NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

Intelligent Authentication (IAuth): An Origin Story

Nuance Guest Blogger

29 June 2020

In this guest blog, lead analyst at Opus Research Dan Miller explores how we arrived at 'Intelligent Authentication' and where biometrics plays a role in providing secure, convenient authentication at scale.

About the author: Dan Miller *is Founder & Lead Analyst with Opus Research. He*

has over 25 years of experience in marketing, business development and corporate strategy for telecom service providers, computer makers and application software developers

At the turn of the century, Intelligent Authentication emerged from the same primordial goo that spawned every initiative to “Kill the Password”. The value proposition was simple: “People should not have to remember a PIN or answer a series of questions in order to carry out business over the telephone.” Spoken words were a natural for business or queries initiated over the phone, including the rapidly growing population of mobile customers and citizens.

The technologies to support what was pretty much limited to “text-dependent caller authentication” were so novel that a telco subsidiary that was responsible for developing a citizen authentication system for the tax authority in Australia called on Opus Research to investigate and describe the global market potential for voice authentication. This led to some of the first spade work to discover solutions and use cases in other countries and in “the usual suspects” of industries; meaning banking, telecommunications and healthcare.

Our work gave rise to early optimism based on business cases that showed voice authentication shaved as much as a minute in the average handle time (AHT) for frequent calls. This had the side benefit of improving customer experience, while reducing the potential for the fraud loss that occurs when an imposter succeeds in gaining access to a personal information and financial assets. Improved customer experience was a further plus.

In the ensuing few years, we learned there were more barriers than we expected. Enrollment proved to be a major barrier. Each caller needed to be convinced to register his or her voiceprint by repeating the chosen phrase three times. In the absence of a financial incentive (like accelerating a refund) or an “opt-out” approach, enrollment rates could be as low as 30%; hardly ubiquitous deployment.

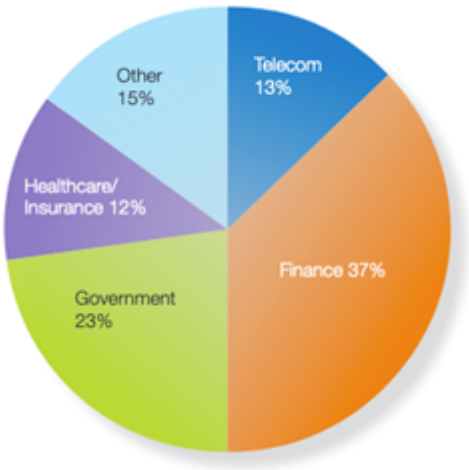
Another concern, at the time, was accuracy. Remember, this was more than a decade before the world

went wild over applications that used deep neural networks and artificial intelligence to detect patterns that affirmed an individual's identity or anomalies that exposed imposters. False accept rates in the 2% range matched with false reject rates in roughly the same range were fairly routine. The former was of concern to security departments that said they wanted "zero false accepts" while the latter, referred to those horrible instances where a legitimate customer is rejected from accomplishing a task for no apparent reason.

These shortcomings were overcome by technological advancements, improved packaging and integration, and proven use cases in the selected vertical markets.

Single-Channel Success: IAuth's Adolescence

Fast forward to 2016. Over 200 million individuals had enrolled their voiceprints for use in IVR or contact center-based customer authentication. In the introduction to our "Voice Biometrics Census" we asserted that the industry as "on the road to 1 billion enrollments" with the projected number of "protected users" as 600 million in 2020. As for the mix of industries, they went pretty much as expected (as illustrated below). Large banks and brokerages eclipsed government implementations, with "Finance" representing over one-third of the companies deploying voice biometrics in their contact centers and government agencies accounting for a little fewer than one-quarter. Telecom and Healthcare were roughly tied with 13% and 12%, respectively.



Source: Opus Research "Voice Biometrics Census" (September 2016)

The banks, healthcare companies, and telcos that implemented voice authentication in their contact centers share the characteristics of early adopters. Most were large companies with budgets allocated to "innovation" and "digital transformation". The government agencies added cost-consciousness and compliance concerns. All prospective deployers of voice biometrics-based solutions benefit from their input and feedback to solution providers.

Over the next five years, these single-factor, contact center-based solutions served as the raw material for more formidable offerings that integrated multiple biometrics (finger, face, behavioral), accommodated multiple channels (Web, messaging, video) and employed "artificial intelligence" for risk awareness and policy orchestration.

Wheel of Authentication: Introducing "Continuity" as The Fourth Factor

Source: Opus Research, 2020

If there's a single element that will shape the future of secure Conversational Commerce in the coming years, it is the addition of "fourth factor" for Intelligent Authentication. Common wisdom asserts that there are only three factors need to be employed for strong authentication of an asserted identity. As illustrated above, they are:

- **Possession**: "Something you have" – like an ID card or, in the online world, a credential or smartphone that can illustrate a one-time password.
- **Knowledge**: "Something you know" – primarily a PIN, password or answers to a challenge question.
- **Inherence**: "Something you are" – which used to refer to a narrow range of biometrics (eye, fingerprint, voiceprint) but now adds behavioral factors (gait, breathing patterns).

Add to these basics a measure of "continuity" or a running tally of the probability that the person who was just on a retailer's website using your phone in your home and then initiates a phone-call from a link in a mobile browser is, indeed, you. It calls for solutions with new key attributes. A quick checklist includes:

- **Real-Time:** Support rapid identification and authentication of a customer
- **Risk-Aware:** Assign the proper level of security based on the risk associated with an individual or action
- **Multifactor:** Achieve high levels of accuracy
- **Zero Effort:** Enroll and authenticate individuals without requiring action on their part

That is the starting point. It took twenty years or so to get here but remember: "That journey of a million miles starts with a single step." Well, chances are you needed a ride-share to get to the event's starting line.

Tags: Opus research, Biometric authentication

More Information