call centre management association

Solving the Authentication Puzzle

March 2022

Supporting Partner

Pindrop®

A CCMA Research Initiative

A difficult trade-off

According to UK Finance, in the first half of 2021 more than £750m of bank customers' funds was lost to fraud, an increase of more than 20% over the same period in 2020[1].

The rapid growth of omni-channel customer service in recent years has benefitted customers but has also given bad actors new methods of gaining unauthorised access. Fraudsters are using ever more varied means, ranging in sophistication from brute-forcing to social engineering. Action Fraud counted 875,622 reports of fraud attempts in the 12 months from April 2020 through March 2021[2].

Protection from fraud is not the only reason why organisations might wish to prove a customer's identity. Accessing a customer's profile and contact history is often required to resolve a query. Customers who need dedicated support, for example, vulnerable customers, need to be flagged as such.

Every contact centre grapples with how to authenticate securely but at the same time minimise friction for the customer and (if in a phone or chat environment) the contact centre advisor.

On which side of this trade-off are contact centres landing? Is it possible to deliver an authentication experience that is both secure and seamless? To find out more, CCMA interviewed both industry leaders (via in-depth discussions) as well as consumers (via a structured survey).

Research methodology

This research comprised two distinct phases.

In the first phase, we held group discussions with contact centre leaders representing a broad mix of sectors, contact centre sizes and types.

In the second phase, n=1,016 online interviews were conducted with UK consumers from 10-17 February 2022. Quotas were set by age, gender and region to ensure a nationally representative sample. The composition of the sample was as follows:

Gender

Male	Female
490	511

Age groups

18-24	25-34	35-44	45-54	55-64	65+
111	175	187	183	155	205

Region

East Midlands	East of England	London	North East England	North West England	Northern Ireland	Scotland
82	85	141	42	113	31	92

South East England	South West England	Wales	West Midlands	Yorkshire & the Humber
141	91	53	52	93

[1] *https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/2021-half-year-fraud-report*
[2] *https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf*

With thanks to...

The CCMA and Pindrop extend their sincere thanks to all contributors for their generous participation in the study.

Iane Abad, Quality Assurance Team Manager, Financial Times

Andrew Allman, Senior Technical Director, ECR Risk & Solutions at Estee Lauder Companies

Dan Badham-Browne, Contact Development Manager, Norwich City Council

William Carson, Director of Market Engagement, Ascensos

Danny Clark, Head of Fraud Prevention. NewDay

Daniel Cotton, Head of Operational Innovation, Simply Business

Paul Ford, Head of Customer Services, Starling Bank

Ketan Hindocha, Quality, Compliance & Customer Resolutions Director, EE

Alan Mullen, Customer Service Manager, Superdry

Patrice Redhead-Smith, Customer Services Manager, Tower Hamlets Homes

Paul Whymark, COO, Sensée

Charity Wood, Head of Operational Excellence, Starling Bank

Foreword from CCMA

Whether it's trying to remember a 'memorable phrase' or waiting for a 'One Time Password' to arrive, every consumer is familiar with authentication.

Being the victim of fraud might seem like something that happens to other people, but as this research reveals, it's more widespread than you might think. Moreover, data from industry and government bodies shows that the rate of fraud or attempted fraud has accelerated since the pandemic.

In the contact centre we are constantly walking a tightrope. We absolutely must protect our organisations, our colleagues and our customers from the growing tide of fraud. And there are other good reasons why we might wish to identify customers who contact us. In some case it's simply not possible to resolve a query in the contact centre without knowing the customer's identity.

However, a clunky authentication process is bad for both customer and advisor, and it's bad for business as well – as this research shows. Moreover, it's not necessarily a given that a poor authentication experience equates to better security.

Is it possible to have a great experience that also protects? To help you answer this question, we present this research which brings together the view from the industry and the view from the customer.

Leigh Hopwood,
CEO, CCMA

Foreword from Pindrop

Unlike bygone days of meeting the local bank manager, contact centre advisors don't have any personal familiarity with callers, making authenticating a customer much more difficult, as well as potentially paving a path for fraudsters.

Every contact centre has tens of thousands of calls a day handled by hundreds of advisors. Their focus should be on providing excellent customer service, not identifying fraudsters or authenticating callers.

This research conducted by the CCMA shows that one in twelve people (9%) have suffered losses due to unauthorised account access and over a quarter (27%) of customers have become so frustrated with authentication processes, they've stopped doing business with that provider altogether.

The contact centres' need to strike the right balance between secure authentication and customer experience is crying out for a new way to authenticate quickly and seamlessly, so that the advisor can focus on providing top customer service rather than treating the caller like a potential fraudster. Clunky methods like knowledge-based authentication and one-time passwords are causing problems for customers, colleagues and businesses alike and are not doing enough to ensure security.

Recognising the need to adopt new authentication processes using passive technology powered by artificial intelligence (AI) and machine learning (ML) will be a vital next step for organisations looking to provide a personalised experience for their customers whilst protecting their security and privacy.

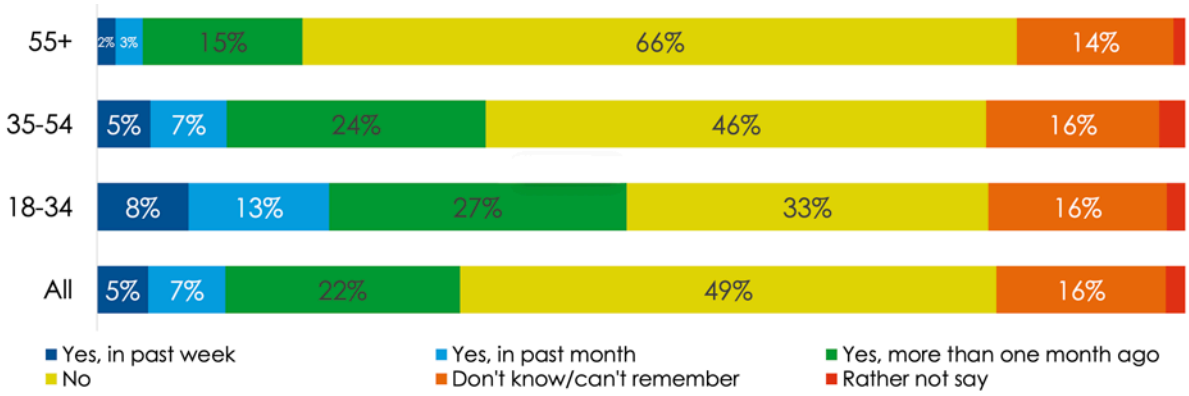
Amit Gupta,
VP of Product at Pindrop

How common is fraud?

One in three people have experienced an unauthorised access attempt.

Fraud might seem like something that only happens to other people, but our survey reveals that as many as 34% of UK adults aged 18+ have experienced an attempt by an unauthorised party to access their accounts. One in eight (12%) said they had experienced a fraud attempt within the past month.

Figure 1: *To your knowledge has anyone ever tried to gain unauthorised access to one or more of your accounts?*



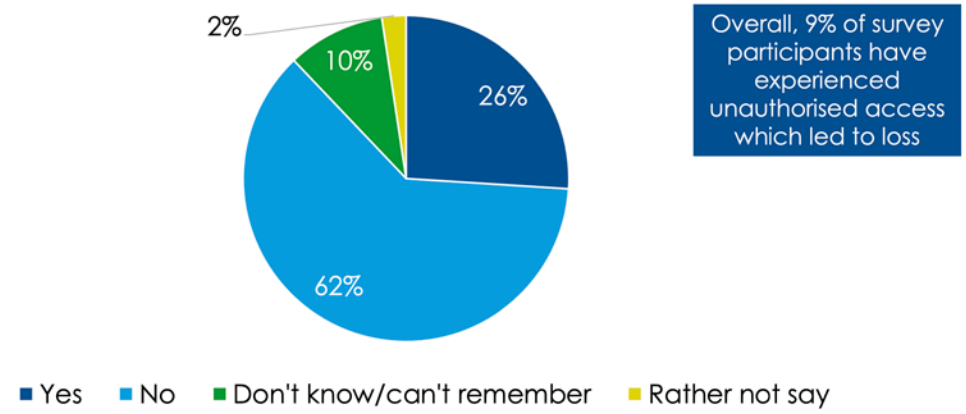
Base: All n=1,016, 18-34 n=286, 35-54 n=370, 55+ n=360

Among people aged 18-34 almost half (48%) said they had experienced an unauthorised access attempt, 21% in the past month. This may be related to a greater tendency for younger people to use the same passwords for multiple accounts, as evidenced later in this report.

Among those who have experienced an attempt at unauthorised access, one in four (26%) had suffered losses as a result.

Three in 10 people have used an assisted channel (phone or live chat) to restore account access within the past month.

Figure 2: *Have you suffered any losses to your knowledge, due to unauthorised access?*



Base: Have experienced an unauthorised access attempt n=339

As more channels become available for customers to interact with providers, there are more opportunities from fraudsters at all levels of sophistication, ranging from brute-forcing IVR systems to using confidence tricks on human advisors in the phone channel.

"We have fraudsters calling multiple times trying to get information. First to understand what questions we're asking. Then they will try to confuse our advisors and convince them to give away information." - Ketan Hindocha, Quality, Compliance & Customer Resolutions Director, EE

The push to deliver more functionality within self-serve channels places a greater onus on the need for security.

"We want customers to self-serve more, to be able to amend their orders. As we develop that we need to bring in more intricate authentication, because customers logging in will see lots more of their personal information." - Alan Mullen, Customer Service Manager, Superdry

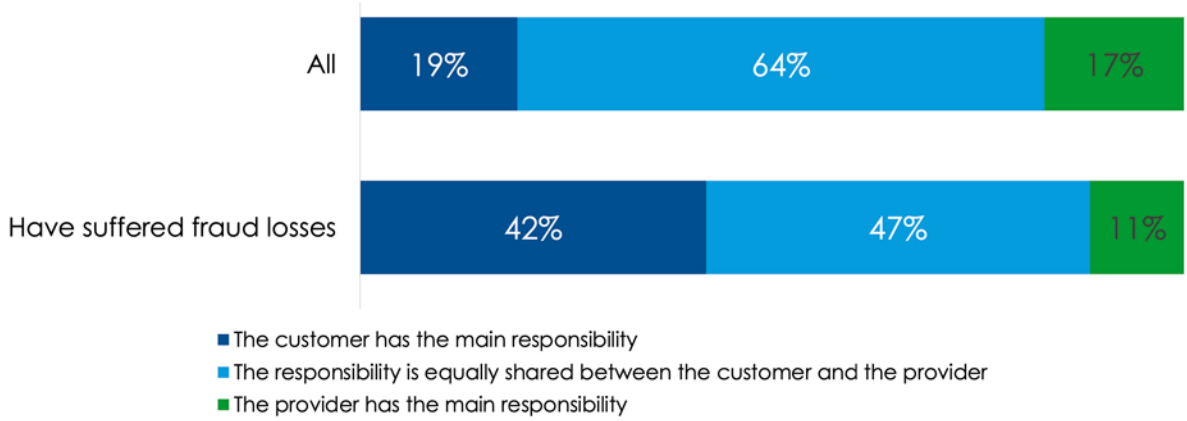
Protecting against fraud

Even when there have been no actual losses, unauthorised access damages customers' trust in the provider and in authentication processes.

"Fraud puts everyone on the back foot, the customer and the brand. That's what we're trying to avoid." - William Carson, Director of Market Engagement, Ascensos

The experience of fraud losses also changes customers' perception of personal responsibility. The majority of people surveyed (64%) believe that responsibility for preventing fraud is shared equally between the customer and the provider. However, as Figure 3 illustrates, those who have suffered losses to fraud are more likely to say the primary responsibility lies with the customer.

Figure 3: *Which of the following statements best describes your view when it comes to preventing unauthorised access to customer accounts?*



Base: Have experienced unauthorised access but not suffered fraud losses n=251, Have suffered fraud losses n=88

Naturally, while fraud victims may blame themselves, providers must continue to take their responsibilities very seriously. Different sectors face different types of fraud risks. Financial-services providers are among those with the most to lose and have some of the most highly-developed security processes, driven by regulation.

"PSD2 legislation mandates multi-factor authentication for online payments over a certain amount. That's driving fraudsters to telephony, which isn't regulated by PSD2." - Danny Clark, Head of Fraud Prevention, NewDay

For councils and other government or public-sector organisations, there are often reasons other than financial gain for bad actors to attempt to access others' accounts.

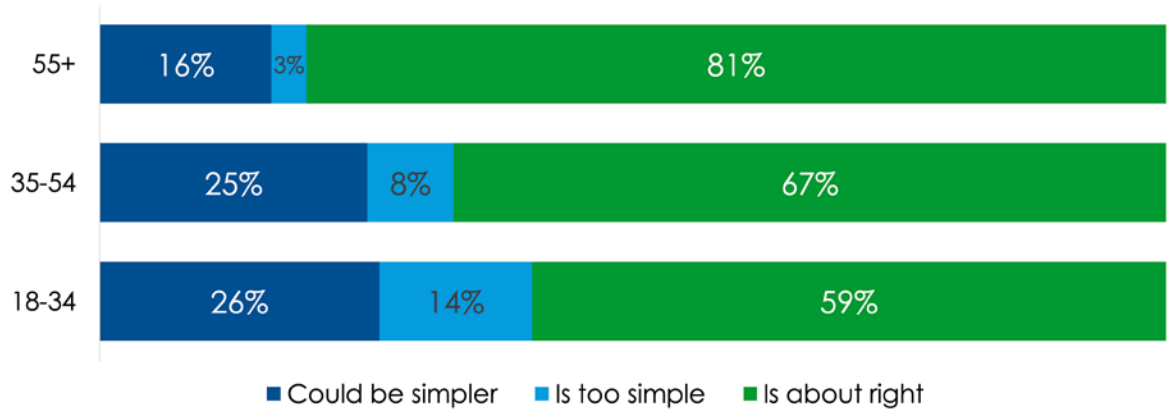
"We get people trying to track down ex partners, potentially victims of domestic violence." - Dan Badham-Browne, Contact Development Manager, Norwich City Council

"If there is a leak, for instance, coming from the flat upstairs, the resident downstairs may pretend to be the resident upstairs, because they want to find out what's happening with the leak." - Patrice Redhead-Smith, Customer Services Manager, Tower Hamlets Homes

Reducing friction in authentication

Authentication has become an accepted part of modern life. The majority of people participating in the CCMA survey felt that the authentication required to access their accounts was 'about right'. However, as Figure 4 illustrates, while four in five (81%) of those aged 55+ say that their authentication experience is 'about right', younger people are more likely to want simpler authentication. One in four (26%) of those aged 18-34 and a comparable proportion of 35-54s (25%) say that authentication 'could be simpler'.

Figure 4: *Overall, would you say that the authentication that you are required to undertake to access your accounts...*



Base: 18-34 n=286, 35-54 n=370, 55+ n=360

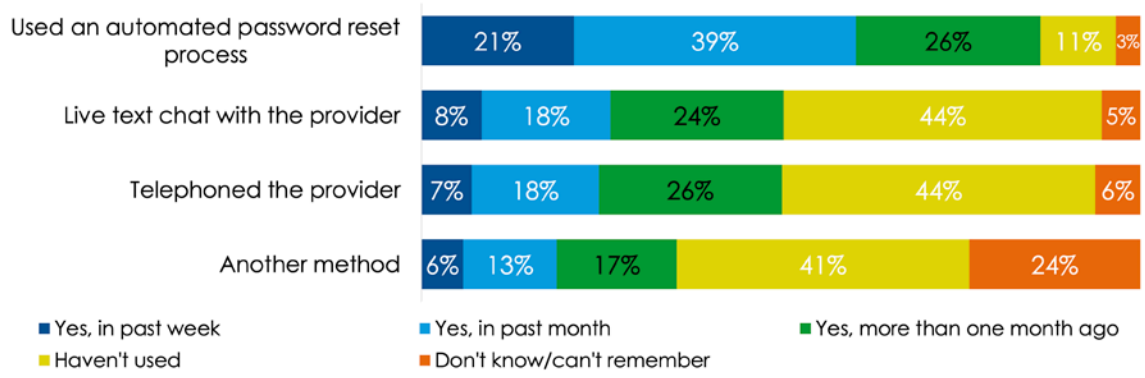
Despite the generally positive ratings for the authentication experience, failure to authenticate is not uncommon. More than half (58%) of consumers we surveyed reported they had been locked out of an account in the past year.

Over half (58%) of consumers have been locked out of an account in the past year. One in three (33%) had been locked out of an account within the prior month.

After being locked out, an automated password reset process is the most commonly-used method of restoring account access. However, as Figure 5 illustrates, half of those who were locked out have turned to live chat and another half have telephoned the provider. There can be no doubt that authentication creates a significant amount of demand into the contact centre.

Three in ten people have used an assisted channel to restore account access within the past month.

Figure 5: *Which of the following methods have you used to restore access after being locked out of your account?*



Base: Have been locked out of account n=702

To understand the demand volume that failed authentication generates, it is helpful to create a 'reason code' linked to authentication. Tracking this over time will help to diagnose the impact of initiatives such as changing authentication methods.

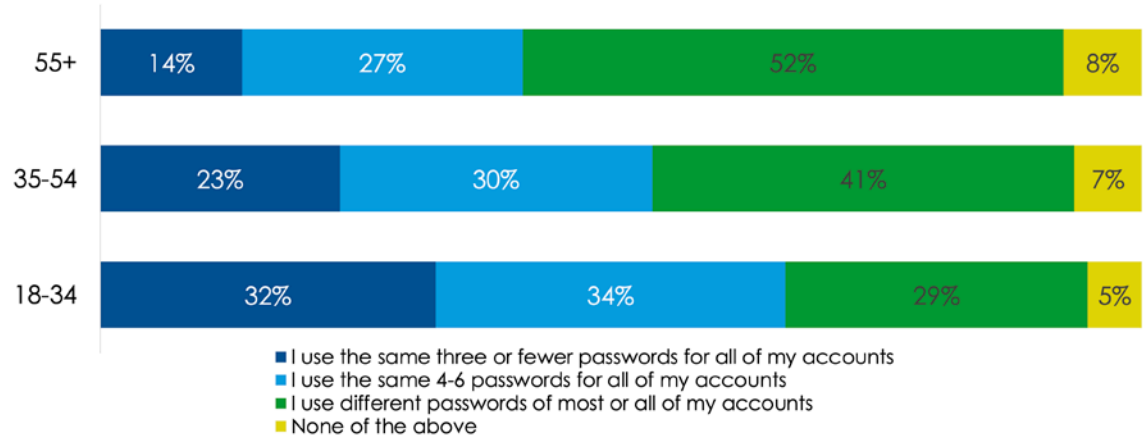
"Sometimes I have been asked for a password, but I don't even recall setting a password up. If a phone password is required to be set up when creating an account, then it should be clear when this password might be used, and that it should be noted by the user for future reference. Especially if this password is different from an online password used with the same organisation." - A consumer

"Setting passwords is becoming more and more complex with a page of rules. Can't be one you've had before, 8 letters, a capital, symbol and number. Can't ever remember these."
- A consumer

Perhaps not surprisingly, the frustration of failed authentication can drive people to search for simpler options. As observed earlier, the desire for simpler authentication is especially strong among younger people.

As shown in Figure 6, younger people tend to use fewer passwords. One in three (32%) of those aged 18-34 say they use three passwords or less in total across all their accounts, compared with 14% of people aged 55+. Another third (34%) of those aged 18-34 say they use between 4-6 passwords for all their accounts.

Figure 6: *Which of the following best describes your approach to passwords?*



Base: Male n=490, Female n=511, 18-34 n=286, 35-54 n=370, 55+ n=360

22% of people say they use three or fewer passwords for all their accounts.

Getting the balance wrong is bad for customers, colleagues and business

Most contact centres are constantly evaluating their authentication methods and exploring new approaches to find the balance between security and a painless experience.

"There lies the rub. You have to ensure authentication is as close to 100% accurate as it can be. But if you do that to the point that you're pushing your customers away, then you're losing revenue and customer base. Where is that fine line between a degree of risk that you're comfortable with, through to successful customer satisfaction and retention?" - Paul Whymark, COO, Sensée

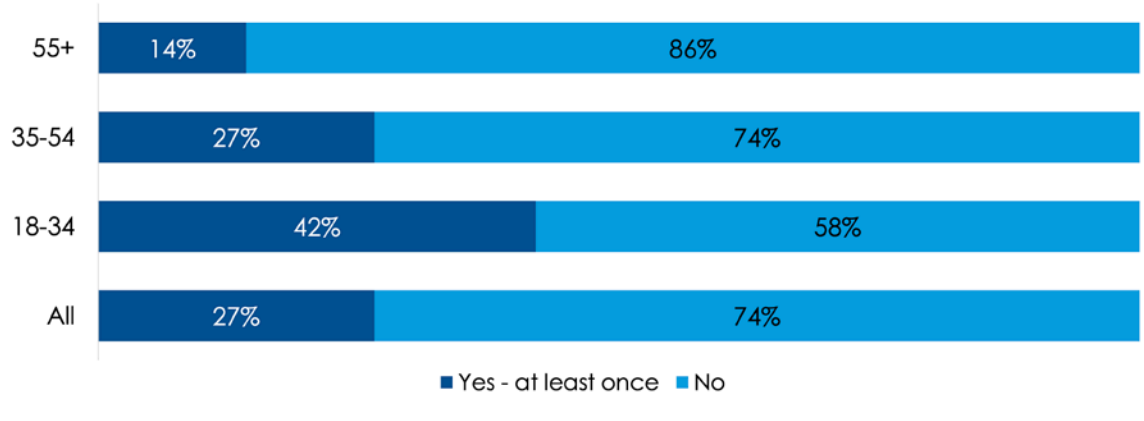
"It's the balance between how many will it help versus how many it won't help." - Ketan Hindocha, Quality, Compliance & Customer Resolutions Director, EE

Our survey provides concrete evidence of the relationship between authentication experience and customer loyalty.

Younger customers are particularly likely to vote with their feet, as Figure 7 shows. 42% of those aged 18-34 have switched away from a provider due to authentication problems.

27% of customers have stopped doing business with a provider due to authentication issues.

Figure 7: *Have you ever stopped using a provider because their authentication methods were too difficult or because of the way they handled an authentication issue?*

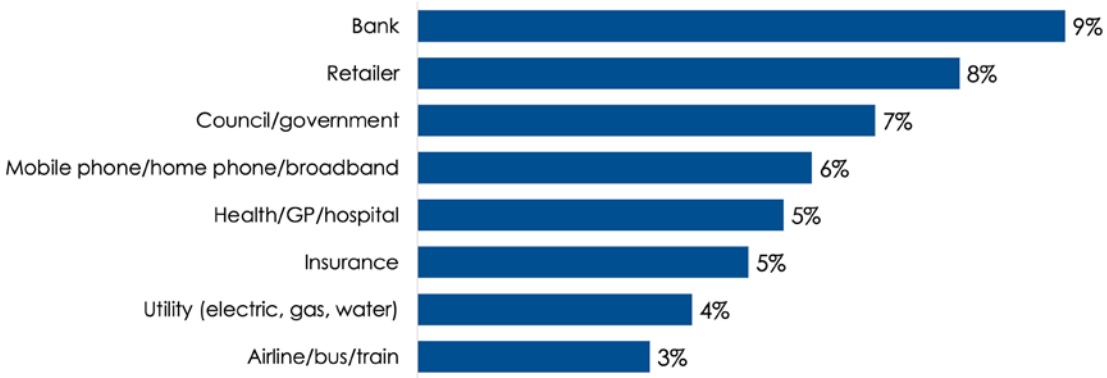


Base: All n=1,016, 18-34 n=286, 35-54 n=370, 55+ n=360

Figure 8 shows that 9% of those surveyed said they had switched banks and 8% said they had stopped buying from a retailer due to a poor authentication experience.

"An app for a bank I used to have an account with had three methods of entry all of which had to be completed, one being password and one being secret word. I constantly got confused between when to use the password and when to use the secret word, and it did my head in. I switched banks. The bank I then switched to required a small device to generate a number before gaining access to the mobile app. I switched away from them as well!" - A consumer

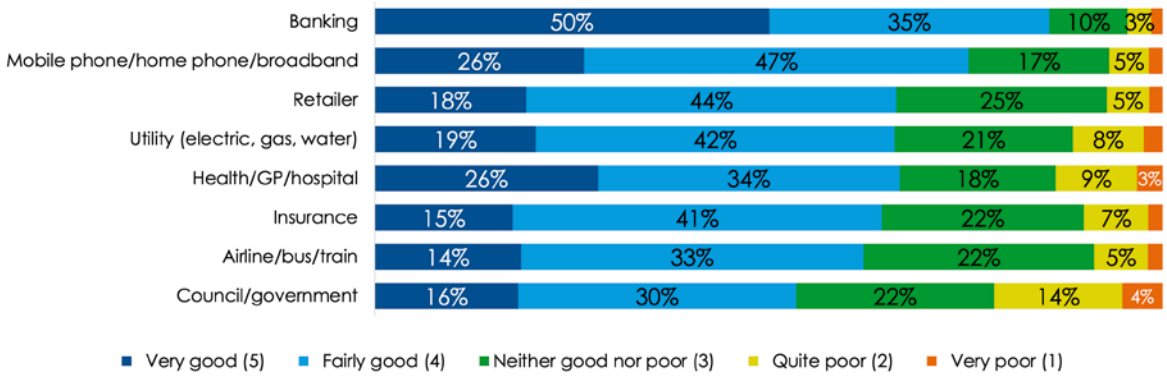
Figure 8: *Have you ever stopped using a provider because their authentication methods were too difficult or because of the way they handled an authentication issue?*



Base: n=1,016

Despite banks having the highest churn rates due to authentication issues, they also receive the most positive ratings for authentication experience. 50% of those surveyed rated bank authentication 'very good' and a further 35% rated bank authentication 'fairly good'. The least favourable ratings are given to councils and government departments, as shown in Figure 9.

Figure 9: *On a scale of 1 to 5, where 5 equals 'very good' and 1 equals 'very poor', generally speaking how would you rate the experience when authenticating your account with each of the following types of organisation?*



Base: n=1,016

How can it be that banks and retailers receive relatively positive ratings for their authentication yet experience the highest churn due to authentication problems? This may be attributed to the low barriers to switching in these sectors, meaning it is especially critical for these organisations to deliver a good authentication experience.

Within assisted channels a poor authentication experience not only frustrates the customer but also affects the advisor, who is forced to deal with an aggrieved customer or cope with the stress of complex authentication processes while the customer is waiting on the line. This includes advisors themselves needing to authenticate into systems, as well as helping customers to authenticate.

"Particularly with the move to working from home, authentication processes have created challenges for advisors. We've got quite a lot of third-party applications, payments for example. One of our payment systems has got a 30-minute log-on window. So my team in an eight-hour shift has to authenticate 16 times a day to log back in. We are resolving this through single sign-on but consideration is needed for the new way of working."

- Alan Mullen, Customer Service Manager, Superdry

"Yesterday one of my staff came into the office with a broken phone charger. He couldn't log into anything, because all the authentication was done through the phone. He had to come in and work in the office." - Alan Mullen, Customer Service Manager, Superdry

Contact centres are responding to the rise in fraud attempts by ramping up the training provided to advisors.

"How do we ensure our guys are well set up to support the customer through authentication, but also are able to spot a fraudster? Can they tell when someone is trying to pull the wool over our eyes?" - Paul Ford, Head of Customer Services, Starling Bank

"We're focus on the training element to ensure that there's an opportunity for the advisor skill-set mindset and also the tool-set to be aligned around the experience for the customer." - William Carson, Director of Market Engagement, Ascensos

Authentication within the voice channel

Within the phone channel there are specific challenges to consider when implementing authentication. Advisor-administered authentication introduces the possibility of human error and of social engineering by fraudsters.

"As a digital bank our customers primarily self-authenticate. When a customer comes to a mediated channel for support and an advisor needs to become the authenticator, balancing customer experience and fraud prevention is critical and we are constantly reviewing this. "
- Charity Wood, Head of Operational Excellence, Starling Bank

Achieving an acceptable compromise between secure authentication on the phone and AHT (Average Handling Time) is top of mind.

"You don't want a long drawn-out authentication. And then the part that they're ringing up to inquire about is less than the time they took to validate."
- Patrice Redhead-Smith, Customer Services Manager, Tower Hamlets Homes

"ID and V (identity and verification) typically takes about 20-25 seconds. It's transactional, a part of the call that doesn't add value. On a three to four-minute call, eliminating that gives seven to ten per cent return. Most Operations Directors would give their right arm for a seven to ten per cent FTE reduction." - Paul Whymark, COO, Sensée

"We have examples where we have simplified the customer validation process to make it more straightforward for agents to comply. We used to think that tailoring the questions to the scenario was optimal but we learned that it added complexity and was harder for agents to follow a compliant route." - Ketan Hindocha, Quality, Compliance & Customer Resolutions Director, EE

Using outbound return calls to authenticate is one solution, although not foolproof in the event that a fraudster has obtained a stolen phone or SIM.

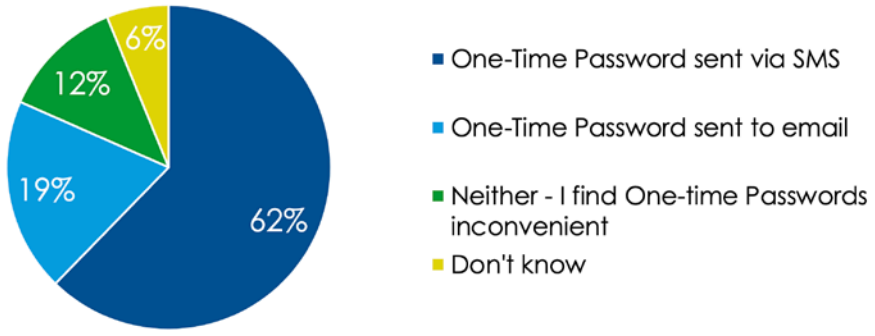
"The financial brands have nailed this. They tend to call you back, just to make sure it's you that they're speaking to. But sometimes advisors can literally forget to authenticate during the call-back as both they and the customer have just been speaking with one another." - Ketan Hindocha, Quality, Compliance & Customer Resolutions Director, EE

One-Time Passwords: the magic bullet?

Thanks to regulators mandating them for online banking, OTPs are now familiar to many of us and have gained substantial traction in non-financial sectors as well.

Our survey shows that OTPs have become widely accepted, with just 12% of people saying that they find OTPs inconvenient. As shown in Figure 10, preference for OTPs via mobile outstrips that for OTPs via email. This is likely due to familiarity with SMS-based OTPs, which are more common today than OTPs via email.

Figure 10: *A 'One-Time Password' is commonly used as an additional authentication method. Which of the following methods would you prefer if given the choice?*



Base: n=1,016

SMS-based OTPs are far from frictionless, as comments from our consumer survey point out.

"At work I get no mobile signal, so getting texted a one-time code with no other option is a pain."
- A consumer

"Providers should always allow registering both email and phone two-step authentication, since sometimes you change phone number and can't access your account." - A consumer

One major limitation of OTPs is that they can be difficult for customers while they are using their mobiles to ring the contact centre. Well suited to self-serve channels, there is evidence that they are much less suited to assisted interactions.

"It is so difficult accessing accounts using my mobile when the one-time code is also sent to my phone. It's extremely frustrating and I hate it."
- A consumer

We used to think that the contact centre channel needed identical validation methods to the digital channel. We learned that customers often need to be treated differently if they call us. Phone is often the route that customers try after failing to self-serve. Hence two-factor for contact centres isn't the route we are going down at the moment. We are evaluating biometric and other means to improve security without the friction."
- Ketan Hindocha, Quality, Compliance & Customer Resolutions Director, EE

"For the majority of our residents English is not their first language. Getting through an IVR is already challenging. Getting them to do a one-time password would be really quite difficult." - Patrice Redhead-Smith, Customer Services Manager, Tower Hamlets Homes

Tiered authentication levels

Some organisations use a standard authentication process for all queries, whereas others implement different ones based on the risk level associated with each query or channel.

"It's a tiered approach based on the risk. We try to serve as many calls within the IVR and self-contain there as much as possible. That's relatively light in terms of authentication. What you find is that some of that information is valuable to a fraudster. They can use that as a method of gathering data to use in the phone channel for I,D and V which is why we introduced one-time passcode via email and SMS."
- Danny Clark, Head of Fraud Prevention. NewDay

We do the same authentication across the board. For sure there could be heightened levels of authentication for certain types of transactions. Our challenge, particularly on an inbound basis, is that we don't always know why the customers are calling us. You can use an IVR decision tree for intent capture, but the reason they're calling and the actual outcome could be quite different."
- Daniel Cotton, Head of Operational Innovation, Simply Business

"Sometimes we don't force people down an authentication route at all. If someone's reporting fly-tipping, we'd like to know who they are so we can feed back to them. But ultimately, if we force them down that route, are they going to do what we want them to do? If the risk is minimal, if we're not talking about financials or sensitive data, we'll give them a choice to authenticate or do it entirely anonymously." - Dan Badham-Browne, Contact Development Manager, Norwich City Council

Some contact centres have landed on full authentication up front as the best approach for both customer and advisors in the phone channel, as opposed to re-authenticating during a call.

"We used to have step-up validation, 'low' and then 'high. Just name, address and postcode to start with allowing advisors to complete certain activities, but not high-risk ones. But that's a poor experience because the advisor hits a barrier and then can't do the next activity until they have re-validate the customer to 'high'. And the customer gets frustrated. So I've removed 'low' for most situations. All customers are fully validated at the start of the call, investing a bit in AHT, giving a better customer and colleague experience and it's safer." - Ketan Hindocha, Quality, Compliance & Customer Resolutions Director, EE

Considerations when implementing new authentication solutions

As self-serve functionality grows and fraud attempts rise, authentication is very much in the spotlight with contact centres continually seeking to upgrade their capabilities.

"Authentication is something that's continuously reviewed. It's not like 'we've fixed it, let's move on.' We're constantly asking, does it work for the agents? Is it still doing what it needs to do to protect the customer?" - Paul Ford, Head of Customer Services, Starling Bank

Another significant barrier to improvement in some organisations is data fragmentation. Authentication relies on the ability to connect contact events to a central database of customer information, which for some organisations does not yet exist.

"Historically, we've run on legacy systems that aren't built to share information. We're gradually moving away from that. Every system has an entirely different way of managing that data. Our biggest challenge is getting to a point where our data is good enough to be reliable."
- Dan Badham-Browne, Contact Development Manager, Norwich City Council

Most contact centre platforms have authentication built in, but should there be a wish to use a separate authentication system, integration is required.

"Our telephony platform is outsourced to a third party and you need to open the doors at that third party to deploy." - Danny Clark, Head of Fraud Prevention, NewDay

As the push for additional capabilities grows there is a risk of creating complexity for both customer and colleague, especially as channels proliferate.

"We've grown quite quickly and we've added things over time. As authentication becomes more critical there is more for the advisor to have to deal with." - Alan Mullen, Customer Service Manager, Superdry

Platform upgrades provide an excellent opportunity to review authentication. Conversely, when upgrading authentication there is an opportunity to review business needs and customer journeys.

Collaboration with customer experience and product teams is an important success ingredient, and wherever possible involving customer-facing colleagues and even customers themselves in the upgrade process will help ensure the solution delivers the required experience.

> ***"First we'll speak to the agents to understand what the challenges are there. That brings it to life."***
> - Paul Ford, Head of Customer Services, Starling Bank

"We're starting to bring our customers into that discovery journey and say, you know, how did it work for you, what feels right, what's tolerable? You know, we want them to use the services and interact with us as much as possible. They're far more involved than before." - Dan Badham-Browne, Contact Development Manager, Norwich City Council

Within organisations it is not uncommon for the contact centre leader to find themselves championing the customer and colleague authentication experience in the face of pressure from other teams, for example to introduce more complex authentication for compliance purposes. Finding a path that satisfies all requires empathy and delicate stakeholder management.

5 discoveries for solving the authentication puzzle

1. The authentication need may be quite different by channel, journey or customer mission, but sometimes a universal solution can be the most efficient.
2. Systems and channel proliferation can create an inconsistent and disjointed authentication experience.
3. 'Reason codes' related to authentication help track the impact of changes.
4. Compliance teams should be the contact centre's friend, not adversary.
5. Authentication experiences affect colleagues as well as customers, and both groups' input can be extremely valuable to the development process.

Join us!

Not a member?

There is no better time to join us. The industry is changing and we are giving our members more opportunities to learn, to network and to support each other.

www.ccma.org.uk/membership

call centre management association

0333 939 9964 | www.ccma.org.uk

@ccmatalk | info@ccma.org.uk