NUANCE

The real-world impact of biometrics on fraud prevention

Meet four banking leaders disrupting fraud with Nuance technologies.

eBook
Nuance Gatekeeper

New fraud threats. Outdated security methods.

From the pandemic to the rising cost of living, we're living in disrupted, uncertain times. Customers' behaviours have changed, and new fears have emerged. Many have become more concerned than they've ever been about their personal finances—and rightly so.

The disruptions of the past few years have created opportunities for fraudsters to successfully target individuals and organisations, preying on citizens' confusion and fear, and organisations' weakened security defences. Now, fraudsters have a wide selection of cunning attack methods to choose from, including:

— **Impersonation fraud** – Many fraudsters have found opportunities to impersonate trusted organisations, tricking customers into sharing credentials and personally identifiable information (PII). In the most extreme examples, some fraudsters even pose as family members or friends to trick their victims on social media and messaging platforms to transfer cash.

— **Intercepting one-time passcodes** – Fraudsters have also been convincing contact centre agents to port customers' numbers, allowing them to intercept one-time passcodes sent out during the authentication process. This method can either be used to gain crucial PII, access to the customer's personal device, or even to authorise banking transactions.

— **Whaling attacks** – Another form of impersonation fraud, whaling attacks involve fraudsters impersonating a senior member of an organisation to target other senior members and solicit sensitive information or steal money.

— **Banking trojans** – This is a method that requires even less effort from the fraudster. Banking trojans involve installing a piece of malware on an employee's device, which then attempts to solicit credentials and financial information from your bank's infrastructure. In many cases, victims are tricked into downloading the malware themselves, practically opening the door to the fraudster.

These are just a selection of fraudsters' capabilities today. Whichever method fraudsters choose, they can use the credentials they gain to easily bypass the knowledge-based authentication checks many organisations still rely on.

Meet the banking leaders fighting fraud

Organisations of all sizes can no longer protect their customers from fraud using traditional security methods. Now more than ever, they need to rethink their approach to fraud prevention and customer authentication.

In this guide, we'll showcase how four banks upgraded their defence against fraud using Nuance biometrics technologies—and how they're actively preventing and fighting fraudsters every day. You'll get an insight into the results they're achieving, and how you can do the same.

NatWest Group protects more than 19 million customers from fraud

Here's what NatWest Group achieved in just one year:

17M

calls screened for fraud

23,000

fraud alerts generated

>300%

ROI

NatWest

The voice channel has always been a core part of NatWest Group's customer service. But as with many banks, it's also a prime target for fraudulent activity. The banking leader wanted to find a way to protect its 19 million customers from criminal threats—from lone-wolf attackers to organised crime networks—which required a clearer view of fraud indicators across all its engagement channels.

NatWest deployed Nuance Gatekeeper to screen every incoming call and compare voice characteristics to a library of known fraudster voiceprints. Nuance Gatekeeper identifies known fraudsters in real time and alerts the contact centre agents and the fraud team.

Since implementing Nuance Gatekeeper, NatWest Group has also been able to identify and disrupt criminal activity on digital channels—protecting its customers and assisting law enforcement in their fight against fraud.

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

It's not just about stopping financial loss—it's about disrupting criminals. For example, one prolific fraudster identified through Nuance was connected to suspect logins on 1,500 bank accounts. That's helped us protect potential fraud victims and identify the 'mules' being used by the crime network to perpetrate fraud, leading to two arrests so far."

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

HSBC saves more than £400M being stolen by fraudsters

HSBC

In 2016, HSBC started a major initiative to adapt its fraud prevention strategy to defend against modern attack methods and protect nearly 40 million customers from fraud. The bank wanted to support its 16,000 contact centre agents by giving them the tools to identify and authenticate genuine customers.

Using Nuance Gatekeeper at the centre of its fraud prevention strategy, HSBC has created a seamless authentication service powered by voice biometrics. The authentication service, named 'Voice ID', compares the characteristics of a caller's voice with the pre-recorded voiceprint—helping agents identify fraudsters among genuine customers.

The data gathered by Nuance Gatekeeper feeds into the rest of HSBC's fraud detection and prevention infrastructure, helping the bank build out behaviour profiles, strengthen its payment tracking initiatives, and ultimately create safer experiences for its customers.

"Fraudsters may attempt to impersonate customers by stealing or guessing personal information to pass security checks—but it's extremely difficult to replicate someone's voice."

— David Callington, Head of Fraud, HSBC UK

"Voice ID has not only made telephone banking more convenient for customers accessing their accounts, it's also been instrumental in stopping attempts at telephone banking fraud, protecting customers' money. Scammers are sophisticated and it's a constant challenge to keep ahead of them, but this is promising—we've seen a 50% drop in reported telephone banking fraud year-on-year."

— Kerri Mills, Head of Contact Centre and Customer Service, HSBC UK

£400M

of customers' money prevented from being stolen in one year

60%

reduction in telephone fraud victims within a year

50,000

fraudulent calls identified since deployment

Kennebunk Savings sets a new bar for fraud prevention among community banks

Kennebunk Savings, a mutual savings bank in Maine, saw fraud rise among smaller community banks and credit unions and wanted to find a way to improve its defences. The bank wanted to protect its customers without overwhelming them with security measures that damaged their personal banking relationships.

The bank implemented voice biometrics technology as part of Nuance Gatekeeper to compare callers' voices against their recorded voiceprints, and easily spot fraudsters attempting to break the bank's voice channel. Using Nuance Gatekeeper, agents can determine whether a customer is genuine or a fraudster within seconds.

In just a few months, Kennebunk Savings verified more than 3,700 customers using Nuance Gatekeeper, and it has now screened more than 38,000 calls have been screened for fraudulent activity.

"A lot of fraudsters are sitting at home trying to figure out our weak points. Knowing we have Nuance Gatekeeper as an added layer of security has really been a great benefit for us.

Nuance Gatekeeper is a game-changer for our agents. They're no longer under pressure to make difficult decisions when authenticating customers—they can focus on delivering standout customer service."

— Jennifer Johnson, Senior Vice President, Senior Customer Experience Manager, Kennebunk Savings

38,000

calls screened for fraudulent activity

8,000

customers enrolled in the voice biometrics service

3,700

customers verified using Nuance Gatekeeper since launch

Bangor Savings Bank protects its community from rising fraud

Bangor Savings Bank is a state-chartered bank operating in Maine and New Hampshire. Seeing a rise in fraud within its communities, the bank wanted to protect its 250,000 customers from any new threats.

Now, when someone calls the bank's contact centre, it uses Nuance Gatekeeper to compare their voice against a database of customer and known fraudster voiceprints. If the caller's voiceprint matches with a known fraudster, Nuance Gatekeeper automatically generates a real-time alert so the call can be immediately investigated by the bank's security team.

Bangor Savings Bank has been using Nuance Gatekeeper for nearly two years. Within the first 18 months of deployment, the bank identified 34 confirmed fraudsters. And towards the end of the 18-month period, it was spotting an average of four fraudsters per month.

"Our customers love VoiceID, as it completely removes the friction from the authentication process. Now, it only takes around ten seconds to authenticate our customers, and our overall call times have been reduced by more than a minute.

Creating a new authentication experience isn't an easy project, but working with Nuance, the whole process has been seamless. They've helped us every step of the way, providing all the training and change management support we needed—we never had any major roadblocks."

— Chris Lobley, Vice President and Support Department Manager, Bangor Savings Bank

4

fraudsters spotted every month

34

confirmed fraudsters caught in the first 18 months of deployment

91%

customer enrolment rate in voice biometrics

Intelligent fraud detection and biometric authentication

Here's why so many financial institutions trust Nuance Gatekeeper:

3x

fraud cases handled daily, with 90% reduction in manual reviews

90%

detection of fraudsters in 15 seconds or less

<1 sec

of audio to authentication vs. 57+ sec with other authentication methods

99%

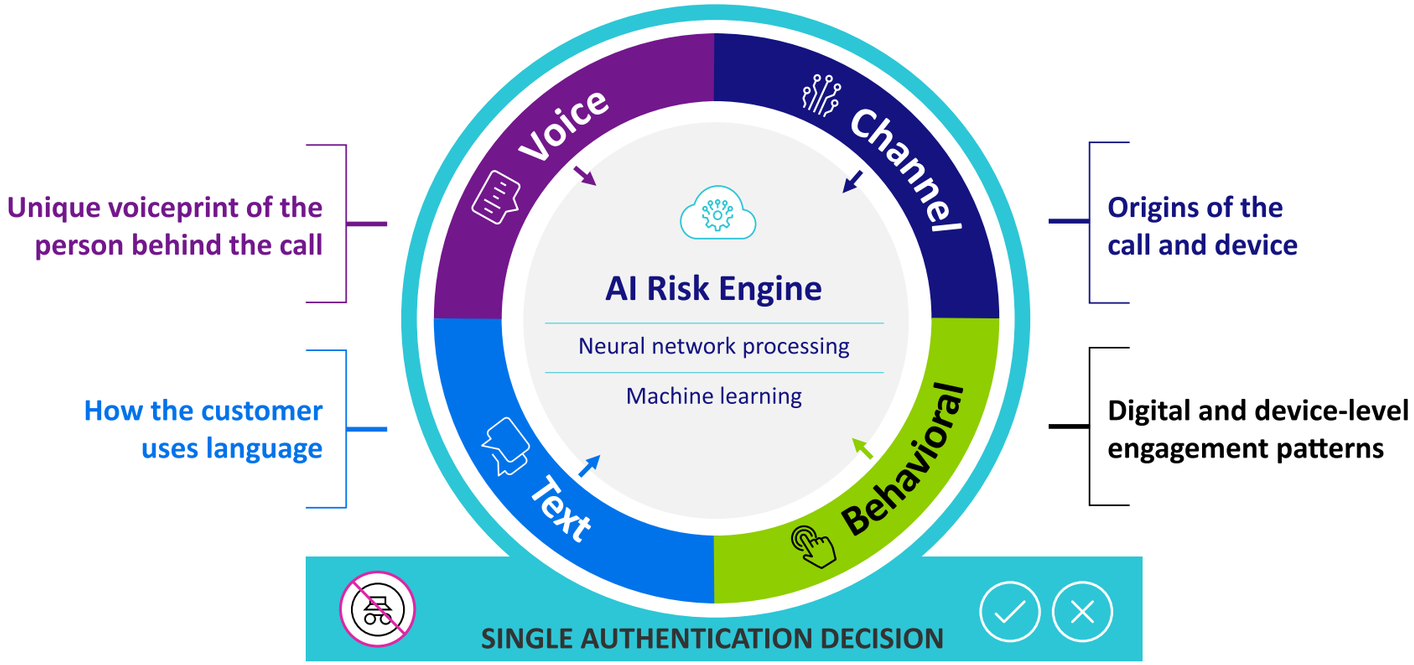
authentication success vs. <80% with passwords, PINs, or security questions

One thing that unites all these banks—and hundreds of other banking leaders worldwide—is their use of Nuance Gatekeeper, our biometric authentication and intelligent fraud prevention solution.

Gatekeeper replaces outdated verification factors and prevention methods, helping companies verify the actual person behind the interaction and easily spot fraudsters across every engagement channel.

The security solution uses deep neural networks and industry-leading AI to determine a single, transparent authentication decision for every engagement—considering voice, text, behavioural, and engagement channel characteristics.

Multilayered Biometric Security



Protect your customers with intelligent fraud prevention today

As disruption continues, the opportunities for fraudsters will only increase—and their attack methods will become more advanced. But these banking leaders have shown it's possible to stay one step ahead and continue protecting customers far into the future.

To keep your customers safe across every engagement channel and stop fraudsters in their tracks, you need an intelligent fraud prevention solution that's based on biometrics technology.

Ready to learn more?

If you're ready to learn more about Nuance Gatekeeper, or want to talk about your own fraud prevention strategy, you can:

Visit our dedicated fraud infohub—to learn how Nuance Gatekeeper can help you strengthen your defence against fraud.

Get in touch at cxexperts@nuance.com—for personalised advice from one of our fraud prevention experts.

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_4728_01_EB_UK, Aug 16, 2022