NUANCE

Biometrics for Telecoms

Improving customer authentication and fraud prevention.

In collaboration with Microsoft

Contents

Nuance and Microsoft: a strategic collaboration that prevents fraud and improves customer experiences.

Nuance and Microsoft are streamlining and protecting the customer experience for telco organizations with solutions for frictionless biometric authentication and intelligent fraud prevention.

Gatekeeper, Nuance's biometrics security solution, powered by Microsoft's trusted and intelligent Azure and AI services, helps telcos:

— **Create superior experiences for customers and employees** by making the customer authentication process seamless and secure

— **Prevent fraud and protect your brand** with intelligent, proactive fraud detection

— **Increase profits** by drastically reducing operational and fraud costs

Microsoft's Azure cloud delivers security advantages on an innovative and trusted platform that underpins Nuance Gatekeeper. Together, the solution protects customer experiences by identifying humans behind each interaction, enabling more personalized service while managing and reducing fraud risk.

In this white paper:

☑ Learn about the current customer engagement risk factors facing telecoms today

☑ Discover how biometrics work

☑ And get inspired by the results being achieved by other telco organizations

While today's telecom networks themselves are very secure, fraud in the industry continues to be a challenge. From individuals to organized crime rings, fraudsters are obtaining devices and services by taking over accounts using stolen information, creating new accounts using synthetic identities, and targeting customer service agents with social engineering. Every leak of logins, passwords and personal information results in more and more consumer data being available for fraudsters to exploit.

Executive summary

Consider the results of a 2019 Cyber-Telecom Crime report finding that showed global telecom fraud losses to be $32.7 billion,[1] and reporting in the ACFE Report to the Nations that organizations lose 5 percent of revenue to fraud every year.[2] If someone is able to fraudulently access a subscriber account, whether in a store, online or through a contact center, they will be able to order an extra line on the account, which can then be sold for cash on the street; they can obtain a new phone or other device which is again sold immediately for cash; they can purchase accessories, again charged to the account; or they can use their access to the customer's telco account to gain access to the customer's financial holdings and other accounts.

Carriers are constantly creating new ways for customers to interact with them that require as little friction and effort as possible. Unfortunately, this positively impacts the fraudster watching and waiting for any vulnerabilities in the carrier's customer care infrastructure. These bad actors—whether motivated by money or more nefarious reasons—are constantly retooling and exploiting new techniques, in many cases working in teams to feed off each other and share real-time activities to strike when an opportunity is found.

iGR, a market research consultancy focused on the wireless and mobile industry, has conducted a considerable amount of research over the past few years on how mobile subscribers interact with operators: on average, iGR believes that each subscriber calls customer care once per quarter, across all channels and for the entire population, but not everyone calls each month; on average, those subscribers that do contact customer support do so on average every two months.

And it should come as no surprise that the quality of customer support by a mobile operator is a factor determining the churn rate. In a recent iGR survey, nearly 17 percent of subscribers who had recently switched mobile operators said that a customer service or billing issue was a reason to churn.

17%

of subscribers who had recently switched mobile operators said that a customer service or billing issue was a reason to churn

1.62B

customer interactions need authenticating (and by 2023, iGR forecasts that the total number of interactions will increase to 1.765B)

In 2019, the number of mobile subscriptions in the U.S. was at 404.57 million.[3] If the average subscriber contacts the operator for support four times per year, that is 1.62 billion customer care interactions. That means that is 1.62 billion interactions need authenticating. And by 2023, iGR forecasts that the total number of interactions will increase to 1.765 billion.

Every one of these interactions requires some level of authentication—and every authentication is a chance to make or break the customer's experience. What's more, every one of these interactions is potentially a fraudster trying to compromise a customer account. Telcos therefore need to find a way to protect their subscribers without adding undue friction and frustration to their experiences.

As this paper will show, telcos of all stripes around the world are turning to biometrics for seamless authentication that enhances the customer experience and intelligent fraud prevention that protects their interactions.

Today's telcos face four fundamental problems that challenge their core business:

1. Protecting their subscribers
2. Reliably authenticating customer identities without adding undue friction
3. Reducing agent costs and handling time
4. Providing a consistent, personalized experience across all channels

Biometrics are being adopted for many reasons – here are three of the most compelling:

- Biometrics **span virtually every engagement channel** that a carrier may offer, from voice (live agents and interactive voice response systems) to digital (web, mobile and messaging apps).
- Biometric authentication is **proven to improve the customer experience** while increasing agent productivity and reducing average handle time.
- At the same time that they improve authentication for legitimate customers, biometrics **simultaneously detect and prevent fraud**.

Current risk issues

Anyone who has contacted their mobile operator for customer care knows the drill: call or log in and then answer a series of questions to confirm your identity. On the web, for example, the standard approach is to require a login and password and then, before any purchase can be made, to confirm the account holder's identity with a follow-up question or two-factor authentication, such as sending an email link or a code via SMS.

Nowadays, LTE networks are very secure and are able to detect unauthorized devices on the network. But it is still possible to fraudulently obtain devices and services through customer care channels by imitating a valid subscriber. Every leak of logins, passwords and personal information exacerbates the problem.

If someone is able to fraudulently access a subscriber account, whether in a store, online, or through a contact center, then they will be able to:

- Order an extra line on the account, which can then be sold for cash on the street; by the time the subscriber and operator have discovered the fraud, the phone or SIM will have been sold.
- Obtain a new phone or other device (charged to the account), which is again sold immediately for cash.
- Obtain accessories, again charged to the account.
- Use access to the telecom account to obtain other information or access to other accounts, such as bank accounts, etc.

Obviously, mobile operators take steps to authenticate the identity of the genuine subscriber. But as more precautions are put in place, the customer interaction becomes more intrusive and disruptive. For example, this whitepaper author's recent customer care interaction with a major mobile carrier required authentication of his identity three times in three different ways. The initial call was authenticated with a knowledge-based authentication (KBA) question before being passed to a different department to resolve the issue. The second interaction required another KBA question. Finally, the call was passed to technical support, which again authenticated the account, this time using a PIN. But also note that in many cases, the fraudsters have accurate personal information on the subscriber, while the actual account holder may forget a PIN or password.

The problem with current authentication methods is that they can become a pain point for the actual subscriber. Remembering a range of KBA questions, PINs and other data becomes challenging and can strain the interaction with the mobile operator. This increases the friction between customers and the operator and increases the level of effort required on the part of the subscriber. Many consumers resort to writing the answers down or using simple, easy-to-remember questions and answers. This, of course, makes the fraudster's work easier.

In summary, telcos need to solve two core challenges: how to easily authenticate the customer as they access customer care, with as little friction as possible; and how to prevent fraud across all customer support channels.

Telcos need to solve two core challenges:

1. How to easily authenticate the customer as they access customer care, with as little friction as possible
2. How to prevent fraud across all customer support channels

Determining the size of the problem

According to the 2019 Cyber-Telecom Crime Report, global fraud losses were estimated to be $32.7 billion. Obviously, if a potential weakness is publicized by mobile operators, the fraudsters are more likely to try to exploit that weakness.

Determining the potential size of the problem therefore comes down to understanding the size of the customer support operation in the telecom industry. iGR has conducted a considerable amount of research over the past few years on how mobile subscribers interact with operators:

— On average, iGR believes that each subscriber calls customer care once per quarter.

— Not everyone calls each month; typically, consumers will have multiple interactions in order to resolve an issue.

— According to iGR's research, 35 percent of subscribers have not contacted customer care/support in the last year and 15 percent have contacted support just once.

— Those subscribers that do contact customer support do so on average every two months.

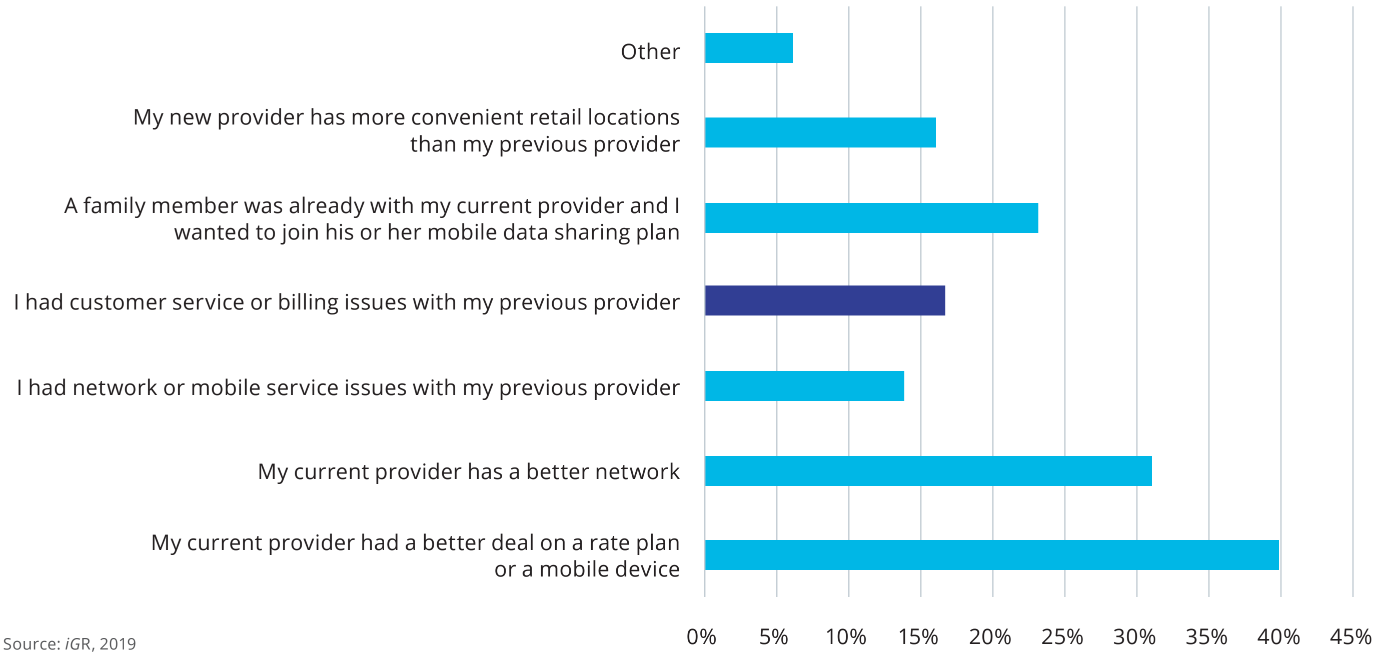
$32.7B

Global telecom fraud losses in 2019[4]

Why customer care is important

It should come as no surprise that the quality of customer support by a mobile operator is a factor determining the churn rate, as figure 1 shows, nearly 17 percent of subscribers who had recently switched mobile operators said that a customer service or billing issue was a reason to churn.

Figure 1: Reasons for Switching Mobile Service Providers



Source: *iGR*, 2019

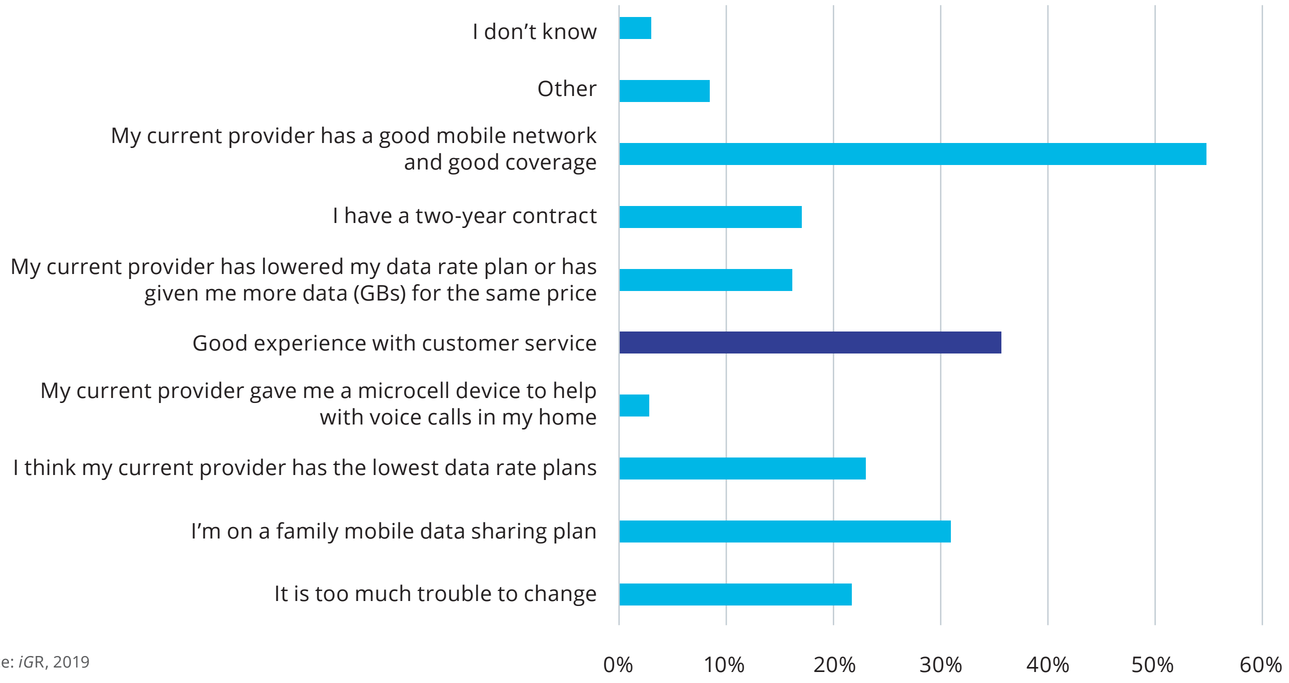
The quality of customer service is also a reason not to churn; i.e., to stay with the current mobile provider. Figure 2 shows the reasons subscribers say they chose to stay with their current mobile provider. In this case, "good customer care" is the second most popular reason, after network quality.

Thus, the quality of customer support a mobile operator provides is critical to maintaining the subscriber base and avoiding churn. And note that churn is expensive for the mobile operator: iGR's recent research has shown that the average acquisition cost for a mobile subscriber in the U.S. is $362. It is therefore **far cheaper to retain an existing customer** than to replace a lost customer.

If a customer service interaction is to be successful, authentication needs to be as seamless and painless as possible. Lengthy authentication processes add friction and frustration to the subscriber experience that could lead them to churn.

What's more, customers expect that they won't need to reauthenticate when they switch channels—but that expectation is not being met. According to Gladly, while 71%[5] of consumers say they want a consistent experience across channels, only 29% say that they actually get it. In addition, a Microsoft report found that 72%[6] of consumers expect service agents to already know who they are, what they've purchased, and when they've engaged previously.

Figure 2: Reasons for Staying with Current Mobile Service Provider



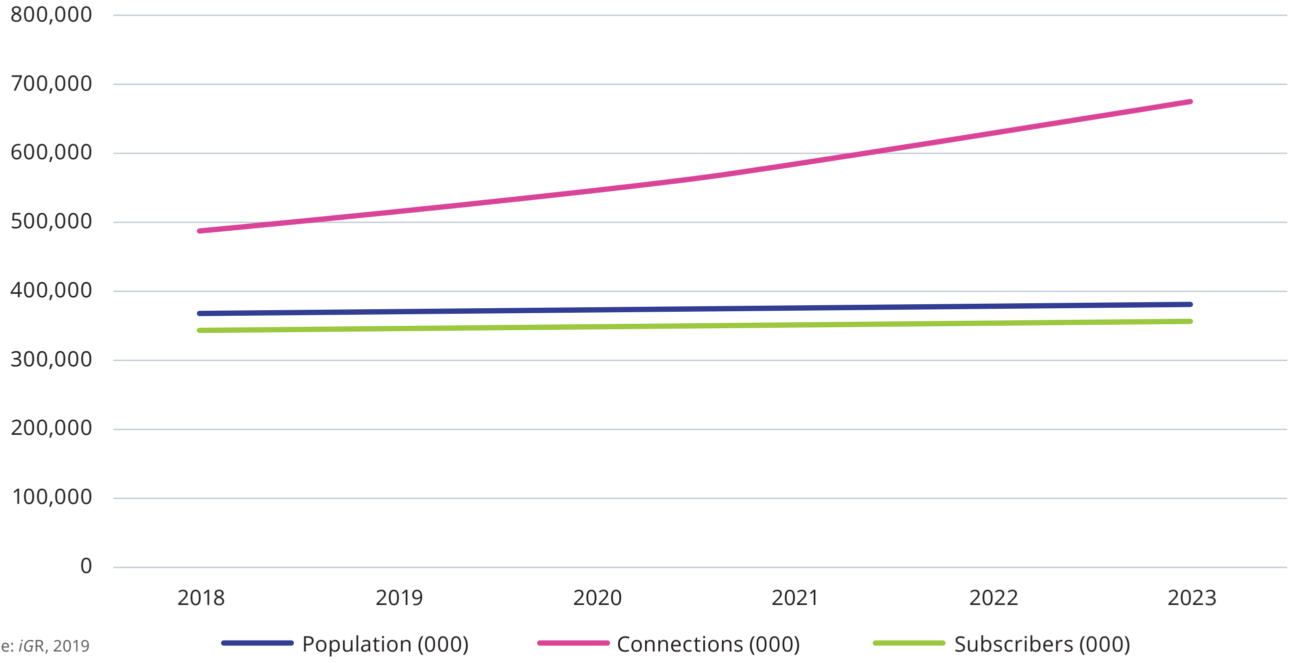
Source: *iGR*, 2019

The need for seamless, secure authentication is growing more and more urgent as consumer behavior shifts to mobile-first. As figure 3 shows, while the number of mobile subscribers is growing very slowly (because most people already have at least one mobile device), the number of mobile connections being made is rising rapidly due to the increasing use of tablets, smart TVs and thermostats, and other connected devices. Every one of these interactions requires some level of authentication—and every authentication is a chance to make or break the subscriber experience.

Mobile operators are also challenged to reduce operating costs, including customer support expenses. According to iGR's estimates, it costs approximately $1 per minute for a telco to provide customer care across all channels. (This includes the amount of time a customer is "on hold"). Thus, the longer the customer care interaction, including the amount of time to authenticate the subscriber, the more expensive the call. And, as the volume of customer support interactions increases, the cost per interaction needs to be reduced as much as possible.

Furthermore, the lines are becoming blurred between the traditional mobile carrier and the cable Multiple System Operator (MSO), as both offer mobile, internet and TV programming services. The need for a positive customer care experience is more vital than ever as the dollar value of a single subscriber across all channels has increased significantly.

Figure 3: North America Population, Mobile Connections and Mobile Subscribers, 2018 – 2023 (000s)



Source: *iGR*, 2019

To put this in perspective, consider the basic math:

- Consider that at the end of 2019, there were just under 404.57 million cellular subscriptions in the U.S. with 488 million mobile connections. If the average subscriber contacts the operator for support four times per year, that is 1.36 billion customer care interactions. That means that 1.36 billion interactions need authenticating.
- By 2023, iGR forecasts that there will be 353 million subscribers but nearly 673 million connections. If each subscriber contacts their mobile operator five times per year (increased due to the greater number of devices), then the total number of interactions is 1.765 billion. This is likely conservative given the significant increase in the number of connections.

Communication service providers need a way to improve customer experiences without compromising on security; indeed, they need to actively increase security to protect their customers without adding undue friction and frustration. This is where biometric authentication and fraud prevention solutions come in.

How biometrics work

Biometrics are the new standard for customer authentication and fraud prevention in telecommunications, financial services, government, and other industries. Consumers regularly interact with biometrics systems either actively or passively:

- **Device-based solutions using facial or fingerprint biometrics to access a mobile device.** These factors are popular for opening user sessions and logging into mobile apps, but don't provide sufficient security for higher-risk interactions and are limited to the users' device, making them inapplicable in a contact center.
- **Voice biometrics in interactive voice response (IVR) systems and with live customer support agents.** Voice biometrics solutions authenticate legitimate customers and identify fraudsters by comparing input voice audio to a collection of stored voice samples ("voiceprints") that are known to be authentic or fraudulent. Voice authentication can be completed during the first few seconds of a subscriber's natural interaction with a live agent or speech-enabled IVR. Voice biometrics are also increasingly being deployed in web and mobile apps as a faster, more secure form of 2-factor or step-up authentication.
- **Behavioral biometrics systems that work in the background of a digital user session** to authenticate and detect fraud based on how a person interacts with their device, including how fast they type, how long they press keys, what pauses they take, how they use a mouse or make swiping motions, and other factors. Behavioral biometrics are an ideal factor for continuous authentication and fraud monitoring in mobile and web applications.
- **Conversational biometrics in messaging apps and live agent environments** that analyze typed and transcribed text to authenticate and detect fraud based on word choice, grammar and sentence structure, emoji and acronym usage, and other elements. In this way, conversational biometrics add an additional authentication layer that detects additional forms of fraud such as mules hired to read from scripts.

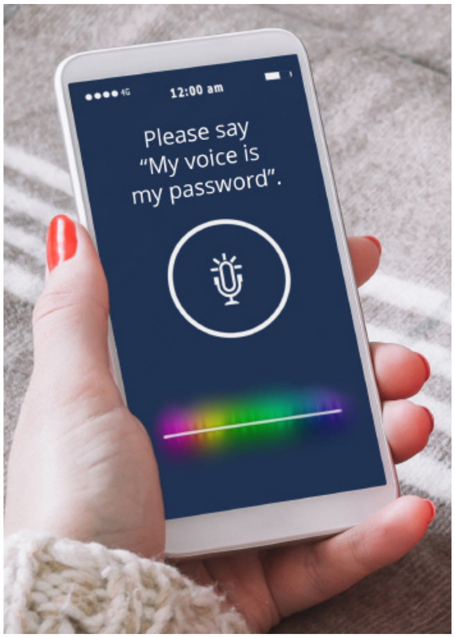
CASE STUDY

Large U.S. Telco
A large U.S. telecommunications provider came to Nuance for help with protecting its customers and business from fraud in its telesales channels.

Since deploying a Nuance fraud prevention solution, the telco operator has prevented over 4,000 confirmed fraud attempts in under three years. Operational costs are low and the benefits were rapid, resulting in a major ROI.

~$7M

transactional losses averted with biometric fraud prevention



The evolution of biometrics in telecommunications

Today's telcos face four fundamental problems when it comes to customer authentication:

1. Reliably verifying each customer's identity without undue friction and without compromising on security
2. Protecting their subscribers from account takeover, SIM swap, identity theft, and other forms of fraud
3. Reducing operational costs and increasing agent efficiency
4. Providing a consistent, personalized experience across channels

Traditional ways of authenticating customers undermine a telco's efforts to meet these challenges. PINs, passwords and security questions rely on customer memory and add major friction and frustration to their experience. Agents are put in the position of interrogating customers instead of helping them, and every poor service interaction can lead to customer churn. What's more, these factors are extremely vulnerable to fraudsters who can easily obtain customer information by buying it on the dark web or socially engineering a contact center agent.

In order to reduce friction in this process, telcos began adopting biometrics for authentication. The first biometric factors to be deployed by telcos were fingerprinting and facial recognition. Once consumers grew accustomed to them through their embedding in mobile devices from Apple, Samsung, and other manufacturers, these factors took off in popularity. Face ID and fingerprint readers quickly became the standard for logging in to mobile devices and apps, and for authenticating small, low-risk transactions.

However, as discussed earlier in this paper, these factors have inherent drawbacks that limit their applicability. And so, telcos are turning to other biometric modalities to authenticate and prevent fraud, including voice, behavioral, and conversational biometrics.

Today, telcos can leverage AI-based solutions that layer these next-gen biometric modalities with environment detectors and anti-spoofing tools to quickly and reliably authenticate legitimate customers and stop fraudsters in their tracks. The best of these solutions can integrate into both digital and voice channels to streamline and protect every customer interaction, no matter where or how they engage.

Biometrics work best in concert with other authentication and fraud detection technologies, including environment detectors and anti-spoofing tools such as:

— Device printing to determine whether the device being used matches a device type previously used by the same caller or digital user

— Network identification to assess the risk of a call based on packet loss

CASE STUDY

Deutsche Telekom
Deutsche Telekom is one of the largest telecom operators in the world, with 168 million mobile subscribers, 28 million fixed network connections and 19 million broadband lines, in multiple countries.

The company was challenged with offering customers a secure but convenient way to access their accounts. Their solution was to deploy Nuance's voice authentication, eliminating the need for subscribers to remember their 10-digit customer number.

The result is fast, seamless authentication that frees agents to focus on addressing customer needs and providing additional services. More than 200,000 customers enrolled their voiceprint in the first five months.

75%

of customers say that voice authentication is more convenient

- Identifying the country and region or city that a call or user session is associated with to detect suspicious location changes
- Call validation to detect spoofed ANIs and suspicious call paths
- Synthetic speech and playback detection to foil attackers who are imitating or parodying legitimate users

Modern authentication and fraud prevention solutions, such as those provided by Nuance, layer all of these elements together in a centralized AI risk engine. This layered, multi-factor approach creates a high-fidelity view of the human behind the device or on the other end of the phone. This in turn leads to higher authentication success rates and increased detection of fraud, and enables detailed personalization by identifying the actual customer involved in every interaction.

Research by Financial Fraud Action UK has shown that voice biometrics can help reduce the cost of fraud in a customer contact center by 90 percent and in the mobile channel by 80 percent. And a major, tier-one U.S. mobile operator has successfully disrupted organized fraud rings using a Nuance solution, preventing more than 4,000 confirmed fraud attempts and saving an average of $2,000 per case, resulting in annual fraud loss mitigation of $1-3 million.

90% reduction in the cost of fraud in a customer contact center through voice biometrics

As well as reducing the potential risk of fraud and account takeover, biometrics can also reduce the risk of churn. 82 percent of consumers have quit a company because of bad customer service, according to Zendesk, and as discussed earlier, customer service issues are a major driver that lead subscribers to switch mobile operators. Biometrics help telcos reduce churn and increase customer lifecycle value by reducing friction in customer support interactions and empowering agents to deliver efficient, personalized service.[7]

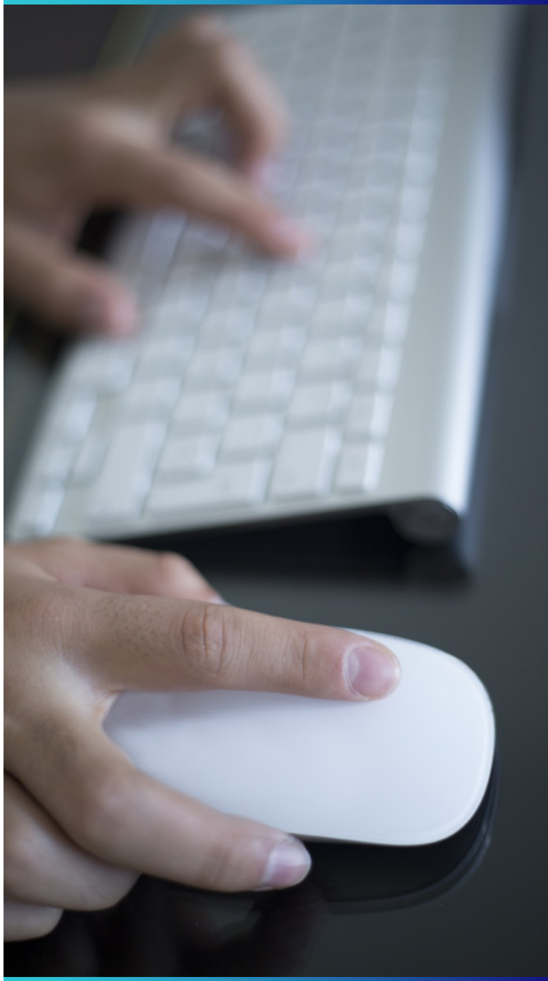
94% of agents at one Nuance customer report that voice authentication makes it easier to deliver quality service

LEARN MORE

□ Learn how Nuance Gatekeeper delivers seamless, secure biometric authentication with intelligent, proactive fraud prevention.

□ Discover why 19 of the top 20 global carriers choose Nuance.

□ Review how a major telco provider disrupts organized fraud with Nuance.



Reducing client/agent effort and friction along with fraud is a win-win for the mobile carrier, the MSO, and consumers.

FOOTNOTES:

[1] Cyber-Telecom Crime Report 2019

[2] 2020 ACFE Report to the Nations

[3] https://www.statista.com/statistics/186122/number-of-mobile-cellular-subscriptions-in-the-united-states-since-2000/

[4] Cyber-Telecom Crime Report 2019

[5] While 71% of consumers want a consistent experience across all channels, only 29% say they actually get it. (Gladly, 2019 Customer Expectations report)

[6] 72% of consumers expect agents to already know who they are, what they've purchased and have insight into their previous engagements (2017 State of Global Customer Service Report, Microsoft)

[7] https://www.zendesk.com/resources/why-companies-should-invest-in-the-customer-experience/