NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention

How biometric security can transform a fraud investigation

Nuance Communications

August 16, 2022

As more organizations embrace biometric security, their fraud teams are pioneering a raft of investigation techniques. In this blog post, I explain how just one of those techniques has been used in real life—to solve a baffling case, identify the guilty party, and prevent financial loss.

Amidst the disruption of the pandemic, many fraudsters shifted their focus to identity theft—in fact, between 2019 and 2021 it was reported that true identity theft increased 81.8% across industries. This, in turn, greatly accelerated the adoption of biometric security. Indeed, there was a 48% year-on-year increase in organizations using biometrics for authentication between 2020 and 2021.

This move towards identifying people by something they are—rather than by something they know, or something they own—isn't just great news for honest customers and citizens, many of whom are now enjoying simpler, more secure authentication experiences.

It's also great news for fraud prevention teams, many of which now have new scope to investigate cases, protect their brand and its customers, and drive criminal prosecutions.

The best way to illustrate this is through the story of a real-life fraud investigation, which I've anonymized to ensure confidentiality. This particular story shows how fraud investigators are harnessing one of the most powerful and versatile forms of biometric security: voice biometrics.

Let's set the scene.

The facts in the case of Jane Doe

Jane Doe calls her bank to report that she's been a victim of fraud. She's noticed that her credit card has been used to make purchases at a local electronics store—purchases she knows nothing about.

You work for the bank's fraud team. You can see that:

- Her account's billing address was recently changed, and a new card requested
- This happened via a call made to your contact center
- The fraudulent transactions were made with chip and PIN
- The sum of the transactions didn't exceed the card's limit

You know that changing someone's billing address and requesting a new card is a classic scam—allowing a fraudster to easily intercept the new card and make legitimate-looking transactions.

But the fact that the fraudster's purchases didn't exceed the card's limit gives you pause . It suggests your fraudster is someone who was not only able to obtain a new card in Jane Doe's name, but knew exactly how much they could spend on it without having a transaction declined.

So—what's really going on? Should your bank absorb the loss?

The fraud investigation begins

First, you listen to the call that was made to change the address and request the new card. You naturally need to confirm that this call wasn't placed by the customer herself.

The person you hear speaking clearly isn't Ms. Doe, but they answer the agent's questions as effortlessly as if they were, and without any attempt at social engineering.

You also know that your organization hasn't encountered this fraudster before. Your contact center uses Nuance biometrics to monitor conversations in real time, and raise the alarm if a caller's voice matches the voice of a fraudster already on its watchlist. It takes just 12 to 15 seconds of conversation to identify a known fraudster based on the sound of their voice—but this call was much longer, and it didn't trigger any alerts.

It seems you've found a brand new fraudster to add to your watchlist. You wonder if Ms. Doe is the only victim—after all, if this newly identified fraudster has targeted other customers, you want to notify those individuals as soon as you can.

How you investigate with voice biometrics: Historical search

This is where voice biometrics begins to transform your investigation. You're able to search your organization's hundreds of thousands of call recordings and identify any that contain the fraudster's voice. In most instances, this will produce a small group of relevant calls you can review.

But—in this case, you don't find a single call that features the same voice.

This seems very strange. Your newly identified fraudster somehow has all the information they need to change Ms. Doe's address, but they've never called before—for example, to socially engineer that information out of your agents—and they have never targeted any other customer.

How you investigate with voice biometrics: Widening the net

In the real case that this story is based on, the fraud investigators decided to push a little further.

They knew that even criminals have their own, personal bank accounts. So, they asked the questions: What if this new fraudster also banks with us? What if they created a voiceprint, on purpose, for their own account?

When they widened their search to their database of voice biometrics enrollment calls, they found a single, strong biometric match—their mysterious new fraudster was an existing customer.

The customer's address was close to Jane Doe's address. The customer was also publicly connected to Jane Doe on social media. And when the bank's investigators obtained surveillance footage from Jane Doe's local electronics store, it clearly showed the customer making the "fraudulent" purchases.

Armed with all this information, they called up Jane Doe.

A case is cracked—and a loss is averted

While being interviewed by the bank's fraud investigators, Ms. Doe abandoned her original story. She confessed that her friend had made the purchases on her card, with her full knowledge and permission.

Ms. Doe's friend, who, as the bank's investigators already suspected, was not a professional fraudster, had promised her it would be "easy money." Their pitch had been along the lines of, "Hey, I read on a forum that if you do this… and this… and say you're a victim of fraud, the bank will just refund you! So let me buy

a couple of iPads with your card, then you call in, and we'll split it down the middle?"

Ultimately, Ms. Doe was held responsible for the purchases and no losses were incurred by the bank.

Biometrics—a transformative technology for fraud investigations

Empowering fraud teams to find a handful of relevant calls, in a haystack of hundreds or thousands of recordings is just one of the many ways that biometrics are transforming fraud investigations.

Today, fraud investigators are also using biometrics to:

- Identify contact center agents who've been targeted with bribes or social engineering
- Identify new attack vectors, such as policy abuse, and assess the scale of the problem
- Connect apparently disconnected fraud cases across channels to better understand how criminals are operating, and to build criminal cases large enough to drive prosecutions

All this is possible because unified, biometrics platforms such as Nuance Gatekeeper give fraud investigators the ability to look beyond specific schemes and systems. They can increasingly monitor the individuals and networks behind the fraud, wherever their criminal journeys take them.

Tags: Security & biometrics, Customer engagement solutions, Nuance Gatekeeper, Authentication & fraud prevention

More Information

Explore our anti-fraud solutions

Discover how to prevent, detect, and investigate more fraud, with AI-based fraud prevention on every channel.

Learn more