call centre management association

Balancing fighting fraud with customer experience

October 2023

Supporting Partner

smartnumbers

A CCMA Research Initiative

Is it possible to minimise friction while maximising protection?

According to UK Finance, in 2022 £1.2bn was lost by UK consumers to fraud.[1]

Every contact centre must implement security measures to identify and protect genuine customers, and flag potentially fraudulent attempts to access customer accounts. Most authentication methods currently in use necessitate a certain amount of 'friction' that impacts the experience not only for customers but also the front line. Friction in authentication increases handle times, reducing productivity.

Minimising journey friction is one of the sacred mantras of customer and colleague experience, but the most frictionless method on offer (no authentication at all) is not an option. And even the best authentication cannot defend against sophisticated scams that persuade genuine customers to hand over money.

To understand how fraud is evolving and what contact centres are doing to stay ahead of fraudsters, CCMA conducted this research supported by Smartnumbers, which gathers perspectives from both industry leaders and from consumers.

Research methodology

This research comprised two distinct phases. In the first phase n=1,001 online interviews were conducted with UK consumers from 8-17 August 2023. Quotas were set by age, gender and region to ensure a nationally representative sample.

In the second phase, we shared findings from the survey in discussion with contact centre leaders who provided commentary and context.

With thanks to

We invited contact centre leaders representing a diverse mix of industries, contact centre types and experiences to a series of discussions to explore the themes uncovered in the consumer survey. The CCMA and Smartnumbers extend sincere thanks to these individuals for their generous participation in the study.

Jon Bowen, Director of Operations, Paymentshield & Lloyd Latchford

Nick Edge, Head of Fraud Technology, Likewize

Sean Gilholme, Head of Customer Service, Atom Bank

Ben Lyons, Vice President, Banking Operations, Chase UK

Craig McKeever, Fraud Analyst, Optimus Cards UK

Amanda Robertshaw, Senior Operations Manager – Fraud & Disputes, NewDay

Janet Scott, Business Change Manager, AIB (Allied Irish Bank)

We also invited **Matt Smallman**, author of 'Unlock Your Call Centre' to offer his thoughts on the research findings and are delighted to feature his comments in this report.

[1] https://www.ukfinance.org.uk/data-and-research/data/fraud

Foreword by CCMA

As I unfortunately discovered over the summer, fraud is not something that only happens to other people. Anyone can become a victim, and it's easy to be apathetic about fraud until it actually happens to you.

For this reason, this research is of special personal relevance. Since my own experience I've gained a far better understanding of both sides of the tricky balance that contact centres must achieve. Like every consumer, I want my contact experiences to be easy, quick and painless. In the past I didn't pay too much attention to my security settings and I was easily frustrated by clunky authentication methods. But today I'm now much more aware of the role that I play in protecting myself, and how hard it is for organisations to defend against the ever-changing and increasingly elaborate techniques used by fraudsters.

I was struck by the counter-intuitive observation contained in this report that in some circumstances, there can be such a thing as too much awareness of fraud. Publicly raising the alarm can tip off fraudsters to change their methods, and if you're in the insurance industry it can lead to a spate of unwanted claims. But for contact centre professionals there can only be benefits to sharing useful knowledge and experiences around this fast-moving topic, which this report does in spades.

Leigh Hopwood,
CEO, CCMA

Foreword by Smartnumbers

The impact of fraud is alarming, affecting millions of people and costing the UK alone almost £7bn annually, accounting for 40% of all crime. More worryingly for CX professionals is the fact that 61% of fraud is connected to the contact centre, and as such, the need to balance multiple controls versus the customer's journey has never been so challenging.

The growth in fraud is happening at a time when more customer interactions are happening remotely, promoting the need to identify people that you have never met. While cyber security has started to address this for digital channels, it has meant that fraudsters have altered their aim and now target more vulnerable channels; the contact centre and customers themselves.

It's therefore no wonder this report shows that in 2023, 36% of consumers have experienced unauthorised account access attempts. Yet, despite us all knowing we shouldn't make life easy for fraudsters, nearly a quarter of us still only use less than three passwords across all our accounts.

It succinctly highlights the challenge that contact centres and our colleagues are facing.

Moving forward we must collectively adopt behaviours that prevent fraud and improve the identification of consumers.
AI-powered technology plays a key role in helping with this challenge, enabling us to identify the first signs of fraudster reconnaissance to create a world where security and customer experience harmoniously coexist.

We hope this report sparks insightful conversations and incites innovative solutions to propel our collective journey to fight fraud.

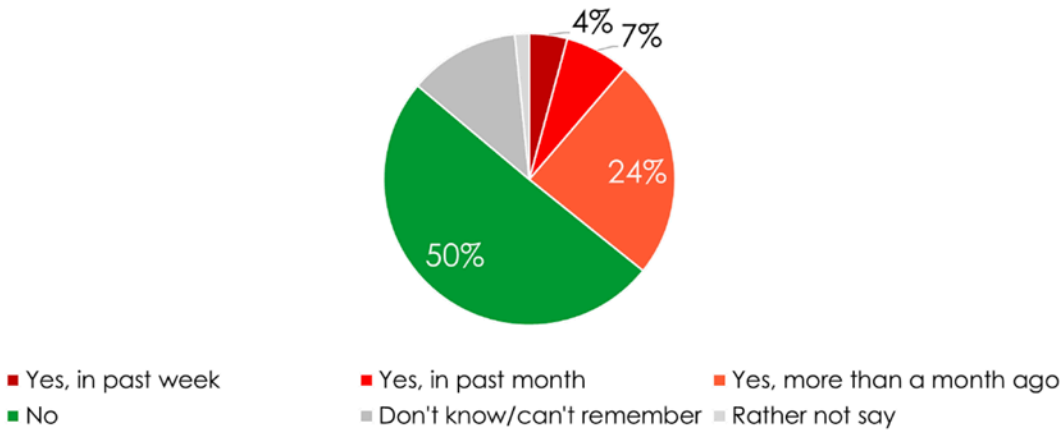
Matthew Addison,
CRO, Smartnumbers

Customer experience of fraud

36% say they have been the victim of a fraud attempt, up from 33% in 2022

According to CCMA's consumer survey and as shown in Figure 1, 36% of people in 2023 reported having experienced an unauthorised attempt to access one or more of their accounts. This is a slight increase over the 33% reported in an earlier CCMA survey, published in March 2022.

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



Base: All (n=1,001)

The customer is the weakest link

According to UK Finance 'authorised push payments' (where a victim is tricked into sending money to a fraudster) comprised 40% of all fraud losses in 2022. Also known as 'coercion', first-party fraud (committed knowingly or unknowingly by genuine customers) is expected to increase as self-serve customer journeys become increasingly commonplace.

Fraudsters are experienced in using emotive and behavioural hooks, putting pressure on the victim to make a decision or take action on the spot.

" Fraudsters will impersonate the fraud team and make customers panic. 'You're about to lose all your money. We need to move your money to a secure account.' If customers say 'why would my bank ever need me to move the money myself?' they will say 'you haven't got time and every second counts" - Craig McKeever, Fraud Analyst, Optimus Cards UK

" If the fraudster has convinced them it is a genuine activity, [as a provider] navigating through that is really difficult. When asked 'do you know what you're doing?' and 'was it you?', the customer answered yes. It's a real test when you're presented with the real customer and they are convinced they are doing the right thing."
- Jon Bowen, Director of Operations, Paymentshield & Lloyd Latchford

" Today, there are instances of fraudsters working with behavioural scientists. They're getting very clever at being able to pull on heartstrings."
- Ben Lyons, Vice President, Banking Operations, Chase UK

Growing sophistication means even savvy customers are at risk. Fraudsters are increasingly adept at obtaining customer details and impersonating legitimate brand representatives.

Some types of fraud are committed not by strangers but by friends or family.

" We see customers where family members will use their policy to claim and they're not even aware of it. They share passwords and login details, sometimes knowing that it will be used for fraud, and sometimes due to naivetë." - Nick Edge, Head of Fraud Technology, Likewize

Younger people especially vulnerable to online scams

Conventional wisdom might suggest that older people are particularly vulnerable to fraud and social engineering, but this is counter-balanced by the growth of various kinds of digital fraud to which younger people are especially susceptible. UK Finance data shows a 33% increase in fraud losses attributable to mobile phones in 2022 compared with 2021.[2]

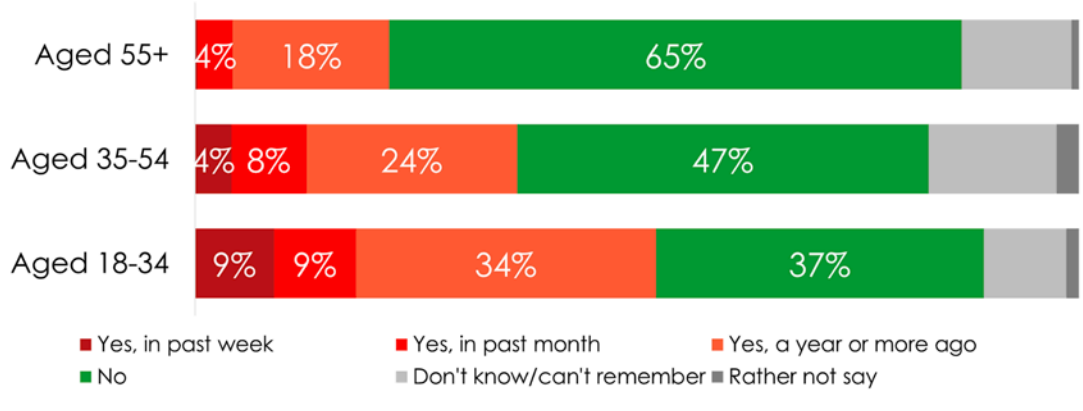
" With deepfakes, I wonder if it's going to be younger, more digitally-enabled consumers that are more easily targeted. - Ben Lyons, Vice President, Banking Operations, Chase UK

"As fraud methods become more sophisticated and more digital, you almost start to lock out some of the older generation." - Jon Bowen, Director of Operations, Paymentshield & Lloyd Latchford

" During the pandemic, there were a lot of younger people being caught in crypto scams and investment scams. And we've seen students targeted to become money mules. 'Get rich quick' is particularly appealing if you don't have much money." - Craig McKeever, Fraud Analyst, Optimus Cards UK

As well as being more likely to be exposed to digital fraud, Figure 2 shows that younger people are also more likely to say they have experienced an unauthorised attempt to access their accounts.

Figure 2: *To your knowledge has anyone ever tried to gain unauthorised access to one or more of your accounts?*



Base: 18-34 (n=280), 35-54 (n=365), 55+ (n=355)

52% of people aged 18-34 say they have experienced an unauthorised access attempt, compared with 22% of over-55s.

[2] https://www.ukfinance.org.uk/data-and-research/data/fraud

Staying ahead of fraudsters

Key to detecting fraud attempts is the ability to spot unusual patterns. This is accomplished both by humans on the front line who are trained to pick up cues, as well as automated analytics applied to behavioural data. As coercion becomes increasingly common, security systems must not only guard against bad actors impersonating customers, but also help genuine customers protect themselves from scams.

" We train the team to spot when you're hearing doesn't fit. If the policy is registered to a 76 year-old and the person who's speaking to you sounds like they're in the middle of running the marathon or about 21, flag it." - Jon Bowen, Director of Operations, Paymentshield & Lloyd Latchford

" It puts more of an onus on behavioural monitoring, transaction monitoring. Your focus is on identifying things that are out of the ordinary, for example someone who previously has not been flagged but is starting to behave in a way that's not in line with their history." - Sean Gilholme, Head of Customer Service, Atom Bank

Whether building and implementing analytics or rolling out training for the front line, operationalising and scaling security can be a complex task for organisations that serve multiple jurisdictions and/or with heterogeneous product lines and customer segments. What works for one group and in one market may not work for another.

" If you operate contact centre teams in different countries, for example from an outsourcing perspective, there are contextual and cultural considerations to take into account when it comes to identifying fraud. The types of fraud that happen in the UK aren't necessarily the same types of fraud that you might see in other countries and territories. You've got to make sure your model can be adopted by the different operational teams on the ground." - Ben Lyons, Vice President, Banking Operations, Chase UK

Need to challenge genuine customers can create a conflict for the front line

The rise of first-party fraud (genuine customers caught in scams) creates a communication and cultural challenge for the contact centre front line who are required to put up barriers and even raise the alarm on potentially fraudulent behaviour.

" Because we work in a [fraud] department where we're effectively calling people out and challenging them, we can be a little bit more authoritative than our contact centre colleagues. And I don't think it's fair on the other advisors to have those challenging conversations because it puts them in an awkward position." - Nick Edge, Head of Fraud Technology, Likewize

" We've spent years training our frontline teams to take ownership of the customer and go the extra mile. It was all about fast resolution. As fraudsters become more sophisticated, you have to design processes differently (for example with secondary reviews). This creates a new challenge in regard to building brand sentiment for frontline colleagues, when we build processes where more and more has to be checked and this can take longer for customers." - Ben Lyons, Vice President, Banking Operations, Chase UK

Even in straightforward cases, the need to handle authentication not only adds to handle times but to the cognitive load experienced by the front line. This represents a powerful use case for automation.

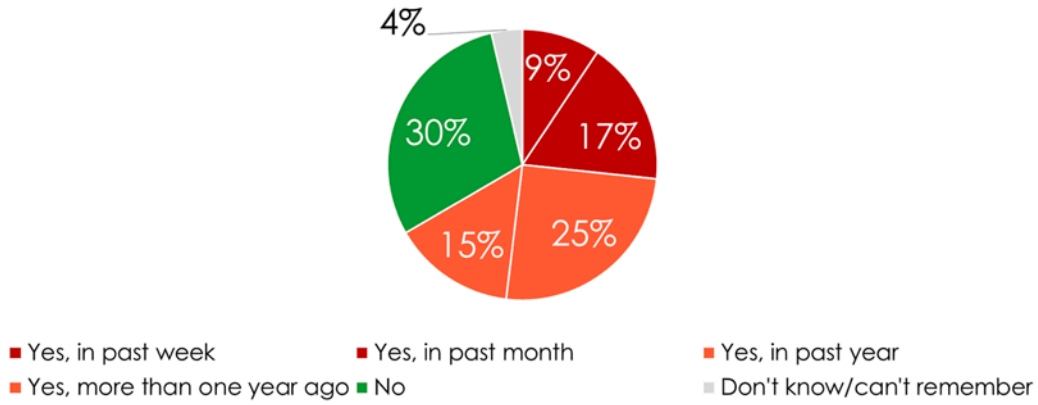
" My team would love to see a chatbot which could manage certain elements of authentication up front. It can be monotonous for staff having to ask customers the same questions on each call. - Janet Scott, Business Change Manager, AIB (Allied Irish Bank)

Getting the balance right

The trade-off between security and friction is a delicate one. Too much friction annoys customers and leads to complaints both directly to the provider and posted on social media, affecting the provider's reputation.

One of the most obvious types of friction that consumers experience is the need to remember and enter passwords. Figure 3 shows that more than one in four consumers (27%) in CCMA's survey reported having been locked out of an account in the past month alone, due to a password problem.

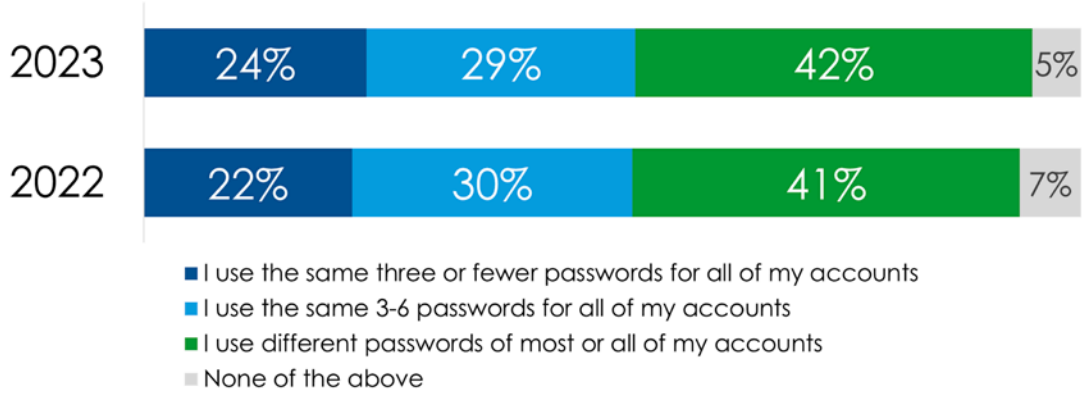
Figure 3: *Have you ever been locked out of accessing an account due to not being able to get through authentication, for example forgetting your password or memorable phrase?*



Base: All (n=1,001)

One of the most widely-recommended steps for consumers to help secure their accounts is to adopt multiple passwords. Despite reminders to do so being built into many account-opening journeys, Figure 4 illustrates that behaviours have remained largely unchanged since 2022. This underscores how difficult it is to convince people to accept friction.

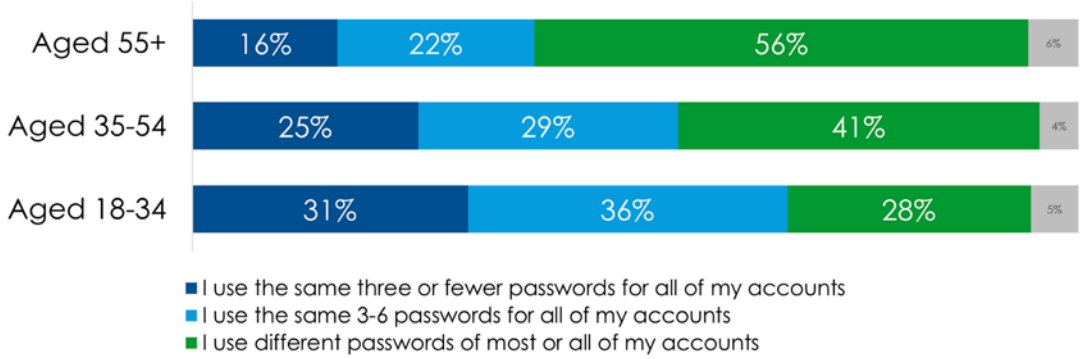
Figure 5: *Which of the following best describes your approach to passwords?*



Base: All (n=1,001)

Younger people tend to use fewer passwords as shown in Figure 6, which suggests they are especially intolerant of friction.

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



Base: 18-34 (n=280), 35-54 (n=365), 55+ (n=355)

Friction is in the spotlight thanks to Consumer Duty

The introduction of Consumer Duty regulations has placed the concept of friction front and centre, and has inspired in many organisation a wholesale re-engineering of processes and journeys with the elimination of 'sludge practices' being a key focus.[3] This promises to be a hugely positive step forward for customers.

However, organisations should be mindful of the difference between sludge practices and necessary friction.

" When I started my career, you'd never design a process for the exception. It was always designing the process for the majority of customers (the happy path), then dealing with the exceptions as they flow through. From a Consumer Duty perspective, that's changing because we have to almost design for every eventuality up front, which is a good thing for consumers." - Ben Lyons, Vice President, Banking Operations, Chase UK

" Consumer Duty is putting a much greater onus on the ability to prove that you're doing what you're doing through the data and the analytics that you undertake. And I think a positive unintended consequence of that is as businesses invest more heavily in analytic capability, it becomes easier to identify patterns and therefore take proactive actions." - Jon Bowen, Director of Operations, Paymentshield & Lloyd Latchford

" There's a danger of getting hooked on the removal of sludge practices. You remove all of the friction thinking you're doing the right thing. Focusing so much on making it too easy that you neglect the other side." - Sean Gilholme, Head of Customer Service, Atom Bank

Ownership of fraud protection is a collective responsibility across the organisation. Naturally contact centre teams tend to gravitate towards customer experience while IT and compliance teams tend to gravitate towards security. Achieving an effective compromise requires alignment from the outset.

" Adopting AI will always be a two-pronged approach. Speech analytics works picks up on intent, language, tone, pace, volume. But to generate the right conversational conditions that speech analytics can pull on, you've got to have the right conversation in the first place. Technology will always just augment how good your people are." - Ben Lyons, Vice President, Banking Operations, Chase UK

[3] 'Sludge practices' are defined by the Financial Conduct Authority as 'an excessive friction that hinders consumers from making decisions in their interests'.

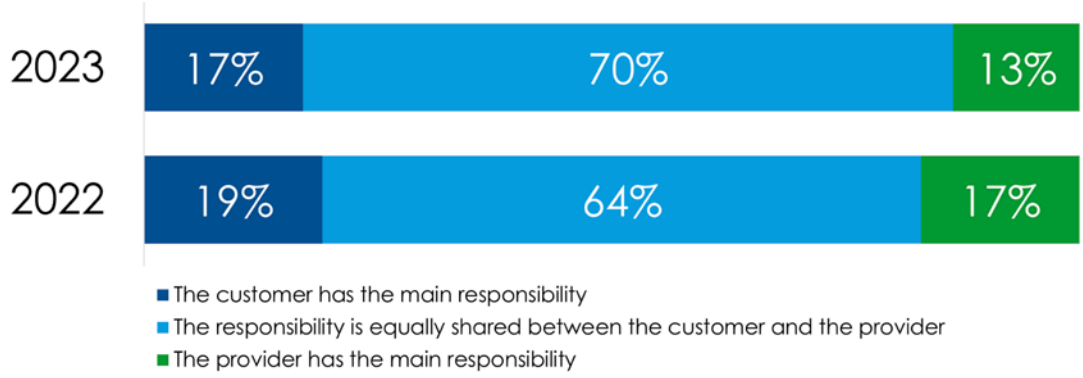
" We've got a security working group with representatives from our legal department, compliance, operational risk, customer support, information security and cybersecurity experts. Everything happens through that working group, which ensures that you do get the opinions early." - Sean Gilholme, Head of Customer Service, Atom Bank

Consumer perceptions of fraud, authentication and security

While it is difficult to convince consumers to accept friction, CCMA's research offers evidence that an increasingly large majority of people understand that responsibility for protection lies with both provider and consumer.

Figure 7 shows that 70% of consumers believe that preventing unauthorised account access is the shared responsibility of both individual and provider, up from 64% in 2022.

Figure 7: *Which of the following statements best describes your view when it comes to preventing unauthorised access to customer accounts?*



Base: All (n=1,001)

Banks lead the way in raising awareness of fraud, no doubt driven by the high frequency of banking transactions which offer regular opportunities to communicate. For some other industries on the other hand, awareness can bring unintended and undesirable consequences.

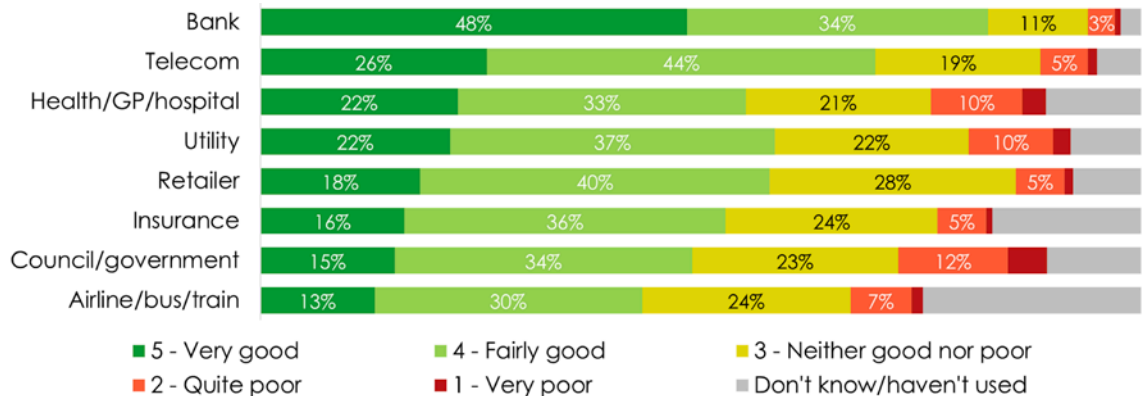
" The financial institutions do a lot of preventative awareness and signposting of fraud. But with gadget insurance, there's no consequence to claiming. Unlike car insurance, your premiums or excess do not increase, it is treated as a product of entitlement but there is a consequence to committing fraud and scheme abuse." - Nick Edge, Head of Fraud Technology, Likewize

Awareness also notifies fraudsters that a change of approach may be needed.

" Once the fraudster knows that we're aware of something they will just move on. And we fall back behind. It's like tipping them off. They can cycle back five years and start doing the same things they were doing then, because everybody's forgotten." - Craig McKeever, Fraud Analyst, Optimus Cards UK

In addition to taking a lead on communication, banks are rated most favourably in terms of authentication experience, as shown in Figure 8.

Figure 8: *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?*



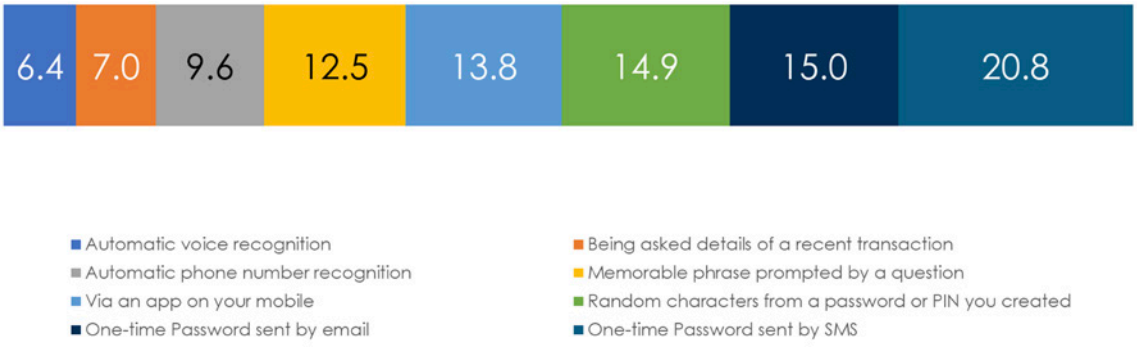
Base: All (n=1,001)

It's not clear the extent to which banks' strong ratings is due to superior authentication experiences, versus familiarity as consumers have become accustomed to banking log-in journeys. The power of familiarity is illustrated in Figure 9, which shows that OTPs (One-Time Passwords) are most highly rated among various telephone authentication methods when it comes to perceived convenience.

How to read Figure 9

Survey participants were asked to allocate a total of 100 points across various authentication options, with more points for options which they felt were more convenient. The scores represent the mean allocation of points for each option across the survey sample, with higher scores denoting more convenient.

Figure 9: *The following are various types of methods used to authenticate account holders over the phone. Please allocate 100 points across each of the following options. Allocate additional points to those options which are most convenient for you. If an option is inconvenient it is okay to allocate zero (0) points to it.*



Base: All (n=1,001)

Objectively speaking, OTPs bring more friction to the customer journey compared with automatic voice or number recognition. Yet the latter methods receive substantially lower ratings for convenience while OTP receive the highest scores. This suggests that perceived friction diminishes as customers acclimatise.

Contact centres are moving away from OTPs as first-party fraud and social engineering proliferate. Despite OTPs having now achieved widespread consumer acceptance, they are becoming less and less effective. Fraudsters are adept at obtaining OTPs via social engineering, while OTPs offer no defence against first-party fraud.

" The OTP has become almost redundant. It's so easy to manipulate the system to get it." - Craig McKeever, Fraud Analyst, Optimus Cards UK

Like OTPs, biometrics are also ineffective at preventing first-party fraud.

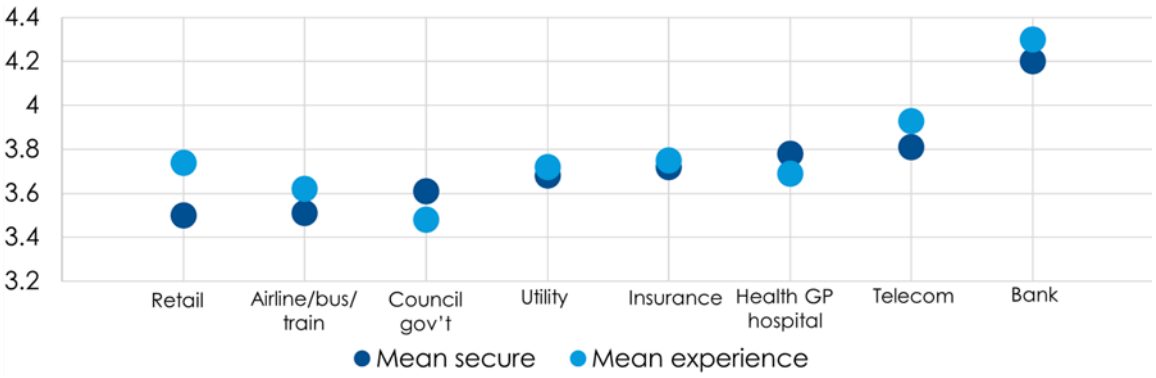
" We'll get numerous claims of unauthorised transactions while we have a customer's phone. That's a physical impossibility because of how we handle their phones. After investigation we find out the customer has logged into someone else's phone, and that phone has remembered their identity and now that someone else has access to their accounts." - Nick Edge, Head of Fraud Technology, Likewize

Security and authentication perceptions by sector are closely linked

When asked about how secure they felt their accounts were across different provider types, consumer perceptions of security broadly align with perceptions of the authentication experience – with banks again scoring highly as shown in Figure 10.

Retailers stand out as they receive more positive ratings for their authentication experience than their ratings for security. The reverse is observed for council and government bodies, which are more highly rated for security than for authentication experience.

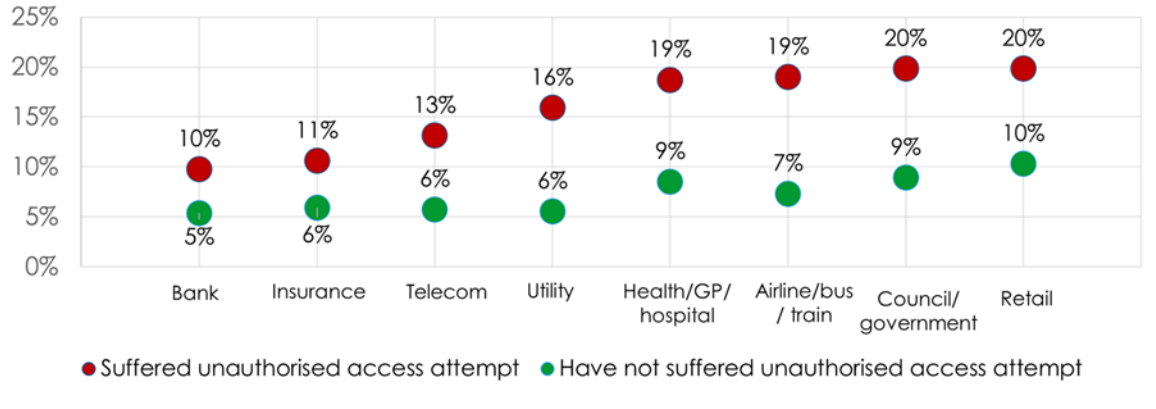
Figure 10: *On a scale of 1 to 5, where 5 equals 'very good' and 1 equals 'very poor', generally speaking how would you rate (a) the experience when authenticating your account with each of the following types of organisation? VS On a scale of 1 to 5, where 5 equals 'very secure' and 1 equals 'very insecure', generally speaking how secure would you say your accounts are against potential breach for the following types of organisation? In other words, how well do you think each type of organisation protects its customers' account security.*



Base: All (n=1,001)

Not surprisingly, people who have experienced a fraud attempt tend to be more critical about provider security, as illustrated in Figure 11.

Figure 11: *On a scale of 1 to 5, where 5 equals 'very secure' and 1 equals 'very insecure', generally speaking how secure would you say your accounts are against potential breach for the following types of organisation? In other words, how well do you think each type of organisation protects its customers' account security? [% 'not very secure' + or 'very insecure'].*



Base: All (n=1,001)

" People's mindset changes if they have the event. You start to ask for more friction in your processes because you want to be safeguarded." - Jon Bowen, Director of Operations, Paymentshield & Lloyd Latchford

The role of analytics and AI

Advanced analytics and AI (artificial intelligence) are playing an increasingly important part on both sides of the balance: emerging technology can help to bolster security and reduce friction by dramatically enhancing the accuracy and the speed of fraud detection, spotting and flagging anomalies.

Machine learning can be deployed to update business rules to reflect fast-changing customer or fraudster behavioural patterns, much more quickly than humans can.

Furthermore, the ability to generate personalised risk profiles and apply tailored business rules at the individual level will not only better protect organisations but also help ensure that customers receive an authentication experience that is appropriate to them, tightening security measures if warranted but making authentication simpler for those with good risk profiles.

" The hope is for it to be able to change rules on the fly. So that we don't have to review after a month or a quarter and make changes. AI could do that in real time. And do it based off of each customer's specific details. You can feed all the information that's fed in from the application stage, customer details, their spending habits, transfer patterns, and it could take all that information and essentially cater the rules that we give to each customer." - Craig McKeever, Fraud Analyst, Optimus Cards UK

" I introduced cohort rules 18 months ago. We analysed claimant behaviours and individual characteristics ranging from age, location, and device type. It took a three-month project to launch because of all the analysis that goes behind it. Whereas I'm now doing a proof of concept with AI, which can do that in 24 hours." - Nick Edge, Head of Fraud Technology, Likewize

New ethical frontiers

The ability to profile individually for risk and apply different rules for different customers will raise questions around privacy and fairness. For example, is it reasonable for people belonging to demographic groups who demonstrate greater risk at a cohort level to receive more stringent authentication measures?

" We had an issue in the past when I was at a previous employer where certain demographics had different rules. We had to change that. The issue is it's a lot easier to write a single rule that does exactly what you want it to do, rather than creating a risk score system, so that everybody has the same rules apply to everybody with the values or the volumes within those rules, whereas the causation of the triggers could be different."

- Craig McKeever, Fraud Analyst, Optimus Cards UK

Another question that emerges, as it has in every field being transformed by AI, is whether robots will supplant humans. The consensus so far, as it is in other areas, is that human expertise will always be needed.

" I think it will always be a two-pronged approach. Because the way that speech analytics works is it picks up on the intent, the language, the tone, the pace, the volume, and even the background. But to generate the right conversation and the sentiment that speech analytics can pull on, you've got to have the right conversation in the first place. Technology will always just augment how good your people are. That investment in people is always going to be absolutely key." - Ben Lyons, Vice President, Banking Operations, Chase UK

" I still need a human to test that the AI has made the right decision. We use AI to write rules and protections but the fraudsters are using AI just as quickly. We know that ChatGPT can create voices. AI is brilliant, but it's going to be used against us as well." - Nick Edge, Head of Fraud Technology, Likewize

6 discoveries

to balance fighting fraud with customer experience

1. 36% of people in 2023 reported having experienced an unauthorised attempt to access one or more of their accounts. This is an increase over the 33% reported in earlier CCMA research, published in March 2022.
2. The customer is now the weakest link, as social engineering grows alongside self-serve. As coercion becomes increasingly common, security systems must not only guard against bad actors impersonating customers, but also help genuine customers protect themselves from scams.
3. Digital fraud is rising especially rapidly, and younger people are particularly vulnerable..
4. Customer friction is in the spotlight thanks to Consumer Duty, but organisations should be mindful of the difference between sludge practices and necessary friction.
5. OTPs have been widely accepted by consumers, but providers are moving away from this method of authentication as efficacy is declining.
6. Analytics and AI will transform fraud detection and will both improve security and reduce friction.

Afterword by Matt Smallman

As someone who spends their life thinking about customer security experiences, getting a reality check from the front line is always healthy, and this year's survey is no exception. For example, while we know SMS OTP is both insecure and inefficient, consumers perceive it as the most secure and usable authentication method. This is a prescient reminder that security is, first and foremost, a human problem, not one of process or even technology.

Consumers' overconfidence and optimism biases refuse to allow them to see themselves as a weak link in the security process even when they sabotage it by, as the survey shows, sharing their secret information across many organisations. They just don't believe bad things will happen until they do, and when they do, a traditional dependence on knowledge-based authentication by most organisations has trained them to correlate friction and effort with security.

Of course, this all comes back to bite us in the call centre, where automated systems and frontline agents must not only handle the fallout of security process failures in other channels but prevent themselves from being exploited. While the rate of suspicious calls is very low, less than 1 in 500 calls, even in high-risk organisations, successful compromises receive significant management attention. As a result, agents can become paranoid and hyper-vigilant, changing the very nature of their interactions with your customers. Further, the cognitive dissonance created by being forced to interrogate every customer as if they were a fraudster (when the numbers suggest they would be lucky to speak to one a month) at the same time as trying to help them is a significant source of workplace stress.

Fortunately, we appear to be at a tipping point. More consumers than ever, either personal victims of fraud or frustrated by their inability to access services, acknowledge that security is a shared responsibility. Similarly, leading CCMA members are following the data to develop risk-based approaches that intelligently tailor the security experience to the customer and context. But there is still work to do; whilst we must take security decisions out of the hands of agents, we shouldn't underestimate the role of consumer perception as we transition to modern security approaches. Methods such as voice biometrics and network authentication deliver objectively higher levels of security with lower levels of effort but are highly dependent on user adoption and hence perception to be effective.

Unlocking your call centre's security processes means recognising the complex interplay between security, customer perception, and agent experience.

Matt Smallman is the author of "Unlock Your Call Centre: A proven way to improve efficiency, security and caller experience" and founder of SymNex Consulting, where he helps organisations transform their call centre security experiences.

About the CCMA

For nearly 30 years, the CCMA (Call Centre Management Association), as the longest established contact centre industry body, has been dedicated to supporting contact centre leaders across the UK. Founded on the principles of sharing best practice and networking to improve skills and knowledge, the CCMA is a thriving community that represents leaders from a huge cross-section of the industry.

Membership of the largest community in the industry offers unique opportunities, such as the opportunity to be an Accredited Contact Centre through the Contact Centre Standards Framework, free annual benchmarking of 25+ KPIs, free entry into the UK National Contact Centre Awards and free tickets to the UK National Contact Centre Conference, invites to Executive Networking Dinners and exclusive events for members-only. Members also benefit from discounted training through the UK National Contact Centre Academy, the industry's training partner.

To support the industry further, the CCMA conducts regular original research for download, including the annual Voice of the Contact Centre Consumer research, the Evolution of the Contact Centre tracking the industry's progress and Good Practice Guides on a variety of topics.

www.ccma.org.uk

About Smartnumbers

Smartnumbers authenticates callers and detects fraud in real-time. Combining the power of AI and community, we build a world of trust in every call.

The impact of fraud is alarming, affecting millions of people and costing the UK alone almost £7bn a year, which accounts for 40% of all crime. Shockingly, 61% of fraud is connected to the contact centre, with one in every 500 calls from a fraudster.

Unfortunately, current authentication methods often frustrate genuine customers, create inefficiencies and fail to stop fraudsters who conceal or manipulate their phone number. With 58% of fraudsters withholding their number, spotting the concealed risk can be challenging.

We are revolutionising the industry by equipping organisations with real-time insight into the risk of a caller. We combine artificial intelligence, deep domain knowledge and a consortium of confirmed fraudsters to prevent fraud and streamline customer experience.

www.smartnumbers.com

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 | info@ccma.org.uk