NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement, Financial services AI

Why biometric security is the smart choice for wealth managers

Brett Beranek | Vice President & General Manager, Security & Biometrics

21 May 2023

As fraudsters actively target high net worth individuals, and legacy authentication processes become increasingly unfit for purpose, wealth management firms need to find new ways to protect their clients. For many, voice biometrics is proving the ideal solution—empowering wealth managers to enhance security and fraud prevention, while meeting their clients' high expectations, and delivering even simpler, faster, and more effortless service.

Fraud losses across the UK banking and financial services industry increased by 8% in 2021, to a total of £1.3 billion. And worse news for wealth management firms, high net worth individuals (HNWIs) are especially at risk; almost three quarters of individuals worth over £3 million have been a victim of financial fraud, with a fifth losing money.

At the same time, traditional authentication processes based on PINs, security answers, and even one-time-passcodes (OTPs) remain a poor deterrent to professional criminals—whose tool kits are bulging with malware, stolen credentials, and social engineering techniques.

To help keep their clients safe, many wealth management firms are now looking to strengthen their defences with advanced biometric security factors, such as voice biometrics.

We've written a white paper to explain why that's the case, and the benefits they're seeing as a result. You can download a copy here, or keep reading for a few of the key takeaways.

The problem with legacy authentication processes

Knowledge-based authentication

Knowledge-based authentication (KBA) is based on the assumption that only you know your password, your first pet, or the street you grew up on. But today, that's a dangerous assumption.

Thanks to large-scale data breaches, phishing and social engineering operations, and credential-stealing malware, an astonishing amount of Personally Identifiable Information (PII), including account and password pairings, is available to fraudsters. HNWIs who are well-known and have an established public presence online can be particularly attractive targets for information and identity theft. And when the information can't be bought or stolen, fraudsters can turn to open-source credential-stuffing and password-cracking tools.

Two-factor authentication with OTPs

Two-factor authentication based on OTPs may be a more modern solution, but like KBA, it's often susceptible to exploitation.

In recent years, we've seen how easy it can be for fraudsters to commit "SIM Swap" attacks, convincing mobile providers to port someone's number to a device they control. If the victim's wealth manager relies on SMS-based OTPs, the fraudster can simply request password resets on that person's financial accounts, confirm them using the OTPs that arrive on their phone, and begin to empty their accounts. Just ask Robert Ross—a tech investor who lost almost $1 million in less than an hour.

Trick your victim into downloading the right kind of malware, and stealing OTPs can be even easier. TeaBot, for example, enables fraudsters to not only steal account credentials as they're entered into apps, but intercept OTPs—sharing them with the fraudster while hiding them from the device's owner.

Facial recognition software and fingerprint scanners

As biometric solutions, facial recognition software and fingerprint scanners at least attempt to check who someone is, rather than what they know, or what they own. But for wealth managers—and financial institutions more generally—these embedded biometric technologies have some major limitations.

Most critically, they don't allow organisations to identify the actual individual attempting to access their services, because the authentication data never leaves the device. Server-side biometric authentication is much more powerful, as it enables fraud prevention professionals to identify known fraudsters, and frustrate fraud attempts, in real time. It also equips them to join the dots between historic fraud attempts, tie multiple attacks back to the same individual, and build comprehensive cases to support arrests and prosecutions.

Voice biometrics: a better way to authenticate

Voice biometrics are popular because they don't share these limitations. Leading solutions analyse millions of different data points, making them incredibly difficult to fool. Even if a fraudster has the time and resources to synthesise or "deepfake" a client's voice, that process leaves tiny artifacts behind on the audio signal which leading voice biometric solutions can identify.

But just as importantly for wealth managers, voice biometrics make life easier for clients, even as they make it harder for criminals. A client's identity can be authenticated in seconds while they explain their need to an agent. The agent sees the confirmation on their screen and can focus on with addressing that need, without asking uncomfortable probing questions.

The technology works the same way when clients interact with a conversational IVR or through messaging channels. Clients are seamlessly authenticated using their voice when speaking with their wealth manager's IVR, or simply by speaking a passphrase into their wealth management app.

Discover how voice biometrics can deliver 300% ROI in a year

There's a lot more to discover about the business benefits of switching to voice-based biometric security, and why it's such an ideal solution for wealth management firms. Download the full guide to learn more.

Tags: Financial services, Biometric authentication

About Brett Beranek

Brett Beranek is responsible for overseeing the security and biometric line of business at Nuance, a Microsoft company. In this role for the past 12 years, Beranek has brought Nuance to a leadership position in the biometric authentication and biometric fraud prevention space. A thought leader in the field of biometrics, Beranek is a frequent contributor in industry events and the media on the topic of AI technology and it's use by the fraud community, and how society can mitigate against these evolving threats. Prior to Nuance, he held various leadership positions in the biometrics and security industry. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management. Beranek is also a certified Master Fraud Prevention Black Belt professional.

View all posts by Brett Beranek