NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

Why are super funds switching to biometric authentication?

Nuance Communications

February 4, 2022

As superannuation funds struggle against a rising tide of fraud, a new partnership between Nuance and financial services consultancy QMV is paving the way for funds to strengthen protection for accounts—while enhancing member experiences and reducing operational costs. Here's why one of the first items on super funds' agendas should be upgrading from slow, unsecure knowledge-based authentication to fast, secure biometrics.

After the successes we've seen Australian banks and government departments achieve with our solutions, we're very excited about our new partnership with QMV, a financial services consultancy that advises superannuation funds on technology investments.

By combining our customer engagement and security innovations with QMV's expertise in super fund operations and technology, we'll be able to deliver high-impact solutions that transform member experiences, reduce operational costs, and improve fraud prevention. In the short term, we plan to work with QMV to help super funds realise immediate business benefits by making the switch to biometric authentication.

It’s time to make the switch

The massive increases in consumer fraud, identity theft, and account takeovers that accompanied the COVID-19 pandemic have prompted super funds to strengthen their fraud prevention capabilities. To protect member accounts effectively, it’s critical that funds move away from the unsecure PINs, security questions, and two-factor code verifications they’ve relied on in the past.

From email and SMS phishing to fraudulent calls, malware, and even stolen mail—fraudsters have numerous ways to get members’ personal information and hijack their accounts. Now it’s time for funds to retake control by replacing knowledge-based authentication methods with biometric authentication powered by advanced AI technology.

By verifying identities based on thousands of unique characteristics in people’s voices, their behaviour, or how they hold conversations, biometric authentication provides the fastest, most secure way to protect member accounts.

Biometric authentication successes in Australia

Perhaps the best-known use case for biometrics in Australia is the passphrase, “In Australia, my voice identifies me,” which was first implemented by the Australian Taxation Office in 2016 and later deployed at MyGov by the Department of Human Services. Biometric authentication has strengthened security and transformed the experience of dealing with government departments, with average handle time (AHT) reduced by up to 48 seconds.

Australian banks like NAB have seen similar successes with biometric authentication across phone and digital channels, accelerating AHT, increasing self-service containment, and enabling step-up security for high-value transactions.

As well as passphrase-based biometric authentication, there’s growing adoption of passive voice authentication (where callers are authenticated from just a few seconds of natural speech), which eliminates the friction of authentication and lets customers get straight to the reason for their call.

The business case for biometrics: six reasons to switch

From our discussions with QMV, and based on our experience of implementing biometric authentication at financial services and government organisations worldwide, it’s clear that super funds can expect to see six major business benefits by making the switch to biometrics.

1: Stronger protection for member accounts

Biometrics solutions dramatically enhance account security and make identity theft much harder for fraudsters. Organisations using Nuance Gatekeeper, for example, see fraud detection rates of 90% or higher, leading to increased consumer trust as well as a lower incidence of successful fraud attacks.

2: Enhanced member experiences

With biometric authentication, members get the rapid, frictionless experiences they expect, helping agents provide faster resolutions rather than wasting time on lengthy authentication methods. Organisations typically see authentication times accelerate by 95% or more—with a corresponding increase in customer satisfaction. It’s also a great way to encourage secure self-service that gets members even faster resolutions to their queries.

3: Better employee experiences
When agents no longer have to interrogate members before they can begin to handle their issues, they can have more meaningful—and more fulfilling—interactions with members. Biometric authentication removes the pressure on agents to assess whether people are who they say they are and lets them do what they do best. Many financial services organisations also use the technology to monitor conversations and provide AI-powered compliance prompts on voice and digital channels, reducing agent stress even further.

4: Lower operational costs

We’ve already seen how biometric authentication reduces AHT to provide major savings in the contact centre. But it also has a major impact on fraud prevention efficiency and resourcing. With biometrics solutions intercepting most fraud attempts in real time, with a high degree of accuracy, fraud teams don’t need to over-resource to keep up with a constant stream of false positives. Instead, they can focus on investigating real fraud attacks to strengthen protection and assist law enforcement in tracking down criminals.

5: Reduced fraud losses

With fewer successful fraud attacks, the costs of fraud investigation and remediation will decrease—and funds can avoid the reputational damage associated with high-profile fraud cases. And as organisations' blacklist of known fraudsters' biometric "voiceprints" grows, losses will continue to fall. In fact, it's not unusual for organisations using Gatekeeper to reduce fraud losses by 92% or more.

6: Less repudiation risk
The strength and accuracy of voice biometrics makes it harder for members to falsely dispute interactions they did, in fact, authorize.

Tags: Financial services, Customer success story