NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement, Retail AI

Retail fraud: Why consumer identities must evolve with biometric security

Nuance Communications

8 November 2021

As fraudsters steal their customers' personal information and identities, retail brands must learn from the authentication challenges recently faced by national governments and create stronger digital identities. This will mean bringing together technologies such as AI-based analytics and biometric security, but it will also mean breaking down silos and sharing knowledge, information, and strategies.

I recently attended the Merchant Risk Council (MRC) Las Vegas Virtual Event 2021. After the disruption of the last year, it's hard to overstate the need for such events where merchants can come together, discuss fraud risks, explore key solutions like biometric security, and share fraud prevention strategies and best practices.

One of the sessions on the agenda was "You Can't Fight Fraud in Silos", a discussion between myself and Jim Eckart, Chief Security Advisor at Microsoft. We wanted to run a joint session because we wanted to lead by example—and show how collaboration enables stronger digital identities for customers and stronger fraud prevention for retail brands.

Digital identities: Learning the lessons of 2020

Every business had to adapt last year. But fraudsters adapted fastest of all. They immediately stepped up their phishing activities, playing on pandemic-related fears and needs to gather information on potential victims. And then, as soon as governments began rolling out relief programs, they seized the opportunity to impersonate real individuals and businesses, or create synthetic IDs, and fraudulently apply for funds. According to the US Federal Trade Commission, identity theft cases doubled in 2020, while scammers stole billions of dollars by claiming unemployment benefit in other people's names.

Criminals found huge success with such schemes. The government organizations they targeted still relied on in-person authentication with physical documents. These organizations were also under tremendous pressure to provide relief funds as quickly as they could. As a result, the new processes and systems put in place to authenticate citizens remotely—based on their digital rather than their physical identity—often weren't sufficiently robust.

This should be a timely lesson for retail brands, most of which still recognize customers based on a relatively flimsy digital identity. When a fraudster has a customer's email address and password, a retailer has to work very hard to differentiate the bad actor from the trusted customer.

But by combining complementary, AI-based technologies, it's possible to create much stronger digital identities for customers—and even minimize the abandonment risks that come with adopting the 3DS 2.0 protocol or maintaining PSD2 compliance.

Towards stronger customer identities with biometric security

The analytics capabilities within solutions like Microsoft Dynamics 365 allow fraud teams to crunch transactional data, evaluate risk factors, and make timely interventions to prevent crime and financial loss. Team up these analytics capabilities with advanced biometric security—for example, through voice biometrics—and retailers can take such decisions with greater confidence and less manual effort, based on a stronger digital identity.

There's also an improvement in customer experience. Imagine you're staying with your parents for few weeks, when your laptop breaks down. You log into your account on their computer and attempt to buy a new laptop and have it sent to their house. The retailer's analytics flag the transaction as suspicious and automatically ask you to complete two-factor authentication, in line with PSD2.

Instead of having to request a one-time password to your phone (which, thanks in part to the rise of malware attacks, is an increasingly weak check), you simply say, "My voice is my password," and biometric authentication verifies your voice against the voiceprint that's part of your digital identity.

It's an easier checkout for you. It's a less risky transaction for the retailer. And it's one less false positive for its fraud team to investigate. The only people who don't benefit from stronger digital identities are the fraudsters currently targeting retail brands of every shape and size.

The fraud threats that retailers need to address

Just like national governments, many small retailers found their existing processes weren't ready for a pandemic. Forced to create digital storefronts rapidly, mom-and-pop stores entered the world of ecommerce without understanding the risks. Fraudsters immediately exploited their inability to spot suspicious activity. They targeted retailers with traditional card not present (CNP) transaction fraud—paying with stolen card details, picking up items from the store, and disappearing. A couple of days later, the retailer would receive notice of the chargeback.

Larger, more established retail brands had already invested heavily in their digital storefronts. They saw fraudsters target their comparatively neglected contact center operations. The fraudsters sought to manipulate agents, many of whom were working away from their colleagues and supervisors for the first time and were more susceptible to social engineering. They made fraudulent CNP transactions, arranged to be refunded for items they would never return, and impersonated customers to claim on their extended warranties.

For many retail brands, these threats still need to be fully addressed. And the creation of stronger digital identities is a vital part of the solution.

The role of biometric security in strengthening digital identities

When a brand knows a customer's voice, it knows whether they're the person calling to make a warranty claim. Equally, when a brand knows the voice of a professional fraudster, it can raise an alert as soon as they start speaking to an agent or a conversational IVR. For this proactive identification of known fraudsters to reach its full potential, data sharing between retailers will need to evolve further to ensure data quality, transparency, and shared definitions of fraudulent activity.

As many customer service teams continue to work from their homes, large retailers would also be wise to build stronger digital identities for their agents. If an agent is serving customers from their spare room, it

can be all too easy for a housemate or family member to get their log-in from a sticky note and start stealing sensitive information. With a combination of AI-based analytics and biometric security, retailers can be confident it's always their agent who's at the screen and on the line.

Diving deeper into retail fraud prevention

When I get to talk fraud prevention with Jim, it's always a great discussion—not least because, as a merchant member of the MRC, Microsoft brings the perspective of both a retailer and a solution provider.

But if you didn't attend this year's MRC Vegas Virtual, don't worry. You can learn much more about the current retail fraud landscape—including how to use analytics and biometrics to combat the most prevalent threats—in Nuance's new white paper, Retail fraud: Key trends and prevention strategies.

Tags: Retail, Fraud prevention, Biometric authentication, Microsoft, Merchant Risk Council, Biometric authentication