NUANCE

Top reasons why painful customer ID&V hurts your whole business

Essential advice for financial services companies who need to simultaneously reduce friction and increase security: CX leader edition.

eBook
Rethinking Customer Authentication

Are you losing sleep over customer authentication?

You're not alone.

If you're responsible for customer experience at your organisation, there's every chance your customer authentication process is giving you some sleepless nights.

After all, the way a financial services institution verifies a customer's identity is pivotal to their experience of the brand. And if these interactions prove too painful, customers can be all too quick to take their business elsewhere.

But you're not the only one who's concerned. The legacy knowledge- and token-based authentication processes that can compromise customer experience are also a massive headache for your business's contact centre and fraud prevention leaders.

Over the next few pages, we'll explore how so many of your problems can be traced back to the same root.

We'll also explain why it's worth bringing everyone together to rethink your Identity and Verification (ID&V) strategy—including the benefits you could all gain by switching to a simpler, more secure authentication process, based on voice biometrics.

96%

of customers become more disloyal after high-effort service interactions.

Gartner[1]

[1] Gartner, via ID R&D, Biometrics to the Rescue report.

The pyramid of authentication pain

Every time a customer forgets their password—or discovers their account has been taken over by a fraudster—the pain they feel cascades down, and out across your business.

77%

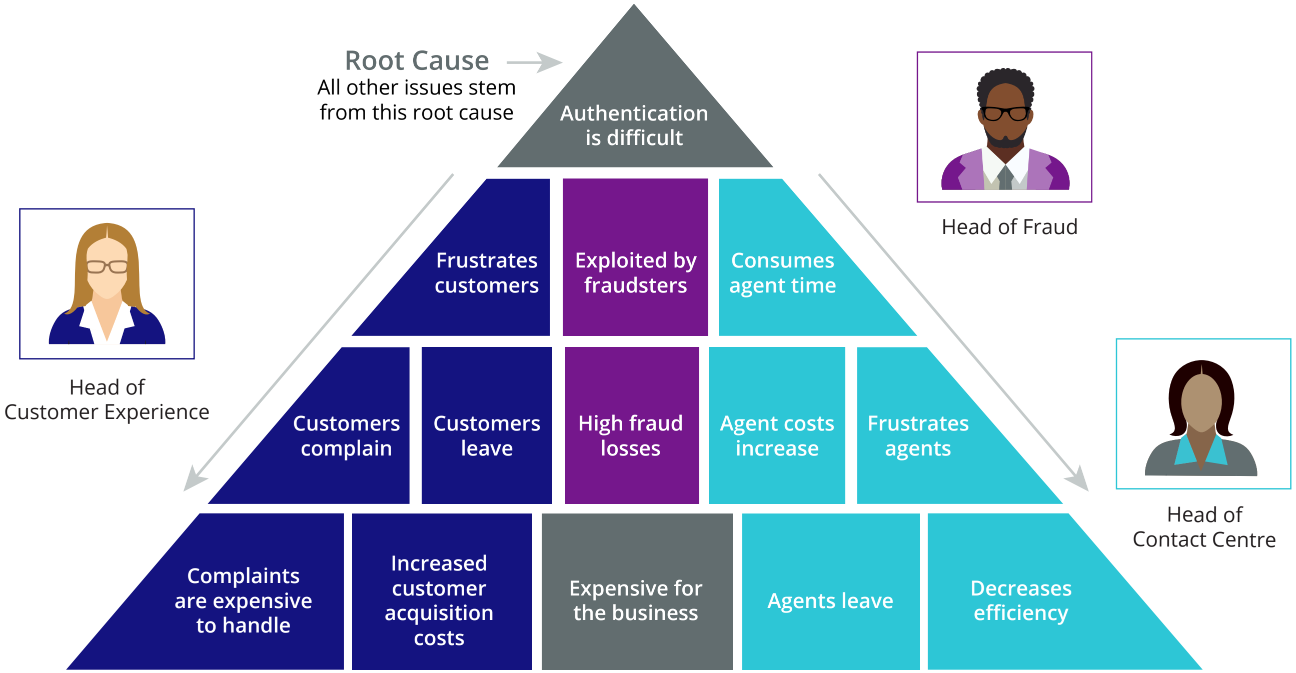
of customers want to switch service providers after a single frustrating interaction with an agent.[2]

The pain *you* feel

Slow, difficult authentication experiences frustrate your customers. They generate complaints—these days, often aired publicly over social media—and your organisation must devote time and resources to responding with due sensitivity and speed.

Worse still, a customer's frustration can cause them to leave your brand for good. PwC reports that a single frustrating interaction with an agent is enough to make 77% of customers want to switch service providers.[2]

To pile pain on top of pain, new customers are harder to win when other brands can tempt them with simpler authentication experiences, based on more modern technologies. Competition in this area is increasingly fierce, with 96% of businesses now seeing identity verification as a competitive differentiator.[3]



Root Cause
All other issues stem from this root cause

Authentication is difficult

Frustrates customers

Exploited by fraudsters

Consumes agent time

Customers complain

Customers leave

High fraud losses

Agent costs increase

Frustrates agents

Complaints are expensive to handle

Increased customer acquisition costs

Expensive for the business

Agents leave

Decreases efficiency

Head of Customer Experience

Head of Fraud

Head of Contact Centre

[2] PwC, 2017 survey "Experience is Everything," Research completed in 2018.
[3] Dology 7th Annual Fraud Report, October 2019.

The pain felt by fraud prevention leaders

The pain of your legacy authentication processes is felt just as keenly within your fraud prevention team.

Knowledge-based authentication asks human beings, your agents, to act as gatekeepers. Even an experienced agent can be socially engineered by an experienced fraudster—allowing the criminal access to a customer account, or to personal information that can be used in subsequent attacks.

But many criminals won't need to deceive your agents into revealing sensitive information. They'll have already purchased it on the dark web.

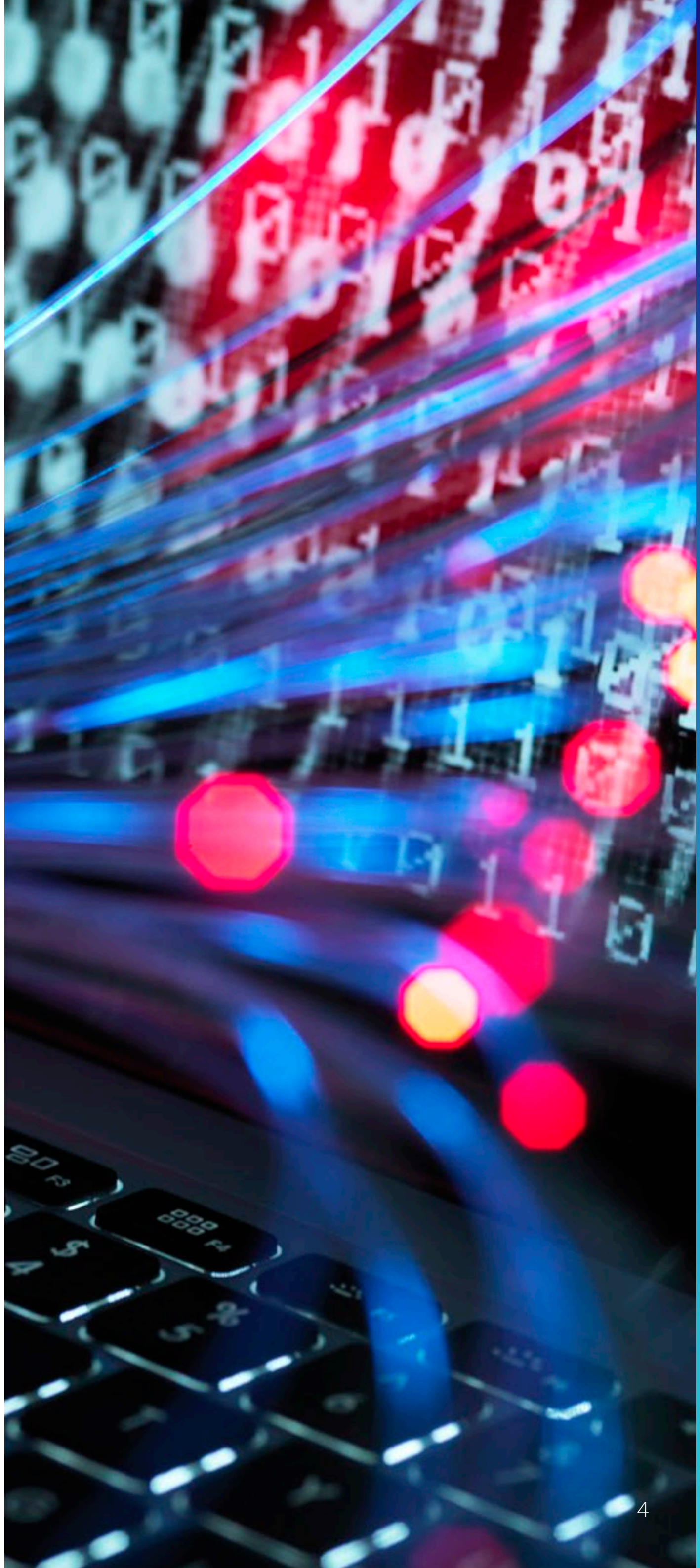
Even if they're missing a customer's password, there is every chance they can crack it. A recent analysis of >1 billion leaked credentials, including 168,919,919 passwords, found 42% were vulnerable to quick dictionary attacks. And 1 in 142 passwords was '123456'.[4]

Token-based authentication—for example, by sending a code to a customer's phone—has its problems too. A fraudster with access to your customer's mobile account only has to swap their number to another SIM before they make their attack.

The bottom line is this: Legacy authentication technologies are too easily exploited—leading to high fraud prevention costs, and high fraud losse

15B

15 billion account username and password combinations are for sale online, including bank accounts.[5]



[4] ZDNet reporting on an analysis of >1 billion leaked credentials that included 168,919,919 passwords, July 2020.
[5] Digital Shadows study reported via ZDNet, July 2020

The pain felt by contact centre leaders

Asking knowledge-based authentication questions takes time—for some organisations, between two and seven minutes.[6] It makes contact centre agents feel like interrogators, and it makes them fear the consequences of failing to spot a criminal.

The result is a long Average Handle Time (AHT), and unhappy, anxious agents. Which, as you can imagine, are the last things that anyone charged with running an efficient and productive contact centre wants to see.

The length of every customer conversation reduces agent efficiency and increases staffing costs. Low agent morale, meanwhile, drives up agent turnover. On top of the extra agent acquisition costs for your contact centre, this leads to a more inexperienced agent workforce, and ultimately impacts your customer experience too.

With more customer interactions moving online, contact centre leaders also need a more efficient way to authenticate customers across channels; 65% of fraud executives say digital fraud attacks are creating costs, volume pressures, or both within the contact centre.[7]

The financial pain for your business (a great reason to fix this together)

So, to summarise—a painful authentication process contributes to:

— Customer complaint costs

— Customer acquisition costs

— Fraud prevention costs

— Fraud losses (and reputational damage)

— Contact centre operational costs

— Agent acquisition costs

Simply put, it's hugely expensive for your business as a whole.

Here's the good news: As a customer experience leader, you're in a perfect position to spearhead change and drive benefits that will be felt throughout your financial services institution.

26%

Companies that keep agent turnover to <15% see a 26% improvement in customer ratings.[8]

[6] Timeframe based on conversations with Nuance customers.
[7] Market Trends in Digital Fraud Mitigation report, Aitë Group.
[8] Nemertes Study conducted April 2020.

Why so many leading brands are switching to biometric authentication

The fundamental problem with legacy authentication processes is easy to grasp: They identify people based on what they know, or what they have, rather than based on who they actually are.

Biometric authentication addresses the issue head-on: identifying who a person actually is. It uses the characteristics unique to your customers—their fingerprints, their face, the way they hold their device, the way they type, the sound of their voice—to confirm who they are.

Voice biometrics, with its ease of use and extremely high degree of accuracy, is an increasingly popular solution for leading financial services institutions.

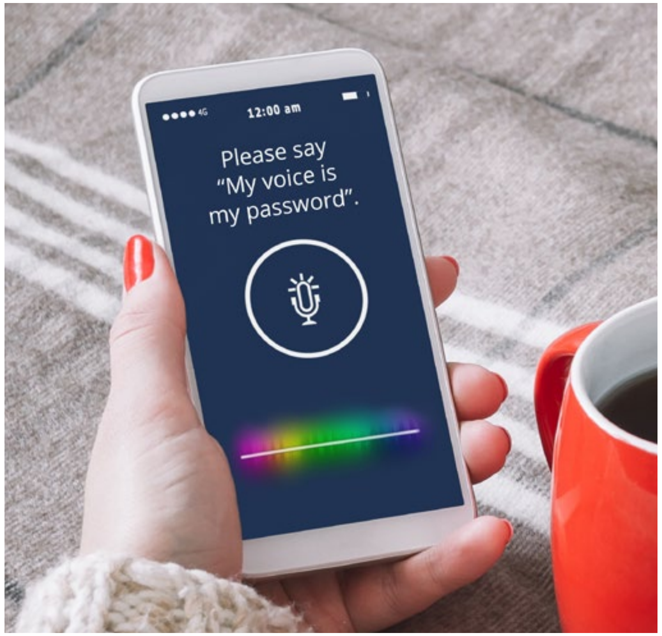
Once a customer has recorded their 'voiceprint' for the brand's use, their identity can be automatically verified within seconds, whether they're speaking to a human agent or an IVR. The customer doesn't have to remember a password or request a one-off code. The agent doesn't have to play the interrogator. Both can focus on the task at hand.

Even better, you can use voice biometrics to proactively identify known criminals by matching their voice against a voiceprint watchlist.

Just as a slow, weak authentication process causes pains throughout a business, the speed and security of voice biometrics can release a cascade of far-reaching benefits.

81%

of consumers view biometrics as a more secure form of identity verification.[9]



[9] Interview with Head of Global Fraud & ID Production Innovation at Experian, February 2020.

The benefits for you: A next-level customer experience

Voice authentication solutions can be ‘active’ or ‘passive’. If active, your customer is asked to say a simple phrase to verify their identity. If passive, the solution listens as they begin their conversation with your IVR or agent, authenticating the customer entirely in the background. Either way, it’s a fast, easy, secure experience.

Voice authentication enables you to contain more calls in your IVR, shortening customer wait times. When a customer does need to talk to an agent, it’s a simpler, more efficient, and less awkward interaction; your customer doesn’t have to struggle to remember a password, and your agent can relax and focus on helping them, knowing they’re protected against being socially engineered.

What’s more, the greater level of security afforded by voice authentication allows brands to extend the range of actions a customer can complete without recourse to a human agent. For a financial services institution, a popular choice is to support some higher risk transactions, like setting up a new payee.

Improving experiences with voice biometrics at Barclays

— Both customer and agent satisfaction increased

— 93% of customers scored 9 or 10 (out of 10) for ID&V

— 90% reduction in complaints

CSAT and ASAT

> “The use of Nuance’s voice biometric technology has been integral in our mission to deliver an excellent customer experience. The customer and employee satisfaction results speak for themselves. We’re looking forward to working with Nuance in the future to use voice biometrics to authenticate even more processes.”
>
> — Anne Grim
> Head of Global Client Experience
> Barclays Wealth and Investment Management

The benefits for your contact centre: Lower AHT, happier agents

Faster, more robust authentication isn't just a win for your customers: It's a win for your contact centre, too.

When compared to knowledge-based authentication, voice authentication solutions reduce AHT by an average of 53 seconds,[10] and often by a minute or more. Better still, because successful authentication no longer depends on your customers' memories, fewer genuine customers fail authentication, and less time is spent handling these cases.

This increase in contact centre efficiency comes coupled with a reduction in agent churn.

As we've seen, voice authentication reduces the burden on agents and protects them against criticism. This allows them to focus on actually helping the customer—increasing the agent's job satisfaction and reducing the likelihood of them leaving their role. This means less time and money spent hiring and training new agents. And when the time does come to hire a new agent, training them to conduct compliant customer conversations is quicker and easier than ever.

Reducing AHT worldwide with voice biometrics

Nuance voice biometrics customer	Reported AHT reduction
Australian Tax Office	48 seconds
Banco Santander	42 seconds
Global Financial Institution	89 seconds
U.S. Regional Bank	60 seconds

[10] Average reduction in AHT calculated based on results reported by Nuance customers.

Preventing fraud with voice biometrics at NatWest Group

17M

calls protected annually

2,500+

fraud calls detected

>300%

ROI in the first year

The benefits for your fraud prevention team: Reduced losses and active prevention

With authentication based on voice biometrics, criminals can no longer use stolen usernames and passwords to launch a successful attack and they have fewer opportunities to socially engineer such information out of your agents.

Add to this the technology's ability to identify known fraudsters—and more effectively flag suspicious and 'bot' calls—and the impact on fraud losses and prevention can be profound.

HSBC UK's voice biometrics system has prevented £608m of attempted fraud in under two years. The bank now has over three million UK customers enrolled in its system, which performs around nine million verifications each year.[11, 12]

> "The ROI from the tool is probably well over 300%, so as payback from a technology deployment, it's been very impressive."
>
> — Jason Costain
> Head of Fraud Strategy and Relationship Management
> NatWest Group (formerly Royal Bank of Scotland Group)

[11] https://www.about.hsbc.co.uk/news-and-media/hsbc-voiceid-attempted-fraud (Accessed February 8th, 2021)

[12] https://www.about.hsbc.co.uk/news-and-media/hsbc-uk-launches-new-voice-driven-technology (Accessed March 24th, 2021)

The reputational benefit for your entire business

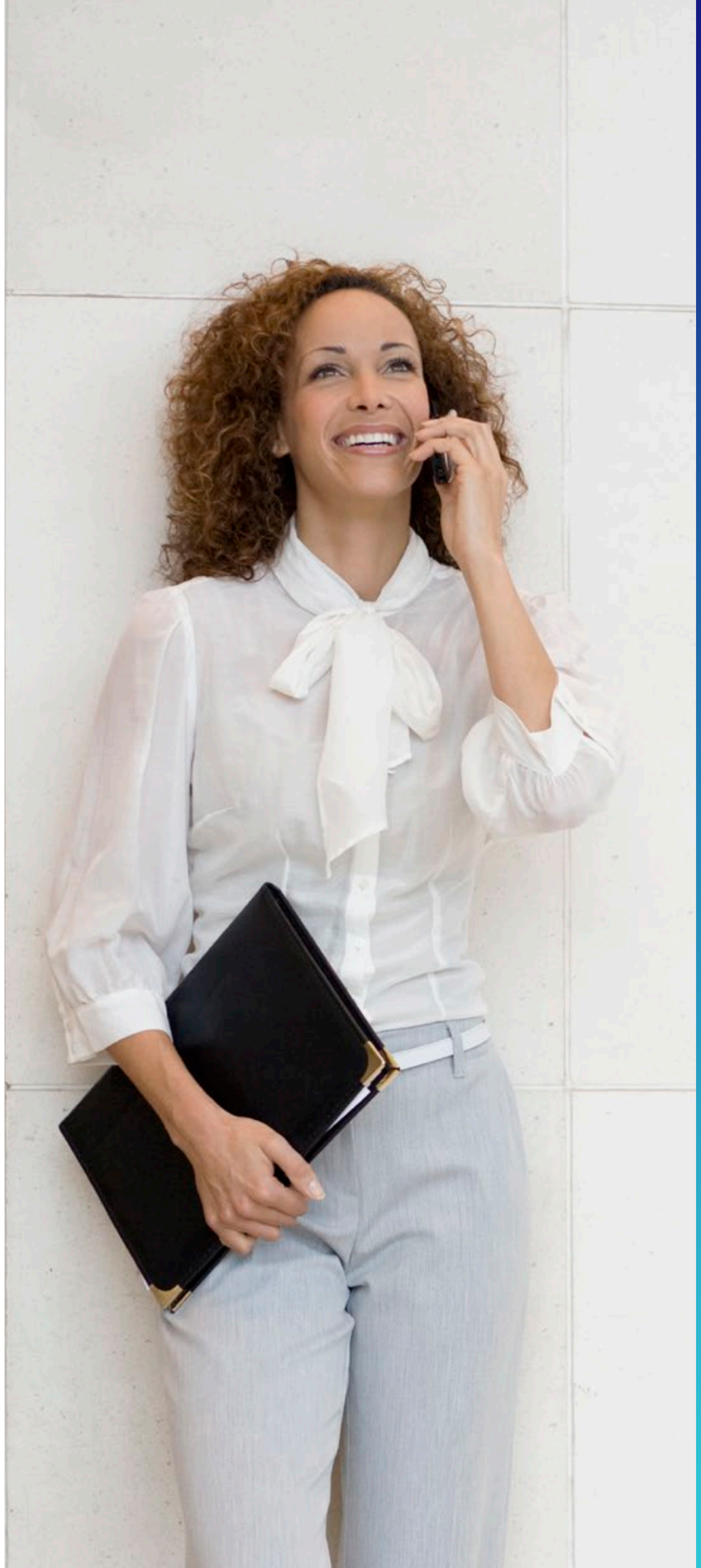
The introduction of voice authentication, or any other technology that improves fraud detection and prevention, bolsters your financial services institution's reputation, clearly signalling your brand's commitment to protecting its customers.

At the same time, it helps protect you against the reputational damage than can result from successful criminal attacks.

88%

of consumers say their perception of a business is improved when a business invests in the customer experience, namely security.[13]

[13] Experian 2020 Global Identity and Fraud Report



It's time to rethink authentication.

Together.

When authentication is painful for your customers and agents, it's painful for your business. Voice biometrics can help, especially when built into a multi-factor solution that provides a unified view of authentication—and fraud attempts—across all engagement channels.

As a customer experience leader, you're ideally placed to bring your colleagues in fraud prevention and your contact centre together to initiate a transformation that will ultimately help all of you to achieve your goals.

But you don't have to do it alone: Nuance is here to help you, just as we've helped so many other financial services brands.

LEARN MORE

Visit our website to learn more about Nuance's biometric authentication and fraud prevention solutions.

Discover why Opus Research named Nuance the "undisputed market leader" in its 2020 Intelligent Authentication and Voice Biometrics Intelliview.