What's next

Authentication & Fraud Prevention, Customer Engagement, Enterprise

Enhancing the Telco Customer Experience and Preventing Fraud with Biometrics

Improve security and customer experience with biometrics. Explore how biometrics empower telecom organizations to strengthen fraud prevention while improving customer care.

Simon Marchand, CFE, C.Adm.
Posted March 23, 2021

Each year, there are 1.62 billion customer interactions with telecom companies — a number

that iGR, a market research consultancy, predicts will increase to 1.765 billion within the next two years.

Unfortunately, prevalent fraud in the industry threatens the security of each of these interactions. With every one of these interactions representing real human beings, fraud has the potential to bring physical and psychological harm to millions of customers.

Telecom organizations hoping to protect consumers must verify customer identities without disrupting the experience with their brands. Telcos that are unable to offer a quick yet highly secure authentication process risk losing their customers to competitors.

Using Nuance's biometric authentication and fraud prevention solutions, telcos can improve customer experiences, increase profits, protect their customers and their brands from fraud, and tap into all the benefits of Microsoft Azure and AI services. Microsoft's Azure cloud delivers security advantages to telcos on an innovative and trusted platform that underpins Nuance Gatekeeper.

In a recent white paper, Nuance and Microsoft reveal why telcos must start embracing biometrics in order to maximize fraud prevention and facilitate exceptional, frictionless customer experiences across channels. Explore an overview of the white paper below.

Understanding Fraud in the Telecom Industry

Even as telcos continue to innovate and build their security capabilities, fraudsters are becoming craftier in how they take over existing accounts or create fake ones. These criminals are always searching for a way to outsmart security barriers so they can steal personal information and customer accounts and then place fraudulent orders for devices, phone plans, accessories, and services.

In 2019 alone, the annual Cyber-Telecom Crime Report highlights how telco providers lost $32.7 billion to fraud. The 2020 Association of Certified Fraud Examiners Report to the Nations also indicates that organizations lose 5% of their revenue each year to fraudsters.

If telcos want to prevent fraud and protect their brands, they must take action by implementing stronger customer authentication methods, both online and over the phone. But they also must consider the impact on customer experience.

Consider how you verify a customer's identity at your company today. Do you ask them for personal information, security question answers, or perhaps a customer number? Do you send one-time passcodes to their mobile device or email?

All of these security factors add friction and frustration to the customer's experience — and they're not even very secure. Fraudsters can easily purchase personal information and account credentials online or intercept mobile SMS to hijack one-time passcodes.

When 96% of consumers become more disloyal after high-effort service interactions, telcos can't afford to increase security at the cost of increasing churn. In order to attract, protect, and

retain subscribers in the long run, telcos must find a way to authenticate customers that doesn't compromise on their experience.

Prioritizing Customer Care

For consumers, anything less than an exceptional experience is reason enough to switch telecom providers. iGR reports that around 17% of subscribers who switch mobile operators do so because of a billing or customer service issue. This finding reinforces the fact that in order to increase subscriber retention rates, telco providers must exceed customer expectations during support calls and online interactions.

According to iGR, cellular providers spend $362 earning each new customer in the U.S. — which could be costing organizations up to five times the cost of retaining each customer.. iGR also highlights that telcos spend $1 for every minute they provide support to customers, including time spent on hold over the phone.

By strengthening and streamlining lengthy authentication processes, telcos can improve the experience for customers to reduce subscriber churn and cut down on costs.

Elevate the Customer Experience and Prevent Fraud with Biometrics

Today, the majority of telco providers rely on a combination of a security PIN and questions to verify a customer's identity. However, these strategies are not sufficient to meet customer expectations around convenience and security: PINs, passwords, and security questions are difficult for customers to keep track of, and easy for fraudsters to cheat or circumvent. Authenticating customers based on these factors takes minutes to complete and offers an easy opportunity for fraudsters to exploit, leading to high operational and fraud costs.

Telecommunications companies can swiftly and dramatically increase security and reduce fraud costs simply by applying biometrics to customer authentication processes.

Nuance's biometric security solutions, for example, prevented over 4,000 cases of fraud for a U.S. cellular operator, saving the company between $1 and $6 million annually.

Through biometrics, users are authenticated consistently across channels (web, app, IVR, and call center) based on their voice, their behavior, and even their use of language — a novel new biometric modality known as conversational biometrics.

Not only do biometrics offer telcos the ability to increase their fraud detection and prevent account takeovers, they also improve the customer experience by accelerating verification processes. Biometric authentication takes mere seconds to complete with extremely high accuracy, streamlining and protecting the interaction.

As telecom providers enhance fraud prevention and customer authentication with biometrics, their subscriber relationships improve as well, resulting in less churn and higher profits overall.

Interested in learning more about why biometrics is suitable for your telco brand? Access our complete white paper, "Biometrics in Telecom: Improving Customer Authentication and Fraud Prevention," for more information.

Tags: Biometric Authentication, Customer Experience, Fraud Prevention, Microsoft Azure, Telco

More Information

Improve security and customer experience with biometrics
Explore how biometrics empower telecom organizations to strengthen fraud prevention while improving customer care.
Download

About Simon Marchand, CFE, C.Adm.

Simon Marchand is Nuance's chief fraud prevention officer for security and biometrics. Certified Fraud Examiner, Simon has extensive expertise in fraud prevention, detection and management - as well as in authentication and identity - in both the banking and telecom industries, with more than 10 years of experience in the field. Prior to Nuance, Simon held key fraud prevention positions at Montreal-based Laurentian Bank, at Bell Canada, and at Québec's Order of Chartered Administrators, where he managed its professional inspection program. As chief fraud prevention officer, he works closely with Nuance clients to design biometric-based fraud prevention and authentication strategies that disrupt criminals while reducing effort and friction for legitimate customers. He regularly shares his expertise in various conferences and with associations around the world and he speaks on the risks of fraud and the ethical use of biometrics in the media.

View all posts by Simon Marchand, CFE, C.Adm.