THE FRAUD RISK CHALLENGE:

How are FSIs using AI and biometric authentication to crack down on fraud and provide a seamless customer experience?

FStech

NUANCE®

INTRODUCTION & METHODOLOGY

INTRODUCTION

Over the past two years, society has leapfrogged into a new digital age. Restrictions, lockdowns, and growing bank branch closures have driven consumers toward online channels and self-service, with demand for digital financial services at record highs.

Unsurprisingly, the shift to digital products and services has completely transformed the fraud risk landscape, generating a variety of new threats and challenges for financial services institutions (FSIs) across the UK, which were already a top target for fraudsters pre-pandemic.

FStech and Nuance Communications conducted a survey of financial services decision makers to assess the role of authentication technologies as organisations adapt to changing fraud methods while preparing for the deadline of Strong Customer Authentication (SCA) and responding to rising customer demand for secure and seamless login processes.

METHODOLOGY

FStech and Nuance Communications surveyed 101 senior decision makers including chief executives, heads of risk, heads of compliance, chief information officers, risk analysts, as well as others, from the UK's leading banks, insurance companies, building societies, asset management firms, and challenger banks.

CONTENTS

EXECUTIVE SUMMARY

Financial institutions are facing a momentous upsurge in online fraud, largely triggered by a vast move towards digital channels and services.

With the shift to online showing no signs of slowing, fraudsters are varying their techniques to find consumer weak spots. The survey found that online banking is a key method for criminals, with nearly 40 per cent of financial services professionals identifying this as an approach currently being used. Phishing was also recognised as a top tactic by over a third of respondents.

Anti-fraud and compliance teams are responding to changing consumer habits and fraud methods by focussing on remote and digital channels. Over half of respondents chose banking or other apps, telephone banking, and postal banking as areas of focus, while in-branch was selected by just over a fifth of financial services providers.

Biometrics was top of the list when it came to authentication technologies currently being rolled out by FSIs, with 40 per cent of those surveyed choosing voice, 35 per cent selecting facial, and 42 per cent opting for fingerprint biometrics. FSIs are also reaping the benefits of additional layers of protection, with over a third implementing multi-factor authentication and almost 39 per cent deploying token-based authentication.

Consumers are becoming less comfortable with traditional methods of authentication like pin & password login, with nearly 50 per cent of respondents saying their customers were frustrated with this technique. But there is still a long way to go to assure them about simpler options like voice identification – with 55 per cent saying that customers are uncomfortable with this kind of authentication.

Financial services firms are missing out on the wide-ranging benefits of customer verification technologies – with 37 per cent of those surveyed saying they are not using their authentication strategy to streamline or improve customer interactions.

As the industry prepares for the arrival of Strong Customer Authentication (SCA), one of the key challenges for FSIs is coronavirus delays – with 58 per cent choosing this as one of their top three obstacles, closely followed by a lack of guidance at 44 per cent.

While companies understand the importance of inclusivity, it seems that in general the industry is not aware of how technologies like voice authentication can address issues associated with this, with 60 per cent suggesting this would hardly feature in their customer verification strategy.

Finally, the biggest barrier to the adoption of AI-assisted voice authentication was identified as a perception that it is expensive, closely followed by a lack of skills and knowledge around the technology. However, if FSIs knew the ins and outs of the tech and both its cost and time savings, they could easily get rid of these hurdles.

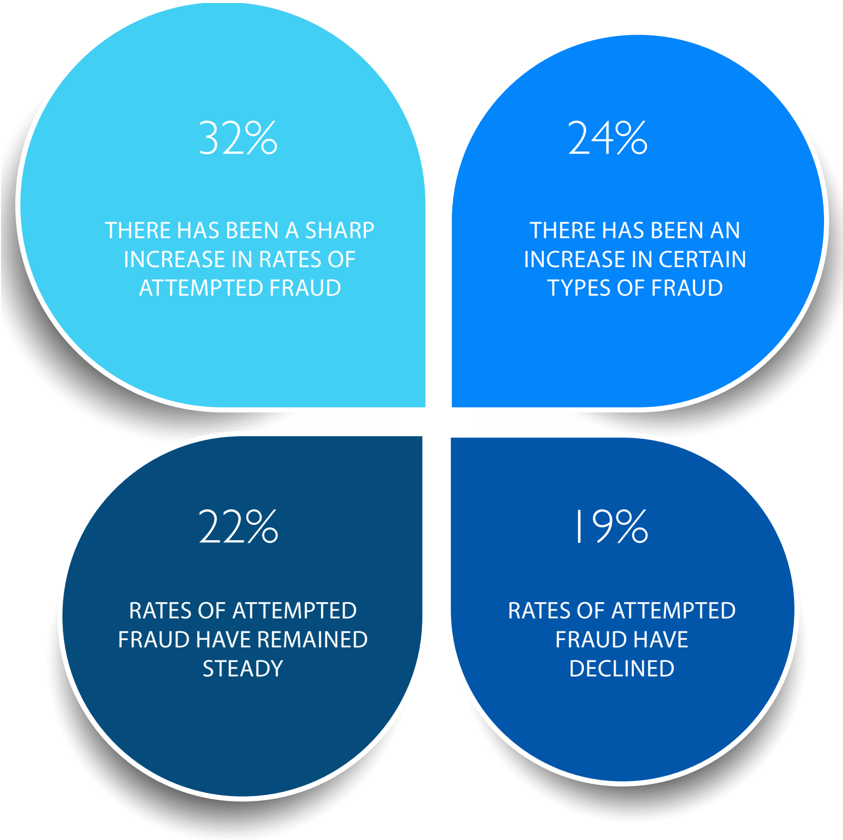
1. How has the fraud risk landscape changed for your organisation in the past 2 years? *(Select the most appropriate)*

Largely driven by the pandemic, a rising demand for digital financial services has widened the target range for online fraudsters. The survey reflects this, with the majority – a combined 56 per cent – having experienced a hike in fraud attempts in one form or another over the past two years.

While almost a quarter of respondents said there had been an increase in certain kinds of fraud, just under a third revealed there had been a significant rise in fraud attempts during the period.

Not only have criminals had access to more potential victims via online channels, they've also exploited consumer concerns about the pandemic by generating emails and text messages pretending to be from official government or NHS sources.

Even though most financial services organisations experienced heightened fraud levels, around a fifth of senior leaders said rates had remained unchanged. A further 19 per cent said attempted fraud had declined. This could suggest that some areas within the financial services environment are less vulnerable to fraud than others.



32%

THERE HAS BEEN A SHARP INCREASE IN RATES OF ATTEMPTED FRAUD

24%

THERE HAS BEEN AN INCREASE IN CERTAIN TYPES OF FRAUD

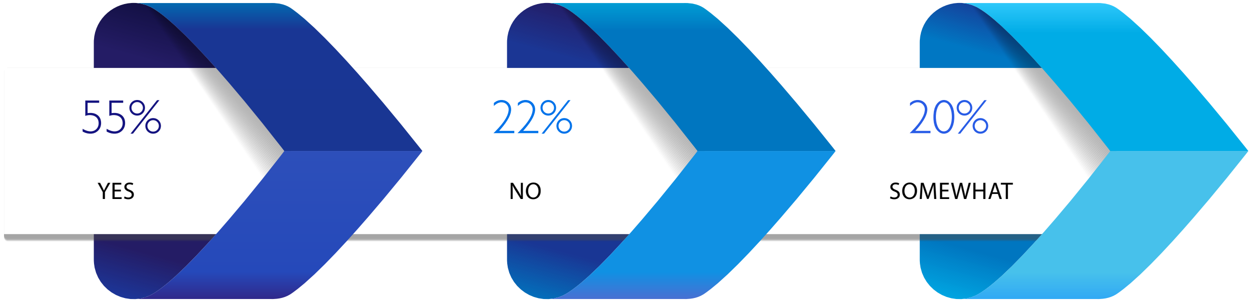
22%

RATES OF ATTEMPTED FRAUD HAVE REMAINED STEADY

19%

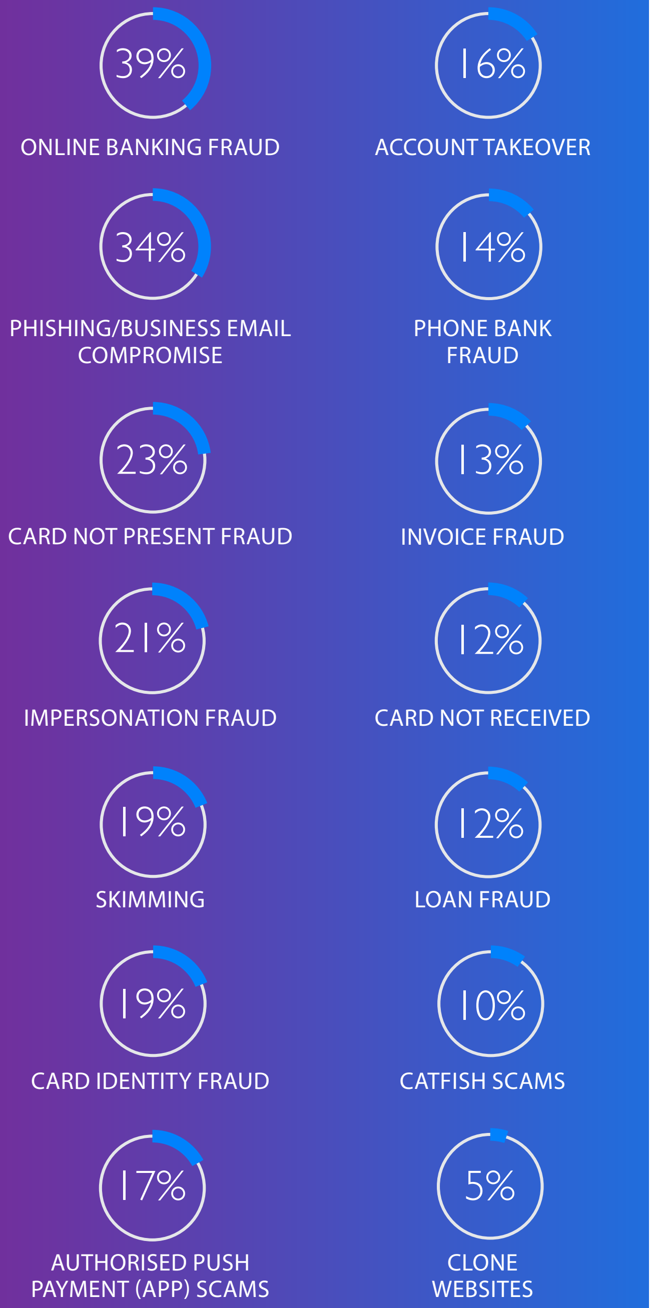
RATES OF ATTEMPTED FRAUD HAVE DECLINED

2. Has the shift to digital channels and self-service in the past year increased fraud risk for your organisation? *(Select the most appropriate)*



Over a half of respondents agreed that an increase in fraud risk was the direct result of a move to online platforms and self-service – reiterating the results of the previous question.

A fifth said that the shift to digital channels had, to an extent, made fraud more of a risk for their organisation. Only a fifth of those that responded felt that the heightened use of digital products and services had no impact on fraud risk. This means the vast majority – three quarters – have seen fraud risk impacted by increased demand for digital financial services.



3.Which of the following methods are fraudsters using to target financial services organisations?

(Tick the top 3)

Online banking was chosen by the highest number of financial services decision-makers – with just under two in five picking this as a popular method for fraudsters.

Close behind was phishing –whereby fraudsters pretend to be reputable organisations in email correspondence – which was identified by over a third of respondents. With fraudsters increasingly using malicious emails to gain access to personal information, often taking advantage of the uncertainty around Covid-19 and supply chain disruption, it's no surprise that many banks and other financial services firms in the survey highlighted this as a common technique used by online criminals.

Card Not Present or Remote fraud – where a criminal uses stolen card details to buy things either online, over the phone, or through mail order – was chosen as a top-three approach by nearly a quarter of respondents. While this type of fraud is understood to be on the decline, it's likely the numbers are still high because fraudsters have taken advantage increased online payments. A further fifth of financial services executives chose impersonation fraud.

Authorised Push Payment (APP) scams – when a customer is tricked into authorising a payment to an account controlled by a criminal – were identified by only 17 per cent of respondents. However, it's likely the industry will see these numbers rise over the coming years, with industry figures from UK Finance suggesting this method overtook card fraud for the first-time in 2021.

While digital fraud appears to be the most popular method for scammers, account take over was chosen by only 16 per cent of those surveyed. Catfish scams and clone websites were also an uncommon choice, with 10 per cent and 5 per cent respectively choosing these options . This could reflect the fact these methods can take more time and effort to carry out.

Non-digital-based scams appear to be much less of a risk for FSIs in the UK. Skimming – where a criminal uses a device attached to an ATM or payment device to steal information from the magnetic strip of a card – and card identity fraud, were both chosen by under a fifth of respondents. Following the same trend, card not received, phone bank fraud, invoice fraud, and loan fraud were all picked by less than 15 per cent of respondents.

The results once again show that scammers are taking advantage of closing bank branches and society's reliance on digital platforms.

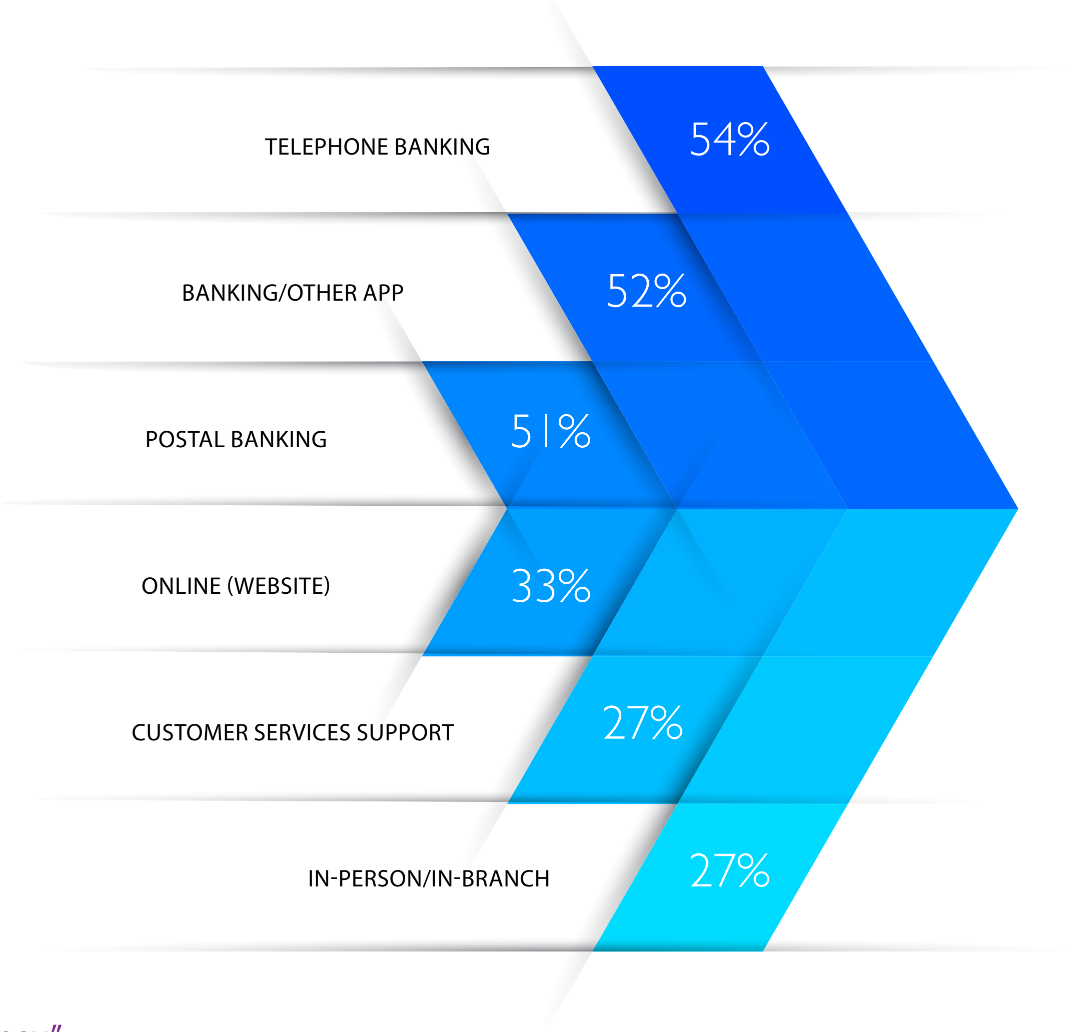
NUANCE

4. Which of the following channels are a focus for anti-fraud and compliance teams? *(Select all that apply)*

Anti-fraud teams are focussing on remote forms of banking. Customer services support and in-branch, for example, were identified by only around a quarter of respondents as a priority for fraud prevention departments. Meanwhile, Telephone banking was the number one choice for FSIs, with over half of senior leaders picking this as a focal point for their compliance teams. Given that thousands of bank branches have been closed across the UK over the past few years, these results are not surprising.

More than half chose banking apps / another online platform as a main concern for fraud prevention, with a further third highlighting websites as a key focus for anti-fraud units. These figures suggest that FSI decisions are being driven by the vast shift to online channels for banking and other financial services.

Amidst the backdrop of bank closures, consumers have become increasingly reliant on post offices – where there has been an uptick in deposits and withdrawals. This trend is reflected in the results, with the majority of respondents saying that their company's anti-fraud employees are focussing on this area. An increase in use of postal banking – where people do not necessarily have to verify their identity – could see a rise in people using cards that don't belong to them to withdraw or deposit money.



"Voice ID has not only made telephone banking more convenient for customers accessing their accounts, but it has also been instrumental in stopping attempts at telephone banking fraud, protecting customers' money."

Kerri-Anne Mills, Head of Contact Centre and Customer Service HSBC UK

5. Which of the following authentication technologies is your organisation currently implementing? *(Select all that apply)*

The results show that biometrics are the most popular form of authentication method currently being rolled out by financial services institutions. The top technology was fingerprint, with just over two in five senior leaders saying they are currently implementing this. Given that this authentication method is already familiar to many consumers, with millions using this technology every day to unlock their mobile phones and other digital devices, it's an obvious choice for FSIs.

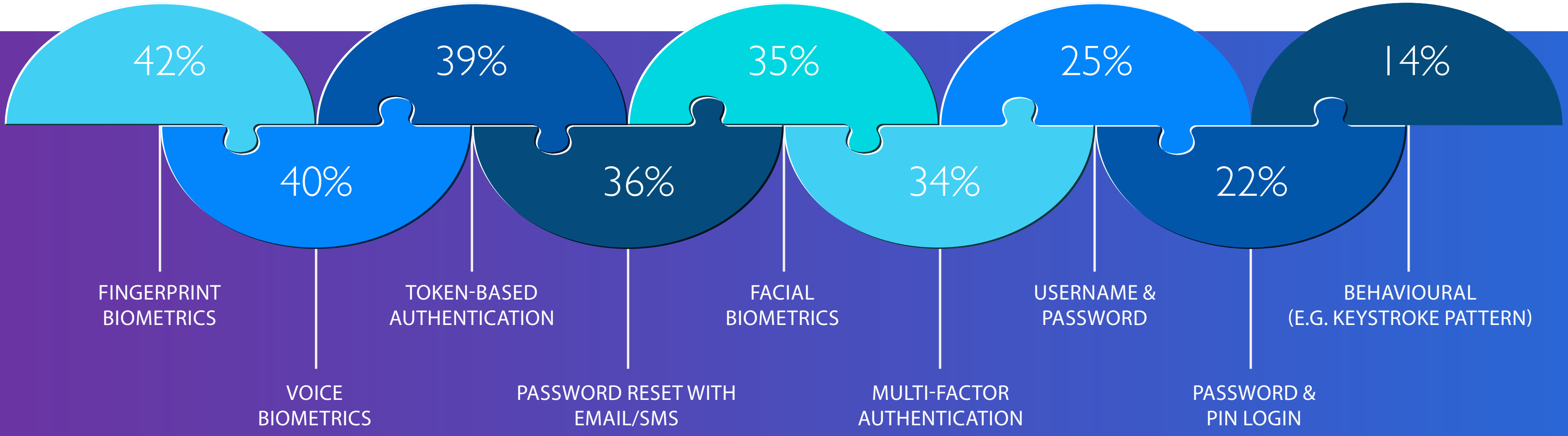
Not far behind was voice biometrics, which can speed-up the authentication process significantly, with two fifths of respondents revealing they are deploying this technology. Facial biometrics was slightly less popular, but still chosen by more than a third of those surveyed.

Behavioural authentication – which analyses the unique ways a customer interacts with their device when making an online purchase - was chosen by less than 15 per cent of respondents. However, it's likely that as the technology continues to be developed over the coming years, it will become a more popular choice for banks and other financial institutions. Some large card providers, for example, are already rolling out this tech across their networks.

The majority of senior leaders – a combined 73 per cent –are currently applying multi-factor and token-based authentication. Password reset with email/SMS was also chosen by more than a third of respondents. This demonstrates that most FSIs recognise the importance of an extra layer of security in their authentication process.

Password & pin login was picked by just over a fifth of those surveyed, while username and password was chosen by only a quarter. Financial services are moving away from these often clunky, longwinded, and less safe verification methods, as they can lead to consumer frustration and abandonment of services. Instead, they are starting to rely on up-to-date technologies that provide a balance between speedy and frictionless processes and protection from rising fraud and changing risks.

> "With Nuance voice biometrics, we get a clearer view of customer and fraudster behaviour, so we can keep genuine customers protected and take the fight to the criminals who are targeting their accounts."
>
> **Jason Costain, Head of Fraud Strategy and Relationship Management NatWest Group**



The survey shows consumers are unsatisfied by legacy authentication methods, with nearly half of senior leaders saying their customers are frustrated with pin & password login. However, it seems there's still work to be done to reassure them about the safety of simpler options like voice identification. The majority of respondents said that customers are uncomfortable with this as a form of identification vs 16 per cent that say the opposite.

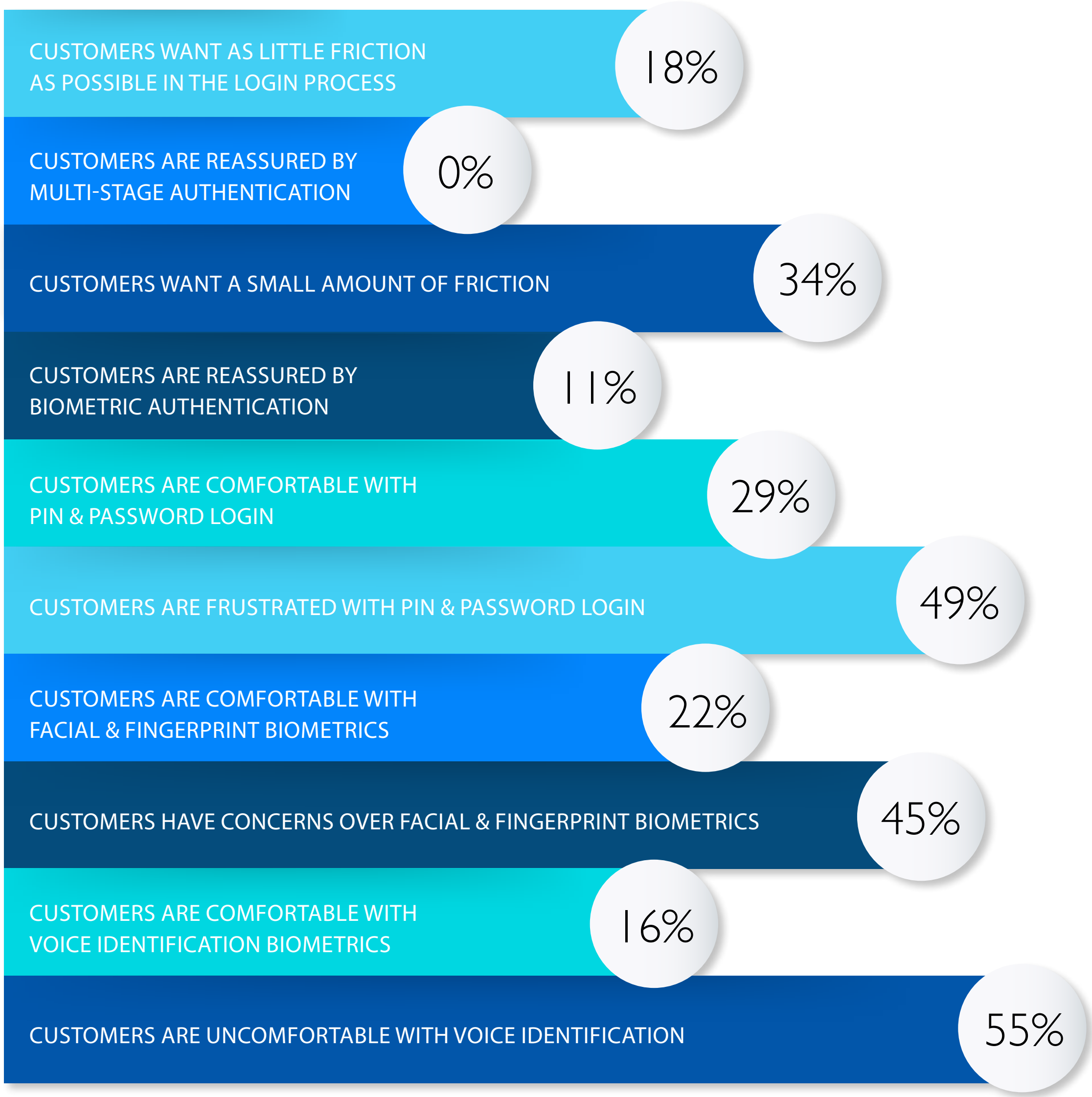
The trend is echoed by other types of biometrics, with two fifths identifying the same hesitance from customers towards facial & fingerprint biometrics compared to just over a fifth who said that consumers are relaxed about utilising these technologies.

While there is a perception that customers are nervous about using biometrics the technology can actually bolster consumer interactions by cutting out longwinded processes, making the authentication journey easier and unobtrusive.

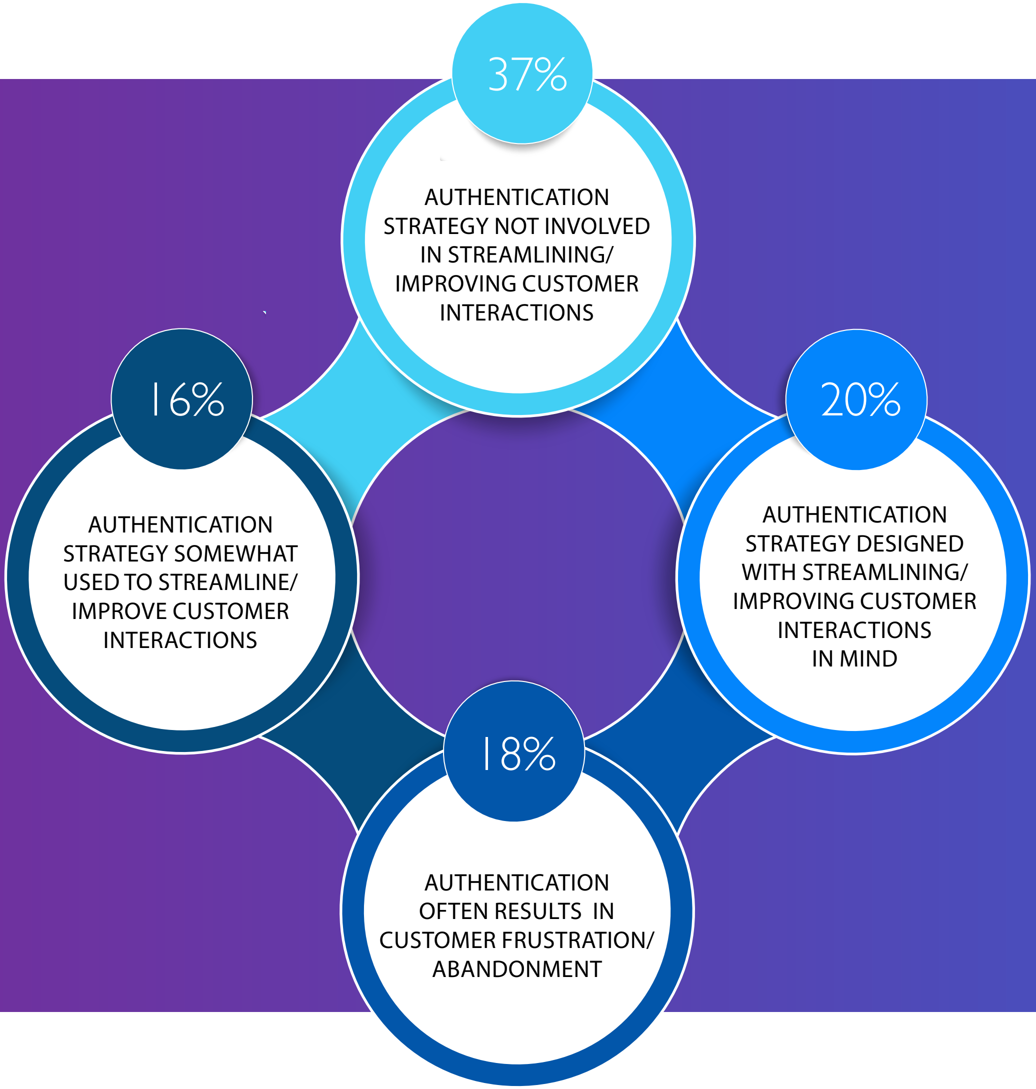
Nearly double the number of people – just over a third – believe that customers want a small amount of friction compared to those that said consumers want the least amount of friction possible (almost 1 in 5). This supports the idea that the perception of security by consumers is as important as the reality. To address this, FSIs can add a small level of friction which will reassure customers. For example, during the voice authentication process, a verification message from a customer service agent could be added.

6.Which of the following best describes customer attitudes to authentication methods?

(Tick top three)



7. To what extent is your organisation using its authentication strategy to streamline and personalise customer interactions? *(Select the most appropriate)*



While authentication technologies like biometrics can save time, energy, and costs by removing clunky, outdated methods, giving customer service operatives more time with customers, the survey shows that most of them are not taking full advantage of these multifaceted features and capabilities.

The majority of senior decision makers – a combined 55 per cent – said that their authentication strategy is either not used at all to streamline customer interactions or is actually putting consumers off. This can lead to customers abandoning the process and ultimately looking elsewhere for easier security and customer service processes.

Only a fifth of respondents said that their current authentication strategy has been specifically designed with streamlining customer interactions in mind, with a further 16 per cent saying that it's used to speed-up communication with customers to some extent.

8. What are the top challenges for your organisation in preparing for the arrival of Strong Customer Authentication (SCA)?

(Tick the top 3)

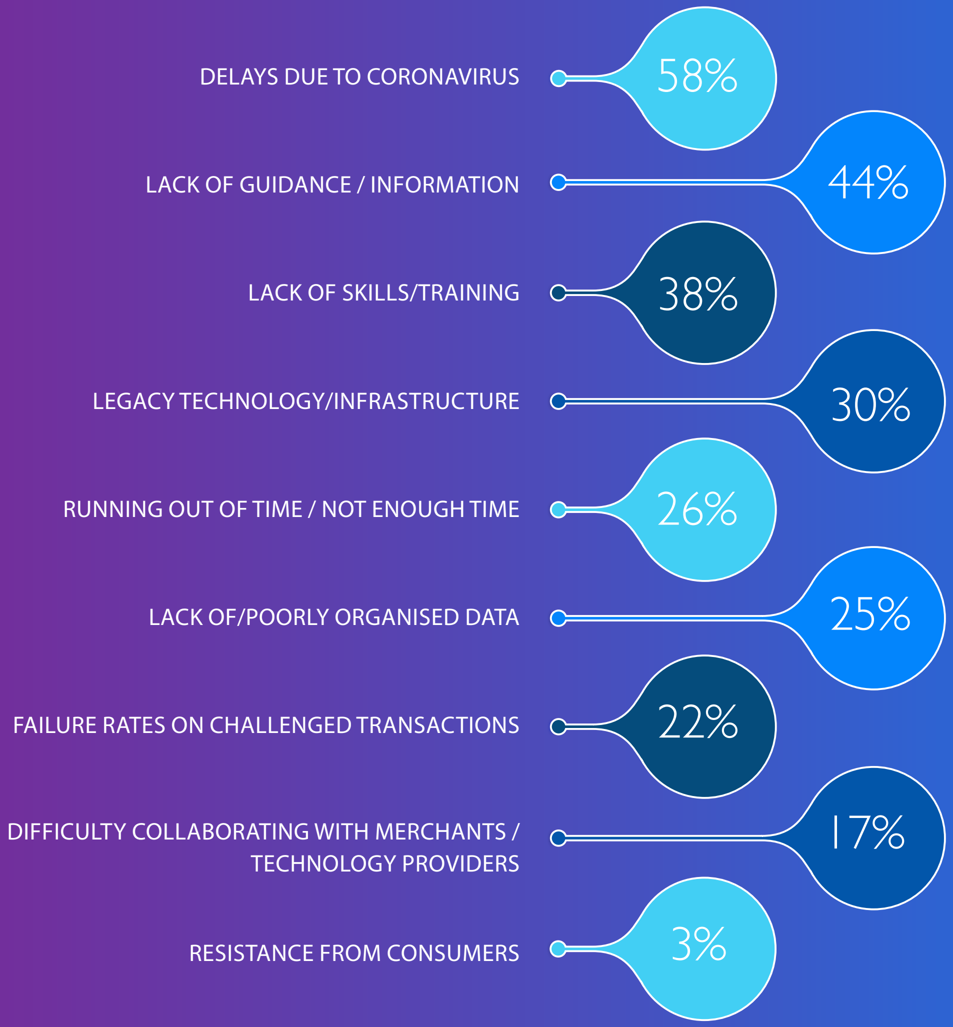
As the deadline for Strong Customer Authentication (SCA) fast approaches – FSIs are still struggling with coronavirus delays – with nearly 60 per cent choosing this as a top challenge.

Lack of understanding or skill around the adoption of the new regulation was identified as a key hurdle – with a combined 82 per cent saying that they are feeling left in the dark without proper guidance or lack of skills and training.

Worryingly, over a quarter feel like they're running out of time, meaning they might not be ready for the upcoming deadline.

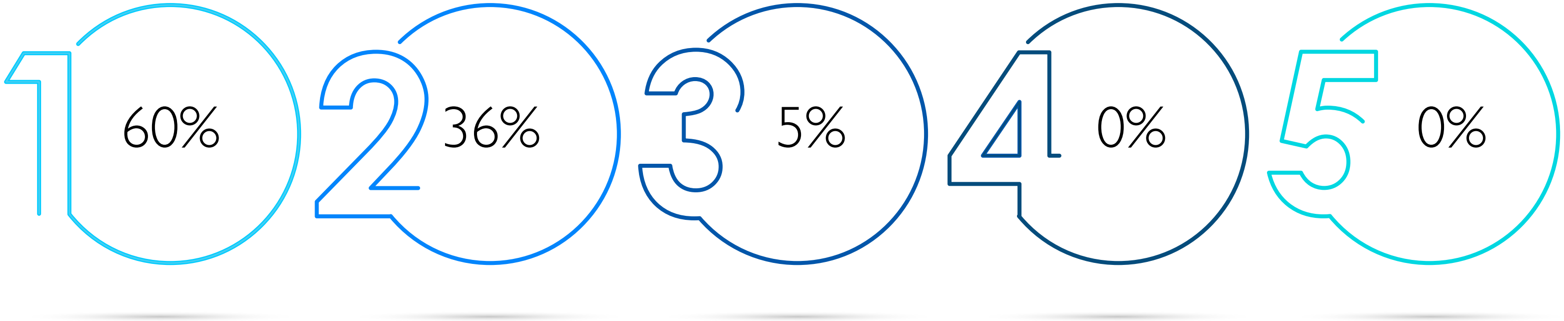
A significant obstacle for many is not having the right digital tools to face the new regulation, with a combined 55 per cent identifying lack of/poorly organised data and legacy technology as a top-three hurdle.

Less of an issue for FSIs was failure rates on challenged transactions, difficulty collaborating with merchants or technology providers, and resistance from consumers. This highlights that the main obstacles are related to a lack of technical skills and tools, as well as unexpected delays caused by the pandemic.



NUANCE

9. On a scale of 1-5, how important is it for your organisation to ensure customer verification methods are inclusive of diversity and vulnerable customer demographics to improve access to support? *(Choose one)*



The majority - three fifths of respondents - chose '1' out of '5' – suggesting that inclusivity would hardly feature in their customer verification strategy.

Just over a third of senior leaders chose '2' and only 5 per cent said that it is somewhat important for their organisation to make sure customer verification is inclusive. This could suggest that while companies recognise the importance of inclusivity, the industry is currently unaware of how authentication technology can address key considerations such as diversity and vulnerable customer demographics. Technologies like AI-assisted voice authentication, for example, can prioritise older customers by identifying those over a certain age and getting them straight to a live agent for service.

10. What are the top barriers to implementing AI-assisted voice authentication?

(Select all that apply)

The top barrier to the implementation of AI-assisted voice authentication is the perception that the technology is expensive, with four out of five respondents choosing this option.

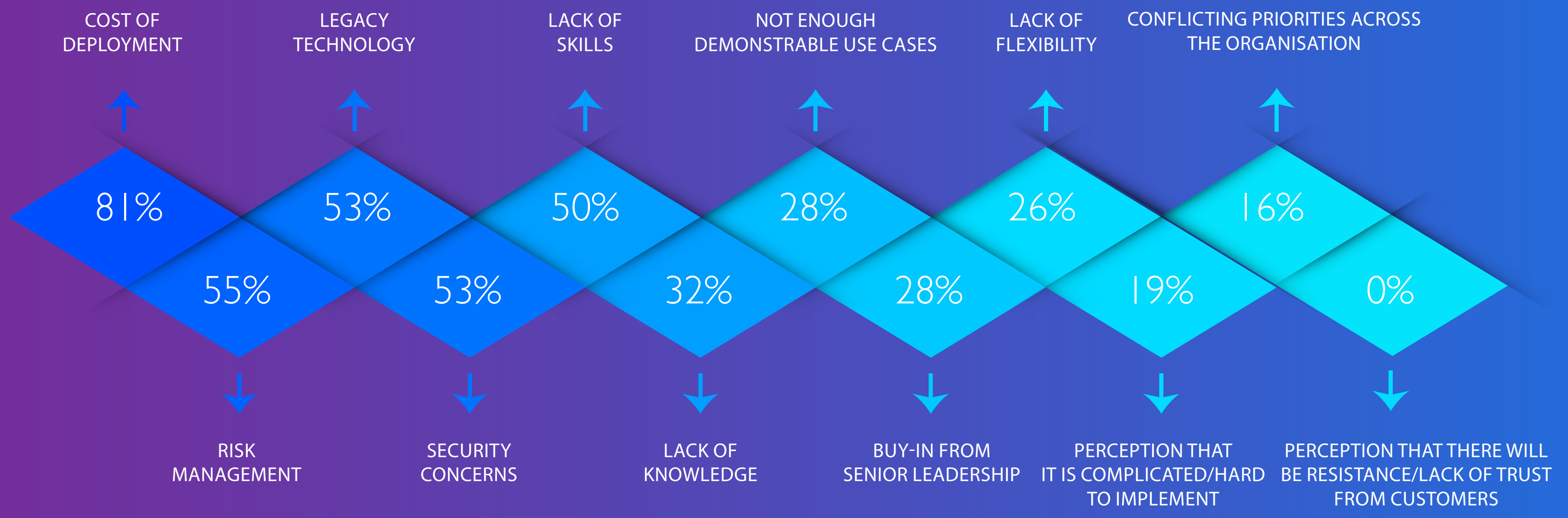
Not having the right tools was also deemed a significant hurdle for the majority of respondents – with lack of skills and knowledge picked by a combined 82 per cent of respondents.

Meanwhile, legacy technology was also a common issue for the roll out of voice tech, with over half of respondents identifying this as a deterrent. Risk management and security concerns were also chosen by more than half of respondents.

Just over a quarter said there weren't enough examples available or that there was a lack of flexibility, while slightly under a third identified buy-in from senior leadership as a hurdle.

Perception that the tech is hard to implement and conflicting priorities across the organisation, were less of a hurdle for organisations, with both chosen by under a fifth of respondents.

The survey shows that the top obstacles to rolling out AI-assisted voice authentication are largely linked to cost, security, and skills rather than customer-related, with none of the 101 respondents saying their organisation thinks there will be resistance or lack of trust from customers. By simply having a better understanding of the technology and its cost savings, financial services organisations could remove these barriers, opening up new layers of protection for their customers.



CONCLUSION

The report shows that over the past couple of years the majority of banks and financial institutions – 56 per cent – have experienced a notable rise in fraud. Roughly the same number identified the shift to digital channels – thus opening up opportunities for fraudsters – as the direct cause for this heightened fraud risk.

As demand for digital financial services grows, criminals are adapting their methods. Online banking was identified by the highest number of people – 2 out of 5 – as a top technique for criminals, with other digital-based fraud like phishing also a common choice for scammers.

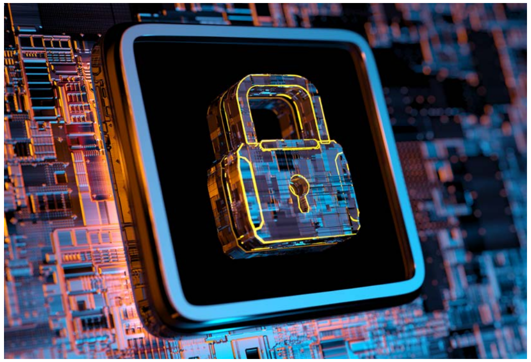
As they turn their heads towards more digital-based scams like APP, Card Not Present is becoming a less popular style of financial fraud for criminals. But it was still a top-three issue for a quarter of those that responded to the survey, largely because criminals have been taking advantage of higher levels of online payments.

Meanwhile, to tackle the digital-heavy fraud currently happening across the industry, anti-fraud and compliance teams are focussing their energy on digital channels like online banking to protect their customers.

The survey revealed that biometrics are currently the most popular form of authentication being used to address these new challenges, with voice, fingerprint, and facial all scoring highly. For an additional layer of protection, 73 per cent of FSIs are implementing some kind of multi-factor or token-based authentication.

It's clear that while companies are investing in the latest technologies and methods, FSIs are not taking full advantage of their multifaceted capabilities.

Only a fifth of financial services professionals said that they are using their authentication strategy to boost customer interactions, while well over a half are not prioritising inclusivity in their verification methods.



Up-to-date technologies like voice authentication can help improve customer relationships and experiences, while at the same time ensuring financial services processes are secure.

As the industry continues to face growing fraud risk and prepares for the fast-approaching Strong Customer Authentication (SCA) deadline, it's those companies that utilise tools and technologies that crack down on fraud whilst providing a seamless customer experience that will see the best outcomes.

CONTACT INFORMATION FOR NUANCE: WEBSITE: WWW.NUANCE.COM/EN-GB PHONE: 01628 491600 EMAIL: CXEXPERTS@NUANCE.COM