how society can mitigate against these evolving threats. Prior to Nuance, he held various leadership positions in the biometrics and security industry. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management. Beranek is also a certified Master Fraud Prevention Black Belt professional.

View all posts by Brett Beranek