Authentication & fraud prevention, Customer engagement

Advice for CX leaders designing their security strategy

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

18 March 2021

In our recent webinar, we asked Nuance Fraud and Biometrics Specialist Ian McGuire to share his up-to-the-minute advice on protecting customers and preventing fraud. The webinar is available to watch on-demand, but in case you don't have time to catch-up, we've gathered some of the key tips here.

When we talk to an organisation about the best practice approach for improving security with voice biometrics, we always let them know—it's rare those best practices will look the same a year down the line. That's because customer expectations change fast, and so do the methods fraudsters will use to attack.

In a recent webinar with Ian McGuire, Nuance Fraud and Biometrics Specialist, he offered some sound advice and an up-to-date perspective on how to approach security challenges with voice biometrics. Here are some of the highlights from the webinar:

Think of your mother when designing your security

strategy

Ian McGuire: When I work with software and UI designers, even if they already understand the concept of user-centricity, they don't tend to be emotionally engaged with the process they're creating. So, I tell them to imagine the person using the security service is their mother. There are several benefits to this approach.

Your mother represents a generation that is more likely to be phoning organisations. Also, she's possibly less technologically savvy than some of the younger demographics, so might need a bit more handholding through the authentication process. And advantage in terms of emotional engagement is clear-cut— that nobody wants to disappoint their mother or be the source of her aggravation.

Consider what makes customers anxious, embarrassed, and angry

Ian McGuire: With knowledge-based authentication, we've an expectation that the questions we're asked won't be too easy. For example, if your question is, "What's your date of birth?", the customer is going to think, "A fraudster could easily find that information and impersonate me!".

But equally if your question is, "What's your favourite food?", it becomes too difficult. They'll think, "My favourite food is sushi, but I opened this account 12 years ago, and I don't know if I'd even tried sushi then!"

You can easily end up with a customer who's nervous and frustrated. That frustration leads to embarrassment and anxiety because they might get locked out of their account—and that leads to anger. So, you've embarrassment, anxiety, and anger, and they aren't good ingredients for success.

But the beauty of biometrics is that, by putting the human at the centre of the process, it not only provides a good balance of security and usability but, improves security and usability over conventional mechanisms like knowledge-based questions.

The technology is just the foundation

Ian McGuire: The technology is the foundation on which you build your solution. So, having the right technology is essential—but it's not a guarantee of success.

To be successful, you also need to think about the customer experience, the business processes that surround your security solution, and how you communicate your solution to your customers.

In fact, communication is one of the most important parts. When you're talking about a security solution, you're talking about trust and credibility, and ensuring you communicate that credibility to your customers is absolutely vital.

Use biometrics to identify fraudsters, not just genuine customers

Ian McGuire: Fraudsters have been quick to exploit the chaos created in many parts of the world by COVID lockdowns. Voice biometrics can not only protect customer accounts during an attack but prevent fraudsters from attacking time and time again.

We do this by creating watchlists of common fraudsters. Using those watchlists we can identify fraudsters by the sound of their voice before an attack can begin. In this way, we make it easier for someone like your mother to access her account, while also keeping her safer.

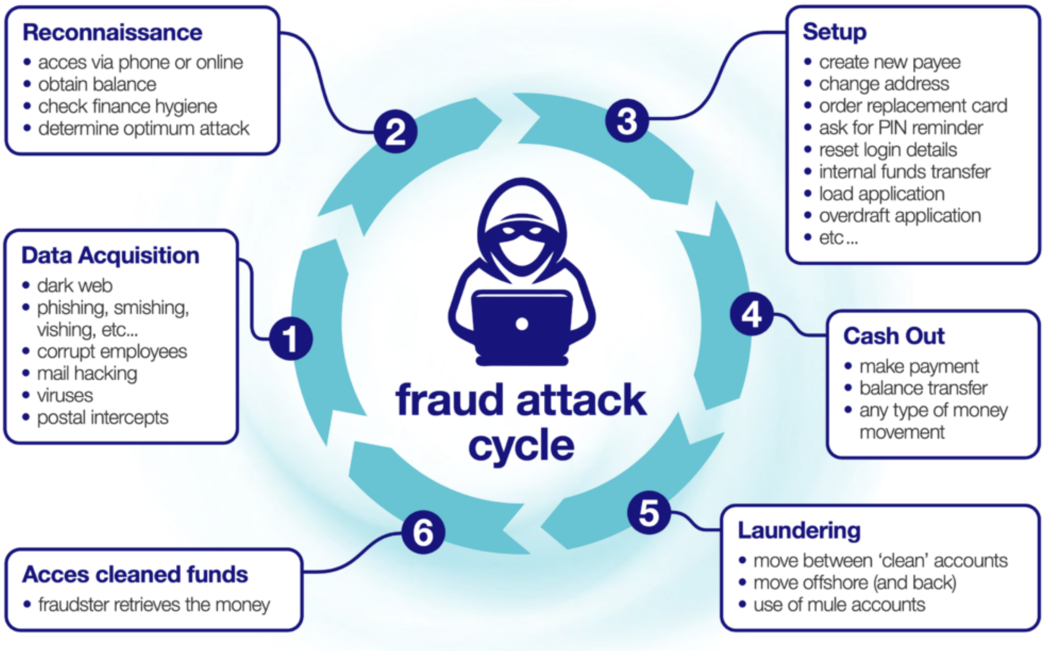
Protect your phone channel, and your digital channels will benefit too

Ian McGuire: Sometimes organisations say to me, "Most of my fraud attacks happen through my digital channels, not my phone channel." But to be frank, that's a slightly narrow view of how fraud works. S

Our research shows that when we put protection mechanisms in place on voice channels, digital channels also see the benefit.

When we analysed data from one of the biggest banks in the UK, we identified six stages of attack. It's not until stage four that the fraudster moves the cash out of the account. We discovered most of the security alerts were happening in stages two, reconnaissance, and three, setting up the crime.

This means we can take preventative action before any money is taken—something that usually happens on a digital channel. So, although we're only protecting the telephone channel, it's creating big benefits for digital channels too.



Fraud Prevention

Audience question: Do you have to use every part of Nuance Gatekeeper ?

Ian McGuire: It's a modular solution—you can choose exactly which features you want. It's about what's right for your requirements. Voice biometrics is the most commonly used part of Nuance Gatekeeper, for authentication and fraudster detection.

A good example is our recent deployment in Spain with Telefónica, as part of its COVID-response strategy. Telefónica wanted to help elderly customers who were at risk of being isolated as a result of the lockdown. The company asked us to deploy voice biometrics—not to identify the customer's identity, but to identify their age. It wanted to give customers over 75 faster access to human agents, by moving them to the front of the queue. So, although the underlying technology was voice biometrics, all we were really interested in was age detection.

Watch the webinar on-demand

While this blog post only covers a few best practice tips—there are many more to discover in the full webinar conversation and Q&A, including how:

- Biometrics can identify both physical and behavioural characteristics
- You can effectively communicate your security services to your customers
- We're helping leading banks to solve their security challenges
- You can balance security with customer experience

Tags: Customer experience, Nuance Gatekeeper, Knowledge-based 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