NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

The key biometrics for fraud prevention: explained

Nuance Communications

30 March 2021

Biometric security has become a vital defense against a rising tide of fraud. But the range of biometrics technologies available to brands and fraud prevention leaders extends far beyond the fingerprint and facial recognition solutions now common in consumer devices. In this post, we explore the three key forms of biometrics for fighting fraud, and some of their most powerful applications.

Over the last decade, the effectiveness of traditional forms of identity authentication have been eroded. At the same time, fraud has become increasingly rife. Losses in the global economy have risen by 56%. In the UK alone, they now approach £190B each year.

At the heart of the problem with traditional methods of authentication is that they don't identify the actual human being that's interacting with a service or a device. Instead, they identify what they have (a token, or a phone), or what they know (their password, personal information, or memorable answers).

Now, as financial institutions seek to protect their customers and themselves, many are looking to biometrics to provide stronger fraud prevention.

Biometrics technologies resolve the problem with traditional methods of authentication by validating an individual's identity based on their physical characteristics, the way they speak, or the way they behave.

All three of these modalities have important applications when it comes to preventing fraud. Let's look at each in turn.

The biometrics modalities: Physical biometrics

Facial and fingerprint biometrics

Among the most ubiquitous physical biometrics are the fingerprint readers and facial recognition cameras we've become so used to relying on to secure our smartphones.

But while both these technologies can assist with fraud prevention—for example, by providing a more secure way to log in to mobile banking apps, or authenticate contactless transactions—they're far from the only physical biometrics that financial institutions should be looking to in their fight against fraud.

Voice biometrics

Another increasingly popular technology is voice biometrics. More and more institutions, including Allied Irish Bank and Barclay's Wealth and Investment Management, are giving their customers the option to record a voiceprint, which can then be used to quickly and securely authenticate their identity when they call.

Some voice biometrics technologies require customers to say a "passphrase"; others run silently in the background of a conversation, checking the customers' identity even as they explain why they're getting in touch.

Crucially, legitimate customers aren't the only people who can be rapidly identified using the sound of their voice. Known criminals can be, too. By comparing the voices of callers to its contact centre with a library of untrusted voiceprints, NatWest formerly named Royal Bank of Scotland has been able to identify one in every 3,500 calls as a fraud attempt. In one case, the bank was able to connect the would-be fraudster to suspect logins on 1,500 bank accounts.

The biometrics modalities: Linguistic biometrics

Just as the sound of our voice is unique, so is the way that we speak. The vocabulary and grammar we use, the way we structure our sentences – they can all be analysed and synthesised to create a "conversation print".

We call this technology linguistic biometrics. Even more versatile than voice biometrics, it can help to prevent fraud on a range of different engagement channels.

Linguistic biometrics on voice channels

Imagine a customer rings their bank's contact centre to query a transaction. Much like voice biometrics, linguistic biometrics can immediately start to verify their identity by comparing their words to an existing conversation print. Also, like voice biometrics, it doesn't matter if they're talking to a human agent or the bank's intelligent IVR system.

Linguistic biometrics on digital channels

Let's say same customer goes online later in the day, to open a new savings account. Whether they're chatting to a virtual assistant or a human agent, linguistic biometrics can still help with identity verification, this time based on the vocabulary and grammar they're known to use when they type.

The biometrics modalities: Behavioural biometrics

Now, what if you could go one step further and identify a legitimate customer not just by the language that they use, but by the way they type? And the way they use their keyboard and mouse, or hold, swipe, and tap on their device?

Well, you can. This is behavioural biometrics, and it's ideal for applications where continuous authentication is required.

Seamless, continuous authentication with behavioural biometrics

Remember that customer we left opening an account online? Imagine that they forget to log out of their online banking portal, and their session gets hijacked by fraudster. If their bank is constantly comparing their activity to an expected profile, it will spot the sudden change in user behaviour. An alert can be triggered, and action taken to mitigate the risk.

Discover how UK banks are using biometrics to prevent fraud, today

What does all this look like in practice? Watch this recent episode of The Fintech Show, and you'll hear NatWest and AIB talk about their own use of biometrics, and the technology's impact on both security and customer experience.

Tags: Financial services