

Customer engagement, Financial services AI

Compelling conversations: Transforming CX at National Australia Bank

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

September 30, 2020



If you missed our interview with Chris Barnes from National Australia Bank (NAB), we're here to catch you up. Discover why NAB implemented voice biometrics, the big business benefits it's seen since launching the system, and practical advice from Chris on how to ensure your own biometrics journey is successful.

Manual authentication can be a stressful process for customers and agents, adding time and effort to even the most routine interactions. At National Australia Bank (NAB), its 2,000 frontline bankers handle more than 8 million inbound calls every year. So, when the bank was looking for ways to reshape the customer experience—and take pressure off its bankers—biometric authentication made perfect sense.

As part of our webinar series, *Creating Compelling Customer Conversations*, I spoke with Chris Barnes, NAB's Head of Direct Channel Development, about the bank's biometrics implementation journey.

Here are the key things we learned from talking to Chris about the challenges the bank faced, the results it's seen since deploying biometrics, and the lessons learned along the way.



The authentication challenge

Relying mainly on manual authentication created a dual problem for NAB.

Firstly, it was difficult and frustrating for customers, who often found the questions challenging to answer. Chris told me that even he found it impossible to pass the bank's manual authentication process without logging into the mobile app for information.

In the best-case scenario, with the whole process running smoothly, manual authentication could take two minutes. In the worst cases, it could take 15-20 minutes to authenticate customers—a very frustrating experience for everyone involved.

Which brings us to the second problem: manual authentication was damaging the agent experience, as well as the customer experience. Not only was it the number one driver for non-compliant calls, the stress of the authentication experience was also the number one driver for bankers deciding that a contact centre role wasn't right for them.

So, when Chris and his team were building the business case for voice biometrics, while the primary goals were around FTE release, improving the customer experience and extending banker tenure were also major pieces of the puzzle.

The business value of biometrics

Today the bank's VoiceID biometric authentication system uses unique physical and behavioural characteristics from customers' speech to create a voiceprint that can be used to verify their identity.

Chris revealed that the benefits NAB is realising from the biometric authentication experience have far exceeded what he was expecting to see. The bank had initially targeted a 30-second reduction in Average Handle Time (AHT) compared to manual and SMS methods. But NAB has actually achieved around a 60-second AHT saving, and in many cases that's closer to 80-90 seconds.

The VoiceID system delivers more than 95% accuracy, and Chris said that figure could go even higher if the bank adjusted the security parameters—there's always a balance to be struck between security and customer convenience.

Since November last year, NAB has enrolled more than 100,000 customers on VoiceID. The bank currently enrolls around 1,200 customers a day onto the system and aims to have a total of 250,000 customers enrolled by the end of 2020.

Over the next 12-18 months, NAB plans to deploy biometrics in its IVR and mobile app. The aim is to authenticate customers in the IVR so they can self-serve on the 50-60% of calls that are routine, low-effort transactions, such as checking an account balance.

Lessons learned

Chris had several pieces of advice for organisations considering implementing biometrics in their contact centre:

1: Be clear on your architecture requirements from the beginning

NAB's biometrics implementation was slowed down by a decision during the project to switch from an on-premises deployment to the cloud. So, Chris advised organisations to make upfront decisions about deployment location, integration points and security architecture to ensure a fast, smooth deployment.

2: Design the right experience

NAB has excellent change management and communications teams who worked closely with the Nuance team and the bank's operations team to design the ideal experience for bankers and customers.

3: Listen to the experts

Chris and his team realised that Nuance has experience in implementing biometric authentication systems in organisations all over the globe, and I was very proud to hear that they valued our expertise and advice about how to set up, deploy, and optimise the platform for success.

Join us for the next session

Over the coming months, we'll be speaking with other organisations about their experience of implementing digital customer engagement and biometric authentication solutions.

Tags: [Financial services](#)



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](#)