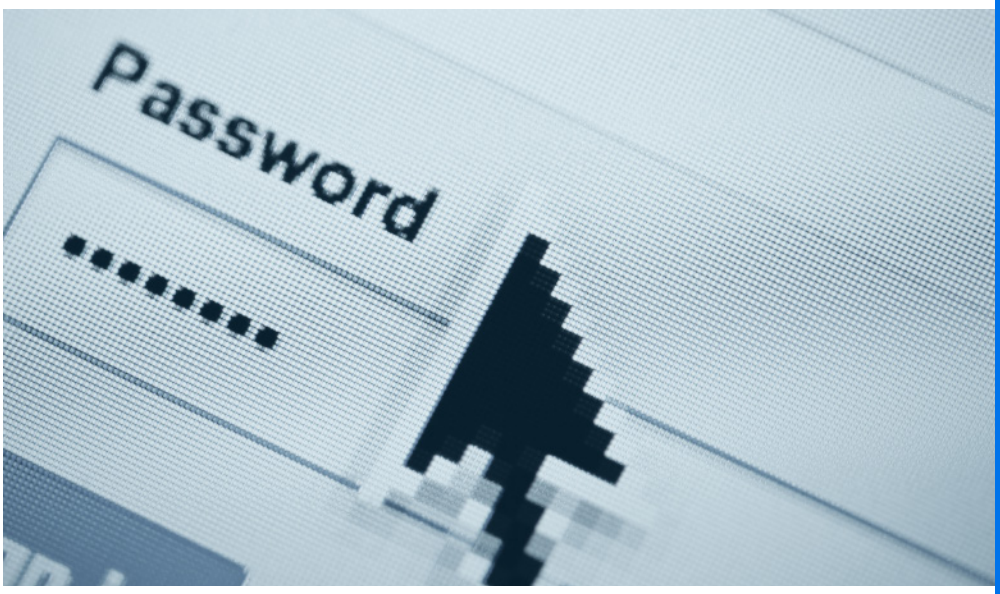
Brochure
Nuance Gatekeeper for Government

Passwords aren't enough to protect your citizens

Why government institutions need biometric security

Contents

There's no such thing as a strong password



For decades, government agencies have relied on PINs, passwords, and other knowledge-based authentication (KBA) credentials to verify customer identities. The trouble is, KBA information is now easy for criminals to steal, buy, or phish to help them carry out fraud attacks.

The disruption of the pandemic gave fraudsters new vulnerabilities to exploit, as worried citizens became more susceptible to phishing, and contact center agents began working from home, without their usual support and oversight.

Plus, many people don't use basic passcode hygiene, making them even more vulnerable to fraud. A 2021 global survey by Nuance and OnePoll revealed that 76% of consumers still don't use different passwords for every website or organization they interact with, and only 18% follow "password strength" indicators and choose the strongest option.

So it's no surprise that one-fifth of respondents had been the victim of fraud in the previous 12 months.

Agency leaders need new security tools*

39%

say citizens are happy with the security of their website

43%

have the security technologies necessary to provide citizens with secure, convenient experiences when accessing online accounts

65%

say AI tools and interconnected devices will improve security and convenience of citizens when accessing online accounts

*Source: TransUnion, Insights for Building Trusted Online Government Services, 2021.

KBA makes life easier for fraudsters—and harder for citizens and agents

KBA creates friction for consumers because people forget or lose passwords. The identification and verification (ID&V) process can become a lengthy interrogation, which increases the frustration of citizens and agents—and ramps up contact center costs. But traditional authentication processes don't bother fraudsters at all, because they always have the information they need.

To help mitigate fraud, most organizations use some form of two-factor authentication to verify customer identities and approve transactions. But these are also vulnerable to attacks that let fraudsters intercept one-time passcodes (OTPs) to execute benefits and claims fraud, account takeovers and other identification theft-driven schemes.

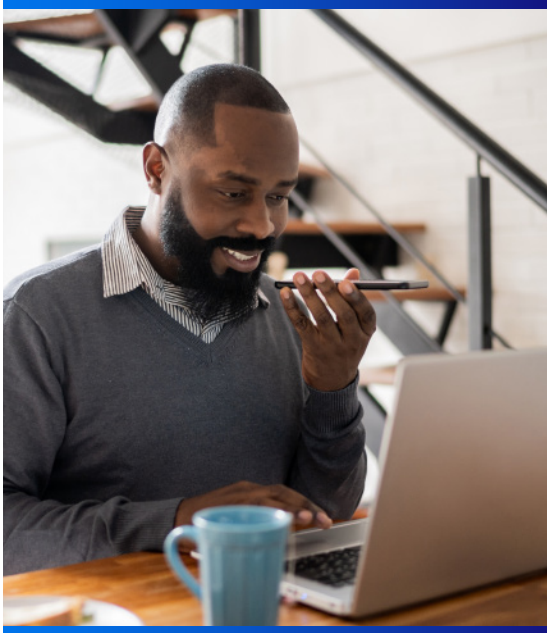
Learn more about why two-factor authentication is failing customers and banks—and find out how to fix it.

Get the Two-factor authentication ebook here.

Prevent fraud, improve experiences, and reduce costs with biometrics
The massive financial impact of fraud on both the government and constituents is obvious—US agencies reported more than $30 billion in confirmed fraud to the Office of Management and Budget in 2021. But the reputational damage of fraud can cause even more long-term harm. And today, every government institution, of every size, is a target for fraudsters. So now, biometric security is the only option.

That's why so many organizations—from government agencies to major retail brands to leading financial institutions—are turning to biometrics to help them improve fraud prevention, reduce fraud losses, avoid reputational damage, and win consumer trust. But they're also using biometric authentication to enhance the customer and agent experience, reduce average handle times, and lower contact center costs.

A major UK bank has used Nuance voice biometrics since 2016, helping it prevent more than $450 million of customers' money from being stolen by fraudsters in 2019 alone.



65%

of agency leaders say AI decision-making tools/technologies and interconnected devices will improve the ability to track citizens' status in order to improve security and convenience when accessing online accounts*

61%

say improvements in identity authentication will improve the state of access governance and, therefore, improve users' experiences*

*Source: TransUnion, Insights for Building Trusted Online Government Services, 2021.

What is biometric authentication?

In traditional ID&V processes, organizations verify consumer identities based on something they know (like a password) or something they have (like an OTP). But as we've seen, this approach is an open invitation to fraudsters.

Biometric security solutions, on the other hand, use powerful AI technologies to identify fraudsters and authenticate genuine citizens based on something that's intrinsic to who they are (like their voice or face). This allows organizations to authenticate the actual person behind every interaction, rather than just verifying their knowledge of a password.

Biometrics modalities like fingerprint scanning and facial recognition are well known, but they're not suited to protecting people from fraud. Aside from concerns about criminals spoofing their fingerprints and faces, and potential racial bias in facial recognition AI, both these techniques rely on consumers having access to a modern smartphone. That's far from ideal for institutions serving a broad range of citizens across different generations and socio-economic groups.

Biometrics modalities for intelligent fraud prevention
To deliver effective fraud prevention and better experiences for all your citizens, it's vital to have a combination of biometrics modalities that can work for anyone, on any channel.

— **Voice biometrics** authenticates callers based on how people sound, analyzing more than 1,000 characteristics in their unique "voiceprint". With the most advanced systems, this is done passively in the first few seconds of a conversation, creating a fast, seamless experience.

— **Behavioral biometrics** authenticates digital users based on how they behave, analyzing how they interact with their device, including how they type, swipe, and click. Importantly, systems like this offer continuous authentication, so they can identify when fraudsters attempt to hijack a legitimate consumer's session.

— **Conversational biometrics** authenticates people across channels, analyzing how they use language, including word choice, grammar, emojis, and acronyms. This adds another layer of protection in omnichannel citizen journeys and helps identify fraud "mules" working from scripts.

Since implementing voice biometrics in its contact center, a major bank has seen a dramatic reduction in telephone fraud attempts:

2019 around 17,000 fraud calls identified

2020 12,000 fraud calls

2021 7,000 fraud calls

A layered approach to security
To offer the highest levels of security to customers, it's vital to layer these biometric factors on top of other non-biometric factors, like call validation, anti-spoofing, and environment detection. When all these factors are plugged into a central AI risk engine, it's possible to quickly identify high-risk interactions, prevent more fraud, and secure every customer engagement channel.

In contact centers and interactive voice response (IVR) systems, you can detect ANI spoofing, virtualized calls, and other threats before contact. Then you can identify fraudsters in real time in the IVR and on calls with agents, based on their unique biometric characteristics.

On digital channels, a layered approach enables you to prevent account takeovers and new account fraud, and quickly spot remote access trojans, bots, social engineering attempts, and fraud mules.

Biometric authentication also helps you guard against the growing problem of employee fraud by continuously verifying agent identities and detecting fraud signals in their behavior and language.

The business value of biometrics

It might seem like advanced biometrics technologies are only for leading companies and major institutions, but in fact they offer a simple, affordable solution for organizations of any size.

Many public institutions—from health and human services and revenue to labor and motor vehicles—are already taking advantage of biometric authentication. And they're finding it quickly pays for itself by delivering significant business benefits.

Better citizen experiences
Biometrics solutions verify citizen identities in seconds with minimal effort. With no more PINs, passwords, or security questions, customers don't feel like they're being interrogated when they get in touch. Instead, they feel known, welcome, and protected, which increases satisfaction and trust.

The Australian Taxation Office used Nuance security solutions and voice biometrics to enroll more than 5M citizen voiceprints, resulting in the reduction of up to 48 seconds for repeat caller handle times. Sixty percent of citizens now prefer to be authenticated with their voice.

Reduced contact center costs and happier employees
Biometric authentication dramatically reduces handle time, helping keep costs under control even during spikes in contact volumes. Agents can focus on delivering efficient, personalized assistance, rather than grilling callers for information and making on-the-spot judgements about fraud risk.

Stronger fraud prevention and lower fraud losses
Intelligent fraud prevention detects more fraud with higher accuracy, enabling fraud teams to focus their efforts on the cases that matter, rather than wading through false positives. Biometric security stops most fraud before it even happens, and helps investigators monitor shifting fraud tactics and uncover new attack vectors.

In its first year of using Nuance Gatekeeper, NatWest Group screened 17 million calls, raised 23,000 fraud alerts—and achieved over 300% ROI.

Customer-focused institutions value biometrics
Organizations in high-contact industries trust biometrics to help them deliver standout experiences while preventing fraud. For example, 75% of global telcos look to biometrics to address gaps in customer care and mitigate fraud threats.[1]

Customers using Nuance biometric security solutions are achieving:

97-99%
faster fraudster identification

92%
fraud loss reduction

3x
fraud cases handled daily

85%
increase in CSAT

89s
AHT reduction

Nuance Gatekeeper: Fast, frictionless authentication and intelligent fraud prevention

Our award-winning biometric security solution, Nuance Gatekeeper, offers fast, accurate, and seamless authentication for legitimate citizens while detecting fraudsters and preventing more fraud—in every engagement channel.

With Gatekeeper, you can replace slow, frustrating, and vulnerable ID&V processes with frictionless, secure biometric authentication that improves experiences for citizens and employees, reduces costs and fraud losses, and protects your reputation.

Opus Research 2022 Intelligent Authentication and Fraud Prevention Intelliview
Learn why Nuance was named as market leader, with Nuance Gatekeeper accurately authenticating voiceprints faster than any other vendor.

Get the report

Award-winning voice biometrics software solutions
Learn why the GSMA awarded Gatekeeper its Global Mobile (GLOMO) Award for Best Mobile Authentication & Security Solution.

Read the press release

"With Nuance voice biometrics, we get a clearer view of customer and fraudster behavior, so we can keep genuine customers protected and take the fight to the criminals who are targeting their accounts."

— Jason Costain, Head of Fraud Strategy and Relationship Management, NatWest Group

Nuance – experience that speaks for itself:

20+ years
of experience in voice biometrics

500+
enterprise deployments

600M+
biometric prints enrolled

2B+
transactions secured annually

$2B+
fraud savings every year

LEARN MORE

If you'd like to discuss any of the opportunities we've highlighted in this guide, or learn more about how we can help, get in touch with us at cxexperts@nuance.com.

Endnote

1 The Fast Mode. (2022.) How Operators are Putting CX First with Biometrics and Artificial Intelligence. The Fast Mode.

About Nuance Communications, Inc.

Nuance Communications 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. Nuance is a Microsoft company.

ENT_4656_01_B, Sep 8, 2022