NUANCE | WHAT'S NEXT BLOG

Customer engagement, Authentication & fraud prevention, Financial services AI

# Credit unions fight fraud and transform member engagement with biometric authentication

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

November 21, 2022

Credit unions face rising fraud, increased operational costs, and severe staff shortages—but AI can help. Here's how AI-powered biometric authentication enables financial institutions of any size to prevent fraud while offering superior member and agent experiences.

In addition to the many challenges of staying competitive and profitable, credit unions face a rising tide of fraud. The entire banking sector saw a significant spike in fraud during the pandemic, as fraudsters pounced on new opportunities created by the disruption. This led many institutions to review their vulnerabilities and implement more sophisticated, AI-powered security measures, including biometric authentication.

Fraudsters will always seek new avenues to commit their crimes. So, while banks protected by biometrics have become harder to penetrate, fraudsters have turned their attention to smaller banks and credit unions that often still rely on outdated knowledge-based authentication (KBA) methods.

## KBA vs. biometric authentication

While credit unions have depended on KBA for many years to help protect their members from fraud, these methods are no longer fit for purpose. PINs, passwords, and answers to security questions are all readily available on the dark web–a 2022 study found that 24 billion username and password combinations are for sale. That makes it simple for criminals to acquire everything they need to breeze through KBA checks and access members' accounts.

And KBA isn't just susceptible to fraud—it also damages the member experience. Lengthy authentication processes that require members to recall multiple pieces of information slow down the interaction and cause frustration. It can feel like an interrogation rather than the warm, personal welcome members are used to receiving when they walk into a branch.

Biometric authentication solutions like Nuance Gatekeeper eliminate these issues by identifying members based on who they are, not what they know or which device they have. In the IVR and the contact center, Gatekeeper's voice biometrics technology analyzes millions of parameters in each caller's voice and compares them to the stored "voiceprint" of the member. Gatekeeper can authenticate using just a few seconds of natural speech, so members don't have to make any effort to prove who they are—making them feel known and valued.

In digital channels, Gatekeeper uses behavioral biometrics to analyze factors like how someone types, swipes, or clicks, and conversational biometrics to identify patterns in the language people use or the way they communicate in chat sessions.

With intelligent fraud prevention from multimodal biometrics, credit unions can shore up their security, while making it easier and more pleasant for legitimate members to do business.

## Reduce costs with biometrics

On her way to winning a People's Choice Award for her Speed Round at the 2022 CUNA Conference, my colleague Rachel Muench, Fraud and Biometrics Specialist, spoke with CU Broadcast. One of the themes she highlighted was the need for credit unions to reduce costs and how biometrics can help. Aside from the obvious cost savings of reducing fraud losses, biometrics helps credit unions save money in several ways.

Biometric technology dramatically speeds up authentication, shrinking average handle times (AHT) and contact center costs. For example, when Virginia Credit Union implemented voice biometrics for member authentication, it saw AHT fall by 84 seconds, delivering productivity gains equivalent to four full-time employees.

With biometric authentication, credit unions can also increase automation and self-service, further reducing costs. Biometric fraud prevention enables credit unions to offer self-service for higher-risk transactions such as transferring money, allowing members who prefer to use digital channels to manage their finances with ease.

## Empower agents with biometrics

Another key challenge highlighted at the CUNA conference was the chronic staff shortages that hamper the effectiveness of credit union contact centers. Biometrics and other AI-powered member engagement solutions can help here too, improving the agent experience while increasing productivity.

When members are effortlessly authenticated by voice biometrics in a conversational IVR, the system can offer a secure, personalized self-service experience for routine transactions, so agents don't have to deal with a constant stream of mundane inquiries. And in cases requiring a live agent's skills, they don't have to spend the first two minutes of the conversation interrogating members for KBA details. Instead, they can greet the customer by name and start dealing with the issue at hand—just like they would if the member had visited a branch.

## Deliver simple, fast, secure experiences with biometric authentication

Biometric authentication offers easier, faster, and more secure experiences for agents and members, which is why more credit unions are turning to biometrics and other conversational AI solutions for member engagement. As Matt Vignale, Vice President, Retail Delivery at Wings Financial Credit Union, says: "We're confident that Nuance's AI technology can enhance our ability to deliver the same personalized, enjoyable experiences our members are used to receiving when visiting our branches while

simultaneously protecting them from fraudsters.”

**Tags:** Nuance Gatekeeper, Authentication & fraud prevention, Financial services

## More Information

### Discover biometric authentication

Learn how a voiceprint can help you protect, personalize, and streamline every member interaction.

Learn more

## 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