

## Voice Biometrics – The Contact Centre’s Security Solution

Voice biometrics is the answer to solving a range of security issues currently existing in contact centres, yet few companies are utilising this technology to date.

Voice Biometrics, what is it and how does it differ from speech recognition?

The application most of us are familiar with is Speech recognition, the technology that allows a computer to recognise what the human voice is saying. It is commonly used in call centres for steering calls to the appropriate agent and for numerous self-service applications as well as for voice dialling on a mobile phone.

Voice biometrics technology differs by using the nuances and characteristics of your voice, ‘*how you say things*’ to identify you as an individual. The sound of every person’s voice and the way they speak is unique. The best example of this is your ability to identify people who you regularly speak with over the phone, for instance your family and friends, without them having to say who they are.

There are two steps to biometric recognition. The first is enrolment, which requires users to positively identify themselves and have a sample of their voice characteristics captured. This is not a voice recording, it is known as a voice print, and is a digital ‘signature’ of the way you speak. The strength of the security of the biometric application is only as strong as the original voice print enrolment.

The second step is verification, and occurs when a user attempts to access the system. The characteristics of the user are compared to the characteristics of the voice print captured at enrolment, and the system assesses the probability that it is the same person. Depending on the probability assessed and the thresholds set, the system either allows the caller access, denies access or passes the caller to an agent for further identification.

The characteristics of your voice have similar ‘uniqueness’ to your fingerprints – even amongst family members. Occasionally same-sex twins have similar voice characteristics, but there are still differences that a good biometric application can usually detect. Many applications also contain ‘liveness’ testing to prevent someone recording your voice and playing it back.

Current security applications that are commonly in use in contact centres are inherently insecure. Below are two examples of commonly used means of identification.

***PIN Numbers:*** Despite warnings to the contrary, PIN numbers are often set to something easy to remember – a postcode or a family member’s birthdate, the first or last digits of a credit card or similar. While making the PIN number easy to remember, it also makes them easy for someone to guess. Further – and be honest here – who else knows your PIN number, family members? Are you absolutely certain that they have never inadvertently passed you PIN to someone else, or used it where it was visible to others?

***Personal Questions:*** Usually include your name, home address, date of birth and (depending on who you are talking to), health insurance number, credit card number or similar. Virtually all of these are kept in your wallet, purse or handbag & are therefore quite readily available to others.

These examples are usually used in conjunction with another piece of information like an account number and are known as two-factor identification – something you have (an account number) and something you know (a PIN number or date of birth). Using voice biometrics in conjunction with these adds a third factor – something you are. As this is a ‘physical’ factor it is significantly harder to use fraudulently as it is not possible to ‘steal’ someone’s voice or impersonate them to the degree required to access a system controlled by biometrics.

Security and useability are normally a trade-off. The security department would like to prevent anyone gaining access to data because then fraud would be impossible, but that would make a system unusable. A Customer Service Manager may want to allow everyone access because that would be the most convenient for the customer – unfortunately that is equally impractical as there would be nothing to prevent fraud.

Voice biometrics is a security system. Companies are using biometrics to control customers’ access to their own data (account information, financial information etc), as well as controlling staff access internally through password resets or similar as it provides a far higher degree of access control than anything else in use in contact centres or over the telephone today and is far more convenient for customers to use. It can’t be forgotten like a PIN or password, it can’t be mislaid like an account number and it can’t be misused by others.

The other good news is the cost of biometric solutions has dropped significantly over the past few years with multiple manufacturers on the market today creating competition and improving quality, making the solution ideal for many applications. In addition, Hosted (pay per use) alternatives are also available, removing the need for an up-front capital spend.

The success of a biometric application depends heavily on a number of factors:

- The underlying technology
- The design of the application
- The training of the users of the system
- The management of an extensive change and communication program to those supporting the system, and to the end users of the system

The way voice biometrics is implemented is equally as important as the technology itself. Some customers are very sensitive about providing a voice print, seeing it almost as providing their DNA and can be suspicious of how it will be used. Some confuse biometrics with speech recognition and recite poor experiences where ‘the system just didn’t understand me’. Others simply don’t believe the technology works and that it dramatically enhances security over anything else in use in contact centres today. More than with any other technology implementation, independent advice from a company experienced in biometrics is invaluable and can assist with:

- Evaluating and choosing the right underlying technology and technology vendor to suit the particular implementation and customer needs
- Evaluating the most appropriate ‘data elements’ to accurately identify your customer while maximising customer convenience
- Designing a change management and communication program for your staff and your customers to ensure the success of the implementation

- Designing and managing a rollout and implementation strategy
- Project and vendor management

Still a relatively new technology, Voice Biometrics will gain popularity quickly when the security benefits over the use of PINs, personal questions and other means of identification available today are fully realised. However the ultimate success of the technology will hinge on correct implementation, detailed change management and a communications program.

About the Author.

Steve Pels – Director, Contact Centre Action

Steve has worked in both the operational and technical aspects of the contact centre industry and specialises in optimising operational and management aspects of contact centres. Steve has extensive experience across many sectors and disciplines related to the Customer Contact Industry, is a regular Keynote speaker, and Chair of related conferences on Customer Contact topics and Best Practice topics locally and internationally. Since commencing Contact Centre Action, Steve has played major role in improving some of Australia's best known companies, including the implementation of high profile speech and biometric deployments.