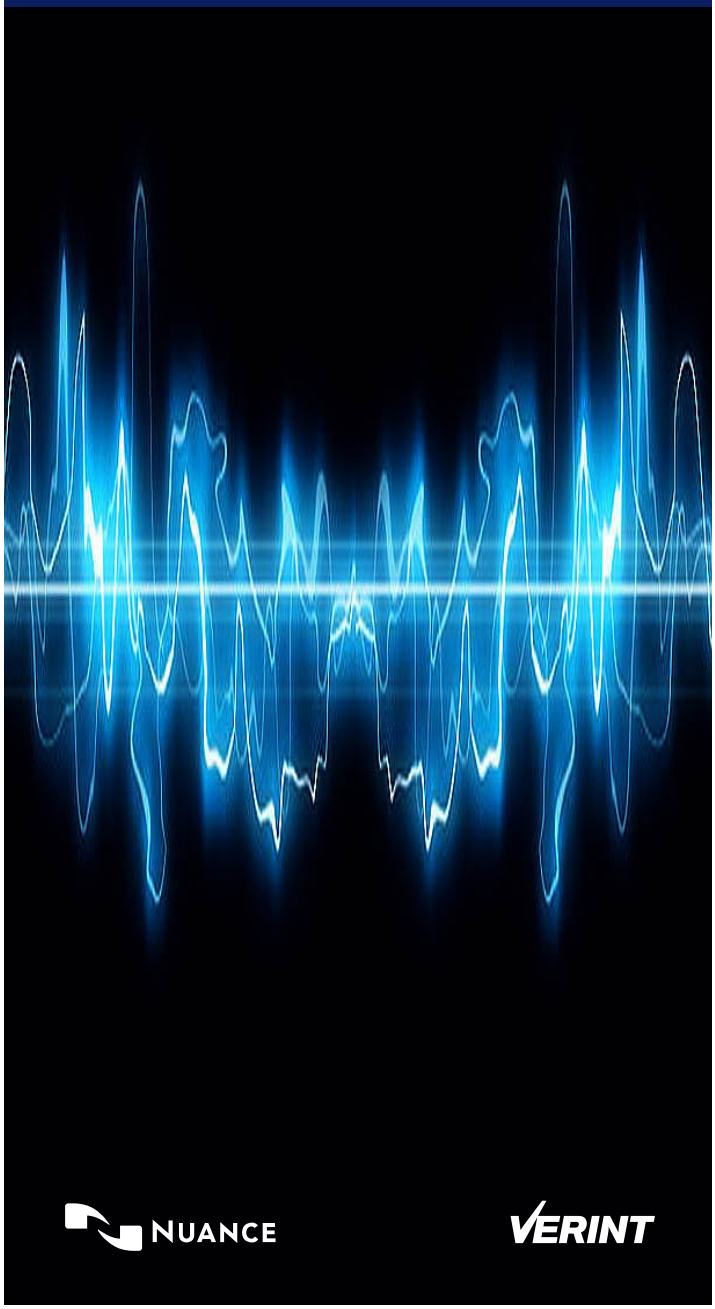
Voice Biometrics goes mainstream

By Dan Whaley
Speech Applications Consultant, Sabio



How the latest voice biometric technologies successfully balance security needs while still enabling a high quality customer experience

sabio

1. Fraudsters stepping up their game

In the Government's 2015 Information Security Breaches survey, research conducted by PwC suggested that nearly nine out of ten large organisations have suffered some form of security breach, with the figure for smaller organisations standing at 74%. This was up on the previous year, where the figures were 81% and 60% respectively.

Security breaches are clearly on the increase; however what's perhaps more disturbing for business is that the ultimate cost of these breaches is also escalating. When factors such as business disruption, lost sales, recovery of assets, fines and compensation are all considered, the average cost of a breach to a larger organisation now stands at some £1.46 million – up from less than half that figure a year ago.

For some the damage can be disruptive in terms of both cost and reputation. When TalkTalk was hacked last year, for example, personal data for over four million customers was stolen, and the brand's value in terms of share capital reduced by £360 million. Perhaps more disturbingly, analysts from Morgan Stanley estimated that the breach could result in a potential net loss of some 25,000 TalkTalk broadband customers over the next year.

What's clear is that fraudsters are stepping up their game, and it's not just the financial services sector that is at risk. Opus Research cites the annual Data Breach Investigation Report (DBIR) that lists 37% of breaches as affecting financial institutions, 24% in retail or restaurants, 20% in the IT and business services sector, and 20% across manufacturing, transport and utilities.

Opus Research also suggests that factors such as the consumerisation of IT, continued growth in hosted solutions, the move towards Bring Your Own Device at work, and the rise in mobility and widespread smartphone penetration are all combining to amplify potential security risks. Inevitably as consumer usage of increasingly powerful and connected PCs and smartphones scales, there is a proportional growth in the number of fraudsters with access to these kinds of devices.

2. Moving beyond traditional passwords

It's perhaps unfortunate that at a time when effective fraud solutions are more essential than ever, customers are becoming increasingly frustrated with traditional knowledge-based authentication solutions such as passwords.

As consumers we actively dislike the pressure of creating and remembering our usernames and passwords, and struggle especially when we have to remember multiple passwords and PINs. SplashData research shows just how bad we are at this. In its 2015 evaluation of North American and Western European users, the three most commonly used passwords were still 123456, password and 12345678. Leaving aside numerical sequences, other Top 20 highlights include qwerty, football, baseball, welcome, monkey and princess. So while we all pay lip service to data security, as individuals we're still poor at making things difficult for fraudsters.

Organisations are doing what they can to make password protection stronger, requiring that passwords are changed on a regular basis, that users come up with longer passwords, and that they apply a combination or letters, numbers and symbols. However, many consumers still respond by using their name and year of birth, their pet's name, or their favourite sports team's nickname. Fraudsters, with ready access to personal social media details, are proving increasingly adept at working these out, indeed Opus Research found that 'guessing, cracking or reusing valid credentials' factored into four out of every five breaches' according to the DBIR Report.

Perhaps as consumers we're too trusting. According to security vendor McAfee, over half of respondents to a recent survey admitted to sharing PINs or password information with their family and friends. Shared household services such as Netflix, iTunes or Amazon often also end up using the same passwords that are used for more sensitive interactions such as personal banking.

As the TalkTalk breach also showed, more complex passwords are still vulnerable when fraudsters reach further to compromise the customer database. As Opus Research highlights: "no matter how the PINs or passwords are compromised, once in the hands of a malicious individual or criminal organisation, the potential for large-scale financial losses are amplified considerably".

Balancing security with usability

While as consumers we clearly all have individual concerns about the security of our personal and financial information, we're also increasingly intolerant of those service providers whose processes are needlessly long and frustrating. Balancing these two positions has always proved challenging for customer service organisations, often leading to a conflict between a firm's customer service department and its compliance operation – that, historically, has served as the policing function.

A key factor in the drive to resolve this disconnect has been an increased focus on customer effort as a measure of business success. The customer effort measure is all about surfacing those issues across channels that are making life harder for customers. Once identified, these can then be systematically addressed to help reduce service costs, decrease customer churn and improve overall service levels.

However, it's no use customer service leaders complaining about compliance being a barrier to task success. With compliance pressures set to remain indefinitely, it's incumbent on those customer engagement teams and compliance departments to find a better way to interact with customers securely. If organisations are serious about reducing customer effort and building a more seamless experience, then it's essential to factor in security and authentication as part of the end-to-end customer journey.

It's of course imperative to reassure customers that their data is safe, however it should also be possible to develop an approach where levels of security are matched to the levels of risk involved. For example, users will be more willing to accept greater levels of security where the perceived risk is greater. So there need to be more security questions and processes in place for a higher value transaction such as a bank account transfer, for example, than there would be for a simpler address change or mobile phone top-up.

The goal here should be to address customer engagement concerns by removing as many overt security checks as possible where they really aren't needed.

Voice Biometrics Traits

Behavioural traits
Pronunciation / emphasis
Speed of speech / accents

Physical traits
Vocal track traits
Mouth shape / size
Nasal passages

That's where the latest biometric technologies can help, enabling customers to be verified based on their unique physical characteristics – whether it's their voice, fingerprint, face or iris. Identifying customers with biometrics provides the strongest levels of identity assurance, and – when compared to traditional PINs and passwords – offers significantly reduced exposure to fraud across the full range of criteria including theft, guessing, eavesdropping, hacking, phishing, vishing, smishing, credential sharing and social engineering.

For organisations looking for a better solution than traditional passwords, the shift towards more advanced authentication methods such as biometrics also opens up significant potential benefits in terms of usability, security and costs. And because multiple biometric options are available, the opportunity to create tiered levels of verification – perhaps combining fingerprint and voice biometrics - is set to play a key role in the crafting of more seamless and effective customer interactions.

3. Improving the user experience and reducing security risk through voice biometric

A year ago Visa Europe research revealed that 75% of 16 to 24 year olds would feel comfortable using biometric security, 69% thought it would be faster and easier than passwords and PINs, and that this demographic felt that passwords would be redundant by 2020.

Since then things have accelerated, with the widespread take-up of biometric authentication technology through the TouchID technology employed by Apple in their latest iOS devices. There's also been growing evidence from real-world voice biometric deployments of authentication success rates of between 95-99%, and some 90% of users of these solutions now say that they prefer voice biometrics over previous authentication approaches.

From a customer usability perspective, voice biometrics does away with the stress of having to remember passwords and related security questions, simply using the customer's unique voiceprint for authentication. A range of different voice biometric approaches are available: passive, where the user can say anything and the system matches their voice to a voiceprint, or more active – with the user required to repeat an agreed passphrase.

Whichever approach is chosen, the result for customers is a much more natural, effortless and accurate means of accreditation.

Service providers benefit from the security that comes from customer voiceprints that cannot be compromised by hackers. Voice biometrics cannot be compromised in this way, and the more that fraudsters engage via the contact centre, via IVRs or through mobile apps, they simply increase the likelihood that their voiceprint will incriminate them.

Organisations that have deployed voice biometrics already find that they can significantly reduce their authentication costs, indeed some now experience a process that is up to 80% faster than passwords and PINs. User acceptance is also growing – hardly surprising when 85% of customers were frustrated by previous security systems – and there's an increasing recognition that the assurance and reduced effort involved for customers can prove an important brand differentiator.

4. Assessing voice biometric approaches

Different voice biometric deployment models are available, ranging from Active and Passive approaches for the contact centre through to solutions for both mobile and web deployment.

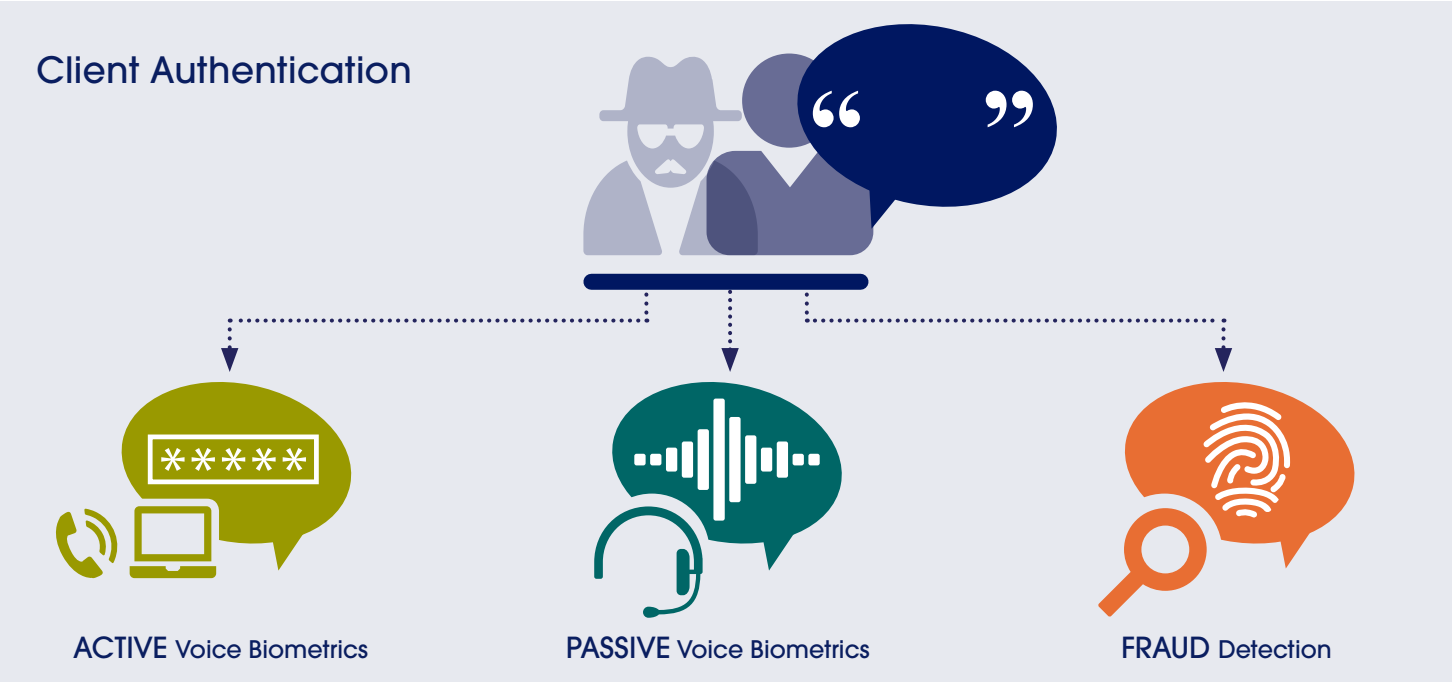
Active Voice Biometrics for contact centres

The 'active' voice biometrics approach is most commonly deployed as part of an IVR solution – replacing standard verification steps, such as requesting a caller's postcode or date of birth. Following an initial enrolment process – where customers complete a verification phrase such as 'my voice is my password' – the voice biometrics solution transparently analyses over 100 unique voice characteristics and compares these to those already stored on the customer voiceprint. This active solution sidesteps all of the traditional security issues associated with information-based approaches, providing seamless verification before customers are either offered self-service functionality or transferred to an agent as fully verified. Thanks to seamless integration with existing CTI and CRM systems, active solutions can also help improve contact centre efficiency by cutting call durations – while at the same time reducing potential fraud activity.

Passive Voice Biometrics for contact centres

These biometric solutions passively enrol the voices of known customers without needing specific passphrases. Following enrolment, the agent – or possibly the IVR – conducts a normal conversation and authentication takes place in the background. This reduces the number of security questions needed and shortens overall agent handling times. For organisations with an existing Verint Workforce Optimisation suite, this kind of passive voice biometrics approach can also take advantage of your existing recording investment.

Over time, passive solutions can enable customer engagement teams to provide a 'fast lane' for legitimate customers, with transparent enrolment and verification without any additional questions. Passive solutions also offer strong fraud detection by screening each call against a database of voiceprints of known fraudsters. Agents are provided with an alert if the caller doesn't match a known voice on the database, giving them the information they need to take appropriate action.



Voice Biometrics for mobile apps and web transactions

Voice biometrics can also be deployed as an additional security check for mobile app or web transactions, particularly those with a higher value. Voice biometrics works well here – in comparison to other biometric methods – because it is available across all channels and ensures a consistent user experience for customers.

Mobile app authentication via voice biometrics offers a significantly more secure and convenient gateway to any app that contains personal information or enables sensitive transactions. Similarly voice biometrics for web transaction validation represents a much quicker and easier-to-use authentication process – not only boosting completion rates but also reducing fraud.

With a range of voice verification options available – including text dependent, text independent and text-prompted - these kind of solutions will prove valuable for service providers needing to authenticate and verify customers across different channels and levels of security.

5. Voice Biometrics in action – unlocking cost and security benefits

Research continues to show that consumers are increasingly demanding a simple yet safe alternative to traditional passwords. New online consumer research findings from YouGov have revealed that 37% of consumers agree that traditional passwords have become an outdated security measure.

Voice biometric solutions directly address this challenge, and there is growing evidence from around the world that voice biometrics can deliver benefits for both customers and their service providers alike. Recent examples of successful voice biometric deployments include:

- **The Australian Taxation Office** - Using voice biometrics to authenticate callers, and with some 1.5m successful voice biometric enrolments, repeat callers are now experiencing a 40-45 second reduction per interaction in the average time that they are on the phone with an agent.
- **ING Netherlands** - Deploying voice biometrics to support voice-activated payments from within its mobile app. Offering a smart alternative to PINs and passwords, voice biometrics allows customers to use the sound of their voice from start to finish in the mobile app.
- **Banco Santander** - 19,000 former fire-fighters and police in Mexico City are working with an active voice biometric solution deployed by Banco Santander to prove their eligibility to receive transfer payments over the phone rather than having to go to a government office or branch bank.
- **HSBC and First Direct** - The largest planned deployment of voice biometric security technology in the UK was recently announced, in parallel with the roll out of Touch ID for mobile banking customers. Its new solution will deliver a more secure banking experience for 15 million UK customers.
- **Barclays Wealth & Investment Management** - Deploying an active voice biometric voiceprint solution, Barclays Wealth & Investment Management has successfully reduced customer authentication from up to four and half minutes of customer time to just 20-30 seconds of natural conversation using voice biometrics. Not surprisingly, it's proving popular with customers. Since its introduction more than 84% of Barclays Wealth customers have enrolled in the voice biometric initiative, and given its success the bank is now keen to expand the programme to its retail banking customers.
- **SK Telecom** - South Korea's leading mobile service provider SK Telecom is using an active voice biometric solution to transform the authentication process by replacing passwords with a simple yet secure means of accessing their account.
- **Turkcell** - With more than four million enrolled voiceprints, Turkcell's use of customer voiceprints makes it one of the world's largest voice biometric deployments in terms of scale.

6. Identifying voice biometric opportunities

With the escalating scale of voice biometrics deployments, particularly the UK's HSBC programme targeting some 15 million customers, it's difficult to deny that the technology has now gone mainstream. This level of widescale biometrics adoption will also help drive other service providers to catch-up.

HSBC has also made the adoption decision somewhat easier for those compliance officers who've perhaps been hesitant in entrusting their critical customer security to technologies such as biometrics. The fact that one of the world's largest banks is now firmly behind biometrics is sure to make it significantly more attractive from a risk management perspective. However, with voice biometrics now the smart choice for many of today's leading customer service organisations, how will the technology evolve?

Securing the Digital Front Door

As cross-channel customer engagement evolves towards a true Digital Front Door model, consumers will gravitate towards those organisations where the end-user experience remains consistent across self-service, social and more traditional assisted service models. With the majority of interactions now coming in from smartphones, and with the accelerated development of WebRTC voice-enabled browsers, organisations will need to design customer journeys that take full account of both security and service needs. Voice biometrics has a valuable role to play here, and its successful and consistent deployment across multiple access channels will prove an important brand differentiator.

Enabling tiered biometric verification

Multiple biometric options – such as fingerprint access, facial or iris recognition, and voiceprints – combine to provide organisations with the opportunity to design service journeys with more appropriate levels of security for specific tasks. For example, customers might complete their initial verification using a smartphone's fingerprint sensor, and then be asked to complete a further voiceprint verification test if they wish to process more complex or higher value transactions. Tiered biometric verification provides customer engagement professionals with the opportunity to apply the right levels of contextual security into cross-channel service journeys, removing the requirement to break out of web or mobile self-service journeys.

Internet of Things brings increased risk

With some research reports predicting up to 50 billion global Internet of Things (IoT) devices connected by 2020, it's clear that IoT connectivity has the potential to revolutionise business processes across the entire value chain. Customer engagement teams will need to prepare for the impact of a ubiquitous IoT-enabled world, and will need to think seriously of IoT as a key component of the customer journey – with associated security implications. Take devices such as Amazon Alexa, for example, and the implications of using this technology to manage home security technology such as alarms. Will a biometric voiceprint be required to permit access? These issues quickly move beyond simple technical concerns, and instead become a critical service design challenge.

7. Sabio – supporting voice biometrics deployments with a comprehensive services wrap

When it comes to designing customer journeys that strike exactly the right balance of customer effort and security, you need to be working with a specialist partner that's able to address all your business, usability and technical challenges.

At Sabio we understand the key role that security technologies such as voice biometrics play in impacting the customer experience. However, no matter how impressive the technology approaches involved, these can only prove successful if they're part of an intelligently crafted customer journey that's consistent across a wide mix of channels.

That's where Sabio can help. Having worked with leading voice biometrics technology provider Nuance since 2005, and as a specialist Verint Premier Partner since 2004, Sabio has an in-depth understanding of the different kinds of voice biometric technologies and solutions available – and can work with you to establish the optimum security approach for your business. Our track record as a leading Avaya Platinum Partner also means we're ideally placed to help integrate technologies such as voice biometrics with your core telephony and contact centre systems infrastructure.

So whether you're looking to deploy an active voice biometrics programme to support potentially millions of customers with personalised voiceprints, or if you want to supercharge your existing Workforce Optimisation deployment with additional voice biometrics security, Sabio has the in-depth business, user experience design and technical skills to help.

Voice biometrics experience backed by proven Speech Practice

With a track record of over a decade delivering successful speech-enabled solutions to leading organisations, Sabio's market-leading team of natural language speech recognition voice self-service, user experience design and security specialists is ideally placed to bring best practice expertise to your voice biometrics project.

To support its deployments, Sabio combines award-winning technologies - from vendors such as Nuance, Verint, Avaya, Semafone, LivePerson, Conversocial, Gamma, RMG Networks and others – backed by a comprehensive, end-to-end services wrap that covers business consulting, customer journey design and testing backed by our in-depth UX/UCD framework, systems integration, training and managed services components. When customers engage Sabio they benefit from our end-to-end capabilities, as well as a significantly less complex supply chain as we assume full responsibility for all aspects of our deployments.

EMEA
+44 344 412 3000
info@sabio.co.uk
www.sabio.co.uk

APAC
+65 6812 0560
info@sabio-apac.com
www.sabio-apac.com

sabio
@sabiosense