

Authentication & fraud prevention, Contact Centre AI, Customer engagement

Why pain-free authentication should be a strategic priority for your contact centre

[Brett Beranek](#) | Vice President & General Manager, Security & Biometrics

27 July 2021



Until recently, FSIs have had little choice but to ask their contact centre agents to shoulder the burden of customer authentication. We explore how the stresses and strains of these legacy processes ripple out, increasing centre costs, and damaging your business as a whole.

If you're managing a contact centre for an FSI, you'll know that agents do their best work when they're able to focus on the customer's needs. And that in a lot of cases, ID&V—while essential—is a stress that they could really do without.

But it's easy to underestimate just how damaging knowledge-based authentication processes are—not just to your agents' morale and service levels, but to a contact centre's efficiency and operating costs.

We've created a white paper that explores this chain reaction of authentication pain in depth—analysing its sources, how far it spreads, and how you can bring your peers together to end it for good. You can download a copy now, or read on, and we'll explain why modernising authentication processes should be such a priority for FSI contact centres.

Customer authentication: the burden on your agents

Knowledge-based authentication (KBA) processes demand that contact centre agents play the interrogator, judge and jury.

They have to ask the customer for a password, PIN, or memorable answer. They have to look out for suspicious behaviour. They have to decide whether to flag fraudulent intent. And if they fail to spot a criminal they have to deal with the consequences.

All of this a recipe of anxious, stressed agents, and low staff morale.

Customer authentication: the impact on your contact centre

Asking security questions takes time—for some organisations, between two and seven minutes^[1] per conversation. That's a huge amount of your workforce's day spent checking who people are, rather than actually addressing their needs.

But that's just the tip of the inefficiency-berg. When agent morale is low, agent churn tends to be high—leaving you with increased recruitment and training costs, and a less experienced workforce.

This can, in turn, have a direct, measurable impact on customer experience; a recent Nemertes study found companies that keep agent turnover below 15% see a 26% improvement in customer ratings.^[2]

Simply put? When authentication is painful for your agents, it's painful for your contact centre as a whole. What's more, if you lead the charge to modernise your ID&V processes, you're likely to have support from right across your business.

You're not the only one affected by painful authentication

Traditional, knowledge-based authentication processes are also a headache for CX and fraud prevention leaders.

Just as contact centre agents don't enjoy feeling like interrogators, honest customers don't enjoy being made to feel like suspects. The real criminals, meanwhile, are increasingly able to buy or crack customer passwords—which, as you might imagine, is a growing problem for many fraud prevention teams.

To learn more about how KBA impacts your peers, do pick up a copy for the white paper. You'll also discover why so many FSIs are looking to biometrics solutions to help them modernise and simplify their ID&V processes, and the benefits being seen by brands including NatWest Group and Barclays Wealth and Investment Management.

[1] Timeframe based on conversations with Nuance customers.

[2] Nemertes Study conducted April 2020.

Tags: [Contact centre strategy](#), [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 its 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](#)