Before we see wide adoption, this second tier of organisation will require both simpler and easily integrated solutions (either with an existing CRM/telephony infrastructure or as part of a suite of identification and authentication solutions) that lower the total cost of ownership. For all the reasons listed above, these organisations will also need to be supported through the human issues. This will require significant effort, to transfer the knowledge and experience of the maybe two or three dozen people globally with real implementation credibility to hundreds of partners. Only then will organisations really have the confidence to influence a significant number of customers' day-to-day interactions.

• **Truly intelligent authentication.** As many who have been down this path realise, the initial implementation of a voice biometrics solution is just the start of a journey. Voice may be a significant step, but in itself won't solve the whole authentication problem. Because just as we invest in deploying this technology, so determined fraudsters will invest in defeating or bypassing it, and there is a continuing need to evolve and adapt.

Culturally, for many organisations this will also be the first time concepts such as risk-based decision making and layered defence have been used by front-line customer service teams. Once they get to grips with the voice channel, the opportunity it provides via continuous and intelligent authentication will becomes apparent, even if the tools to realise it are not yet available.

Inevitably, the technical solutions used in customer authentication – the different decision engines required to fuse information from many sources and translate probabilities into treatment strategies for end users – have been developed purely for digital channels and are often business rather than consumer-facing. They therefore don't contend with all those messy human problems of customer service operations. It is very unlikely that in 10 years' time we will be relying on customer's voices as the sole authentication token. But the concepts are likely to be very similar. So vendors have an opportunity to start laying the groundwork in their products now, to make them the natural choice for future extension.

• **Federation opportunities.** For as long as voice biometrics retains some novelty value, it is unlikely that significant numbers of customers will decline to enrol their voices. However, at some stage we will reach a tipping point where consumers are fed up with registering their voice with multiple organisations. Or a high-profile event will undermine their confidence in the technology. Or consumers will simply insufficiently trust late-adopter organisations. At this point, there will be a case for the most trusted parties to leverage their biometric assets to assert customers' identity to less trusted organisations.

Looking beyond the contact centre, customers will continue to want to do more themselves. So as voice and other user interfaces genuinely become more useful – through better understanding of customer context and predictive ability – it will be increasingly important to secure these systems in an effortless a way as possible. And while voice is a far-from-perfect factor and is often oversold for this problem, those organisations that have already invested in this area have a clear opportunity to leverage that asset.

Road ahead

Decisions on whether to implement voice biometric solutions will continue to be driven by practical commercial considerations, reflecting the total cost of ownership and the benefits derived. Currently the case may still be marginal for all but the highest-risk financial services organisations, but as the balance shifts over the next few years voice biometrics will be a key enabler for the transformation of contact centres.

If we can relieve our front-line colleagues of the burden of thinking every caller is a potential bad guy, and all of the training and process required to make sure they do this, then we can allow them to focus on the job they signed up for. At that point, they will be able to hold genuinely better human-to-human conversations aimed at solving customer problems, rather than simply achieving process compliance.

About the author

Matt Smallman is a co-founder of SymNex Consulting, which exists to bridge the gap between advanced technologies and their application in customer service. He works with organisations to help them make the case, accelerate design and maximise the impact of voice biometrics. He led the award-winning implementation of voice biometrics for Barclays Wealth in 2012 and previously held senior strategy and design roles at both Lloyds and Barclays Banks.

Reference

1. 'Fraud The Facts 2016'. Financial Fraud Action UK, 2016. https://www.financialfraudaction.org.uk/fraudfacts16/

Why financial services should accelerate biometrics adoption

Clayton Locke

Clayton Locke, Intelligent Environments

Keeping customer data and financial information secure is a constant battle for financial institutions of all shapes and sizes. Online fraudsters continue to find new, ingenious ways to steal personal data and hack into financial accounts. To combat this, the financial sector needs to be constantly strengthening its online security.

Traditionally, the initial identity verification process for a new customer has involved an arduous paper-based process. This is now being replaced with more streamlined digital automation – but the question then is: how do you keep data secure, while still providing a great customer experience? Clearly, biometric technologies are an important part of the answer to this. Yet many financial systems still depend on the password as the principal line of defence against hackers, even though consumers increasingly want banks to implement more secure measures – including biometrics such as facial recognition and voice verification – to protect their money and personal data.

The arduous paper-based process for verifying customers is being replaced with more streamlined digital automation: but how do you keep data secure, while still providing a great customer experience?

UK-based research by Intelligent Environments has found that over a third (37%) of consumers are likely to be swayed by the quality of security measures when choosing who to bank with, while 29% say they would be more likely to use a bank that offers biometric security. These findings demonstrate that biometric technology can no longer simply be regarded as a 'nice to have', it will actually attract new customers to the banks who adopt the technology. Increased market penetration and acceptance will be further supported as consumers get comfortable using biometrics on a daily basis using features like Apple's Touch ID. Meanwhile, there is clearly a growing concern among consumers that their personal data must be better protected at a time when news of high-profile cyber attacks is a frequent occurrence.

Yet despite the availability of new biometric technologies and the surge in consumer demand, the majority of banks have yet to adopt biometrics as a mainstream method for authentication. New biometrics are being released that offer increased security, but the financial sector continues to be slow to invest.

Ultimately, the longer the banks resist new technology and rely on traditional security methods, the greater the risk of successful attacks from ever more sophisticated and organised hackers. The recent attack on Tesco Bank is a prime example. While the full investigation hasn't been completed at the time of writing, it is very likely that multi-layered authentication, including biometric logins, could have thwarted that attack.

There are several reasons for this lack of investment among the banking fraternity, but the primary problem is cost. At present, the cash outlay to refund fraud or the penalties from personal data loss add up to less than the cost of implementing stronger security infrastructure. Currently, the difficulty sits with introducing biometrics and other security technology and connecting it with banks' existing legacy system estates. The implementation cost of cross-channel biometrics can be significant, with long-term benefits measured in the level of trust in a bank's brand. However, for the majority of mainstream banks, this long-term benefit doesn't appear to outweigh the short-term consideration of profit margin.

How secure are current biometric authentication systems? Mobile World Congress 2016 saw how fingerprint readers could be hacked with a fake finger made of clay.

Banks and security: BTT comment

Banks and financial services firms are the biggest target industry for cyber criminals. And since 2015, when it emerged that an international crime gang had used the 'Carbanak' banking Trojan to steal up to $1bn from over 100 banks across 30 countries, cases of successful hacking have continued to spiral.

There have been multiple attacks via the SWIFT international inter-bank messaging system, including last year's theft of $81m from the Bangladesh central bank. Banking fraud cases are also soaring, by 64% for online banking and 28% for phone banking between 2014 and 2015, according to consumer group *Which?*. In line with this, research by Intelligent Environments shows that nearly half of all UK consumers are concerned their identity will be stolen.

Faced with these threats, regulators worldwide have upped the pressure on banks to guarantee security. Last year, the world's G7 nations set out new guidelines for protecting the global financial sector from cyber attacks. US regulators also introduced new security standards for the biggest US banks, requiring them to use the most sophisticated anti-hacking tools and be able to recover from any cyber attack within two hours. A revised Payment Services Directive (PSD2) regulation is coming into force, which stipulates strong standards for how banks and online payments providers authenticate their customers' identities. The threat of technologically advanced challenger banks like Metro, Atom and Starling is also putting pressure on the mainstream institutions.

The large banks are themselves innovating in biometric-based security. As *BTT* has reported, this includes Lloyds/Bank of Scotland's recently launch of facial recognition technology for consumers opening bank accounts online, including a 'selfie' photo to confirm their identity. That follows Mastercard's introduction of a smartphone payment app using selfies, while this year Mastercard is due to launch Identity Check Mobile, a fingerprint and FR-based online payment app. Meanwhile, Barclays is using fingervein scanning authentication and Lloyds has pioneered 'phone printing', a kind of audio fingerprinting system that spots fraudsters who phone in impersonating legitimate customers. Other innovations include Ujjivan Financial Services' plans to introduce ATMs that use facial recognition in India.

Despite this, recent *Which?* research found that only five out of 11 banks tested were using two-factor authentication to check users logging into their online banking services. So the jury is out on whether banks are doing enough to earn consumer trust.

On the credit side, PwC's 2017 *Global State of Information Security* survey found that financial services organisations have increased their security spending 67% since 2013. Industry watcher Research and Markets has likewise forecast that the global banking, financial services and insurance biometrics market will grow by a CAGR of 20% through to 2020. And recent Visa research found that consumers are nearly twice as likely to trust banks to store their biometric information safely (60%) than they trust government agencies (33%). In contrast, research by Intelligent Environments shows that 22% of consumers don't trust digital banking apps.

One problem for the sector is that new issues are constantly cropping up. Witness the dramatic rise in mobile phone banking. According to Visa, over half of European consumers now regularly make payments via mobile devices – a rapid rise from less than 20% in 2015. Demand for new, convenient payment services like this in turn open up new opportunities for cyber criminals. The pressure on banks – from consumers, regulators, hackers and rivals – to adopt new biometric-based security will only increase.