NUANCE

Two-factor authentication is broken. Let's fix it.

SMS one-time passcodes are putting your customers at risk—biometric authentication is the answer.

eBook
Nuance Gatekeeper

SMS is not a security tool

Many organisations rely on two-factor authentication (2FA) using one-time passcodes (OTPs) sent by Short Message Service (SMS) to authenticate banking and ecommerce transactions. 2FA performed this way can be fast and easy, but SMS wasn't designed to be a security tool. Sending SMS OTPs assumes that the person receiving the message is the account owner—but that's not always the case.

Fraudsters exploit the vulnerabilities of SMS in numerous ways; it's very easy for fraudsters to buy customers' personal information on the dark web and then arrange account takeovers to intercept SMS OTP messages. Fraudsters are also using targeted malware bots to gain access to customers' devices, steal their information, and intercept OTPs and authenticator codes.

Fraud schemes like these that exploit SMS 2FA—including SIM swap and port-out scams where fraudsters impersonate customers to divert messages to a phone number that they control—are hitting the headlines, and government regulators are taking notice. In the United Kingdom, the government is putting pressure on telecommunications providers to work closely with the banking sector to prevent SIM swap attacks and limit their effects.

But the vulnerability of SMS isn't just a problem for telcos. It's a problem for any brand that uses SMS 2FA.

1 Source: https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version

Act now to build trust

Customers expect you to protect them, and the brands that offer the highest levels of protection will build the highest levels of customer trust and loyalty.

But fraudsters move fast, as we've seen with the rapid rise of banking trojans—malware bots that infect a victim's device and grant access to all their personal information, credit cards, and mobile banking apps. The rapid growth of FluBot, TeaBot, and most recently SharkBot, shows that criminals have latched on to another way to exploit SMS OTP vulnerabilities.

Companies need to move quickly to update their security measures to address these threats and rebuild trust with their customers. But first, it's critical to understand how SMS-based 2FA gets exploited by fraudsters and why possession-based authentication itself can be dangerous.

Phones and SMS authentication are unreliable and not secure

12% of consumers had their mobile phone or service compromised recently

19% of SMS-based account recoveries fail[2]

37% of total successful fraud attempts involved possible disclosure of OTPs[3]

2 Source: joint study by Stanford & Google researchers, from 2015 but still relevant

3 Source: HSBC UK news release, 15 September 2021: https://www.about.hsbc.co.uk/news-and-media/hsbc-uk-issues-customer-warning-as-one-time-passcode-fraud-increases

The many faces of SMS 2FA fraud

Over the last few years, it's become increasingly clear that SMS OTPs are a major fraud risk. HSBC, one of the largest banks in the UK, recently warned its customers that fraudsters are tricking people into disclosing OTPs over the phone. The bank said it had reported over 3,000 cases of successful OTP fraud in the previous six months.

But phishing for passcodes is just one of many methods through which fraudsters take advantage of the vulnerabilities inherent to SMS. Other common fraud schemes include:

— **SIM swap:** A fraudster impersonates a customer and requests that the customer's phone number be ported to a new device that the fraudster controls, so that all calls and messages are rerouted to them.

— **Port-out fraud:** A fraudster opens an account with a different provider using a customer's stolen info and has the victim's phone number transferred to a device with the new provider.

— **Call transfer:** A fraudster impersonates a customer, claims their legitimate device is lost or broken, and asks for all calls and messages to be diverted to a different number.

— **Whaling:** A fraudster impersonates a fraud team representative and asks their victim to confirm a fraudulent transaction. The fraudster tells the victim that a security code will be sent by SMS to complete the procedure, then launches a password reset, triggering an SMS OTP which the victim reads out to the fraudster.

— **Malware:** A fraudster uses phishing or social engineering to convince a victim to download malware, such as FluBot, TeaBot, or SharkBot, onto their device. This malware gives the fraudster access to the victim's credit card details and personal information, and the ability to intercept their SMS messages.

The rising tide of fraud

66% of UK adults have been targeted by a fraudster in the past year[4]

56% of of UK businesses reported they've experienced fraud in the last 24 months[5]

£190B billion lost to identity, credit card, and cyber-fraud per year in the UK[6]

4 Source: https://www.citizensadvice.org.uk/about-us/about-us1/media/press-releases/36-million-brits-targeted-by-a-scammer-so-far-this-year/
5 Source: https://www.pwc.co.uk/services/forensic-services/insights/global-economic-crime-survey-2020.html
6 Source : https://www.bbc.co.uk/news/business-55769991

The devastating impact of fraud on real people
One Friday night in 2016, tech investor Rob Ross lost ~$1 million in one hour to SIM swap fraud, changing his family's life forever. Discover how a smart, tech-savvy person became a fraud victim—and why he's fighting for voice biometrics to be the default option for 2FA.

Hear Rob's story

It's time to "step up" to biometrics-based 2FA

Verifying customer identities based on an OTP sent to a device they possess is inherently unreliable and not secure. Instead, more and more companies are "stepping up" to authenticate people based on who they are with biometrics.

Biometrics authenticate people based on something inherent to them as a unique human being. Using biometrics as a second authentication factor creates a faster, more secure, and more convenient experience than knowledge-based authentication (KBA, like with passwords or security questions) or possession-based authentication (like with SMS OTPs). But not all biometric modalities are equally convenient or secure.

Facial recognition and fingerprint authentication are popular with consumers, but they have critical limitations: They tie customers to a specific device, they have to be re-enrolled every time a customer changes their device (or has it stolen), and fraudsters can often spoof or circumvent them.

Voice biometrics, on the other hand, are ideal for step-up and second-factor authentication, even in digital channels. These systems authenticate legitimate customers and detect fraudsters based on a person's unique "voiceprint", eliminating dependence on KBA and allowing customers to authenticate effortlessly and securely no matter the device or channel they use.

Many brands also use behavioural biometrics to continuously authenticate customers and detect fraud in digital channels. These solutions work passively in the background to analyse how people interact with their device and quickly spot abnormal or fraudulent behaviour.

Choosing your biometrics solution

Regardless of the biometrics modalities you use, it's worth remembering that not every solution provider will deliver everything you need. When you're considering your options for biometric authentication, be sure to ask potential technology partners these important questions:

- How do you approach consent and compliance for collecting, storing, and processing biometric data?
- Can you provide examples of customers you've helped, and put us in touch with reference customers?
- How often do you release new algorithms?
- What experience do you have with deepfakes?
- Do you offer multiple biometric modalities to authenticate customers across voice and digital channels?
- How easy is it to integrate your solutions with our existing customer engagement infrastructure?
- Do you offer flexible deployment options, including edge deployments?

"Fraudsters always look for the weakest link in the security chain, and often that's SMS 2FA. Voice biometrics solutions pull the rug from under the fraudsters' feet, eliminating the vulnerabilities in knowledge-based authentication that they rely on to commit their crimes."

— Simon Marchand, CFE, Chief Fraud Prevention Officer, Nuance

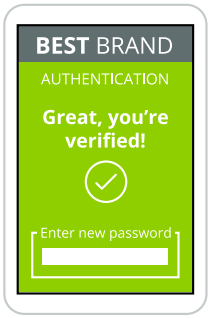
A layered approach to security

1

When a customer needs to perform a high-risk action like resetting a password or swapping or porting a phone number, prompt them to authenticate with their voice rather than receiving a one-time passcode.

2

An AI risk engine analyses the biometric characteristics of their voice while interrogating their device, behaviour, and other factors for signs of fraud.



3

Within seconds, the system authenticates the customer and gives the green light or flags a suspected or known fraudster for escalation to the fraud team.

For an authentication and fraud prevention solution to be effective, it should take a layered, holistic approach. No single factor can solve every authentication and fraud problem in every channel, and many solutions are limited to specific channels, only addressing certain points in the customer's journey. Today's most advanced solutions combine voice, behavioural, and conversational biometrics with various non-biometric factors such as call validation and environment detection into a central AI risk engine.

With a unified solution that deploys across channels, organisations can streamline and protect every customer and employee interaction—whenever, wherever, and however they engage.

The real-world impact of biometrics-based 2FA

90% of fraud detected

99% authentication success rate

92% reduction in fraud losses

* Stats from Nuance customers

Stay one step ahead of the fraudsters

The vulnerabilities of SMS 2FA have been a problem for years, and fraudsters are adept and finding new ways to exploit them. Banking trojans like SharkBot are mainly targeting European banks right now, but as we've seen so often before, successful fraud schemes will soon travel around the world.

So don't wait for your customers to jump ship to your competitors—get ahead of the problem now. Act now, and you can turn a threat into an opportunity to protect your customers and build trust. You'll also stand to gain a significant competitive advantage by improving customer experiences, removing pain points for contact centre agents, and improving NPS.

LEARN MORE
Find out how you can streamline, protect, and personalise every customer interaction, email cxexperts@nuance.com or visit nuance.com/authentication.

Citations

Coronavirus-Related Spear Phishing Attacks See 667% Increase in March 2020. Security Magazine. Retrieved November 17, 2021 from: https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020

Skiba, Katherine. (February 5, 2021). Pandemic Proves to Be Fertile Ground for Identity Thieves. AARP. Retrieved November 17 from: https://www.aarp.org/money/scams-fraud/info-2021/ftc-fraud-report-identity-theft-pandemic.html

GOV.UK (October 26, 2021). Fraud Sector Charter: Telecommunications. Retrieved from: https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version

HSBC UK customer warning: one time passcode fraud increases. HSBC UK. Retrieved November 17 from: https://www.about.hsbc.co.uk/news-and-media/hsbc-uk-issues-customer-warning-as-one-time-passcode-fraud-increases

About Nuance Communications, Inc.
Nuance Communications (Nuance) is a technology pioneer with market leadership in conversational AI and ambient intelligence. A full-service partner trusted by 77 percent of U.S. hospitals and 85 percent of the Fortune 100 companies worldwide, Nuance creates intuitive solutions that amplify people's ability to help others.

ENT_4510_01_EB_UK, Jan 28, 2022