Biometrics in Telecom:
Improving Customer Authentication and Fraud Prevention
CONTENTS

3 Executive summary
5 Current risk issues
7 Determining the size of the problem
8 Why customer care is important
11 How biometrics works today
12 The evolution of biometrics in telecom
EXECUTIVE SUMMARY

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.

Consider the results of a 2017 CFCA (Communications Fraud Control Association) survey that showed global telecom fraud losses to be $29.2 billion, or 1.27 percent of annual telecom revenues. 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; obtain a new phone or other device which is again sold immediately for cash; obtain accessories, again charged to the account; or use access to the telecom account to obtain other information or access to other accounts, such as bank accounts, etc.

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.
If the customer service interaction is to be successful, identity authentication needs to be as seamless and painless as possible. If the customer is repeatedly challenged for their identity throughout the interaction, the risk of having an unsatisfying experience increases. And, as people use more devices, the number of customer service interactions increases, presenting more chances to either make a good impression or fall flat.

To put this in perspective, consider that at the end of 2018, there were just under 340 million cellular subscriptions in the U.S. with 488 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. And by 2023, iGR forecasts that the total number of interactions will increase to 1.765 billion.

Today’s telcos face four fundamental problems when it comes to customer authentication and fraud prevention:

1. Protecting their subscribers.
2. Reliably confirming a customer’s identity without undue intrusion, making the interaction as frictionless as possible.
3. Reducing agent costs and handling time.
4. Providing a consistent, effective experience across all channels.

Biometrics is being adopted for many reasons; three of the most compelling are:

- Biometrics spans virtually every engagement channel that a carrier may offer, from voice (live agents and interactive voice response systems) to digital (web, mobile, apps).
- Biometric authentication is proven to improve the customer experience (including reducing customer effort) while increasing agent productivity/reducing average handle time.
- At the same time that it improves authentication for legitimate customers, biometrics is simultaneously detecting and preventing fraud.

As larger subscriber bases and more devices per subscriber result in more customer interactions, biometrics is a win-win for customers and carriers.
CURRENT RISK ISSUES

Anyone who has called or contacted their mobile operator for customer care knows the drill: call or log in and then be prepared to answer a series of questions to confirm your identity. On the web, the standard approach for customer care systems 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, it is very hard to fraudulently clone a SIM card or obtain free cellular service via any other such method; 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.

As an indication of the size of the problem, consider the results of a 2017 CFCA (Communications Fraud Control Association) survey that showed global telecom fraud losses to be $29.2 billion, or 1.27 percent of annual telecom revenues. While the survey showed fraud losses had fallen by 0.42 percent from 2015, telecom fraud departments had increased by four percent and were spending 14 percent more time on customer care, billing and revenue assurance functions. In addition, 10 percent more cases were reported to law enforcement in 2017 than in 2015.

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 correctly authenticate the identity of the genuine subscriber. But as more steps and precautions are in put in place, the customer care 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, two clear problems need to be addressed: 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.

Two clear problems need to be addressed: 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.
DETERMINING THE SIZE OF THE PROBLEM

According to CFCA’s 2017 survey, global telecom fraud was $29.2 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, across all channels and for the entire population.
- But 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.
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 the following chart shows, the principal drivers of churn relate to price and network quality. 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

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>My new provider has more convenient retail locations than my previous provider</td>
<td>20%</td>
</tr>
<tr>
<td>A family member was already with my current provider and I wanted to join his or her mobile data sharing plan</td>
<td>30%</td>
</tr>
<tr>
<td>I had customer service or billing issues with my previous provider</td>
<td>25%</td>
</tr>
<tr>
<td>I had network or mobile service issues with my previous provider</td>
<td>20%</td>
</tr>
<tr>
<td>My current provider has a better network</td>
<td>15%</td>
</tr>
<tr>
<td>My current provider had a better deal on a rate plan or a mobile device</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: iGR, 2019

The quality of customer service is also a reason not to churn; i.e., to stay with the current mobile provider. The following chart 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 keep an existing customer than to replace a lost customer.

If the customer service interaction is to be successful, customer identity authentication needs to be as seamless and painless as possible. If the customer is repeatedly challenged for their identity throughout the interaction, the risk of having an unsatisfying customer support experience increases. This goes hand-in-hand with the premise of omni-channel communications: To many customers, the term “omni-
channel means that the reason they’re calling or emailing is carried from one communications channel to another. If that context is lost as they move between channels and they’re repeatedly asked to authenticate themselves, customer effort increases quickly: Authenticate customers once reduces that effort and also the lost customer service agent productivity.

**Figure 2: Reasons for Staying with Current Mobile Service Provider**

![Chart showing reasons for staying with current mobile service provider](chart.png)

Source: iGR, 2019

Of course, as more people use more mobile devices, the number of customer service interactions increases and there are simply more chances to either make a good impression or fall flat. As the following chart shows, while the number of subscribers is growing very slowly (because most people already have a mobile device), the number of connections is increasing due to the use of tablets, IoT devices, connected vehicles, etc. Mobile operators are also challenged with minimizing operating expenses, which includes customer support costs; 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.

To put this in perspective, consider the basic math:

- Consider that at the end of 2018, there were just under 340 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.

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

Source: iGR, 2019
HOW BIOMETRICS WORKS TODAY

Biometrics, once the domain of early adopters, has since become common for customer authentication and fraud prevention in telecom, financial services, government, and other industries. The most common solutions that consumers interact with are:

- Device-based solutions using facial or fingerprint biometrics to access a mobile device. Device-based authentication is not used to confirm identity when using a network or interacting with customer support; they are limited to providing access to the device or a specific application.
- Voice biometrics in interactive voice response (IVR) systems and with live customer support agents. Voice biometric solutions rely on having a valid voice print on file; authentication and fraud prevention rely on matching the caller to the voice print on file. Note that this voice print can be obtained actively (by asking the subscriber to say something) or passively, where the subscriber is authenticated during normal conversation with the care agent.

CASE STUDY: LARGE U.S. TELCO

A large U.S. telecommunications provider was faced with the challenge of protecting its customers and business from telephone fraud in the customer support channels. The solution was to use Nuance Security & Biometrics. Since deploying the solution, the telecommunications operator has prevented over 4,000 confirmed fraud attempts in under three years, contributing to savings of up to $7 million in transactional losses alone. Operational costs are low and the benefits were rapid, resulting in a major ROI.
Today’s telcos face four fundamental problems when it comes to authenticating customers in their support channels and reducing fraud:

5. Protecting their subscribers from fraud and identity theft.
6. Reliably confirming a customer’s identity without undue intrusion, making the interaction as frictionless as possible.
7. Reducing agent costs and handling time.
8. Providing a consistent, effective experience across all channels.

These challenges put a considerable strain on the traditional PIN/challenge question combination used by the majority of telcos today. Customer interactions can become frustrating if the subscriber forgets a PIN, for example, and a poor customer service interaction can lead to increased churn. Furthermore, as this paper has discussed, consumer personal information is widely available, potentially allowing fraudulent access to a customer account.

Today’s solutions, such as Nuance Security and Biometrics, include biometric and nonbiometric factors that span voice and digital engagement channels. This coverage is important because telcos need to secure every channel: Subscribers insist on choice, while fraudsters will find and target any weak links. Factors that carriers should consider are:

- Voice biometrics: Because voice is an important way that consumers engage with telcos, voice biometrics reduces the time and effort required to authenticate legitimate customers in IVR systems and with live contact center agents. It also serves the dual purpose of detecting and blocking fraudsters using stolen credentials.

- One of the newest innovations is the ability to compare sentence structure and grammar to a profile rather than simply how a voice sounds. In essence, confirmation is obtained by analyzing what a consumer says and how they say it, rather than how they sound. This can be applied to both voice and digital interactions.
• Behavioral biometrics looks at how a person types, uses a mouse, or even how they pause when accomplishing a task. This creates a profile of the user that can be compared to an expected profile. It excels at continuous authentication where a user is constantly compared to their profile to ensure that someone else has not hijacked the session. Behavioral biometrics is ideal for mobile and website applications.

• Facial recognition allows subscribers to take a picture of themselves in real time that can be compared to a face on file. Applications like Nuance Security and Biometrics achieve high levels of confidence by overcoming facial variances, and liveness detection allows it to detect if the customer is using a photograph.

• These biometric indicators complement other techniques, including:
  o Determining the device type used during the interaction.
  o Analyzing network quality to detect changes.
  o Identifying the country and city the device is associated with.
  o Looking at the call metadata to determine when a call is from a legitimate customer.
  o Detecting when a fraudster is using a recording of the legitimate customer’s voice in addition to when they’re using synthetic speech.
Solutions should scale to address the needs of telcos of different sizes, from regional providers to tier one mobile operators. Simply, larger subscriber bases and more devices per subscriber result in more customer interactions.

The goal is obviously to reduce subscription fraud and account takeover in the telco customer support channels, and thus improve the bottom line. Determining how much is saved by preventing fraud is difficult, but it is clear that improvement is needed over the current PIN/challenge question methodology and that biometrics are an effective answer.

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 found that Nuance’s biometric solution saved approximately $2,000 with every prevented fraud attempt, that more than 4,000 confirmed fraud attempts were prevented and that the resulting annual savings were $1 million to $3 million.

As well as reducing the potential risk of fraud and account takeover, biometrics can also reduce the risk of churn. As discussed earlier, the effectiveness of customer support is a major driver of telco churn. By easing the customer interaction and improving the relationship between agent and customer, by not being continually asked to verify identity, churn can potentially be improved.

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

Nuance is a global provider of advanced biometrics solutions, enabling integrated fraud prevention and authentication across digital and voice channels. With over 500 million voice prints worldwide, the company’s award-winning AI Deep Neural Network biometrics is used by telcos of all sizes to provide better, more secure customer experiences and improve organizational efficiency / productivity.

Opus Research’s 2019 Intelligence Authentication and Voice Biometrics Intelliview Report cites Nuance as the “undisputed market share leader” and notes its “multi-faceted, layered security approach that includes biometrics, non-biometric prints, anti-spoofing measures, intelligent detectors, pattern detection and employing AI techniques.” Nuance led all 13 vendors considered based on its ability to streamline omnichannel customer authentication and stop fraudsters through all points of access.

Learn more at nuance.com/fraud.

ABOUT iGR

iGR is a market strategy consultancy focused on the wireless and mobile communications industry. At iGR, which was founded by Iain Gillott, one of the wireless industry’s leading analysts, we research and analyze the impact new wireless and mobile technologies will have on the industry, on vendors’ competitive positioning, and on our clients’ strategic business plans.

A more complete profile of the company can be found at http://www.iGR-inc.com/.

Disclaimer

The opinions expressed in this white paper are those of iGR and do not reflect the opinions of the companies or organizations referenced in this paper. All research was conducted exclusively and independently by iGR.