



raising security to a new dimension

## Voice Authentication – Securing call centres and online services

### Identity Theft

In January 2003, Philip Cummings was sentenced to 14 years in prison for stealing identities. Over a two-year period, he used his position as a computer help-desk employee to steal personal information from more than 30,000 unwitting customers. He then sold credit card and other stolen details on to other criminals.

Judge George B Daniels said the case “*emphasised how easy it is to wreak havoc on people’s financial and personal lives*”, and added that consequences for individual victims were “*almost unimaginable*”. Losses were estimated to be between US\$50m (£38m) and US\$100m (£76m), making it the largest case of identity theft in U.S. history.

In Pune India, police arrested 16 people in an investigation into the fraudulent transfer of more than US\$400,000 from Citibank customer accounts in the United States to bogus accounts in India. Investigators said employees of a business process outsourcing company (BPO) used Citibank customers’ PINs to access accounts.

Whilst the amount stolen in this case was not large, it raised a significant issue on the credibility and trustworthiness of offshore call centres, with some commentators suggesting that the incident could trigger as much as a 30% down turn in India’s offshore call centre industry.

Identity-related fraud is now one of the fastest growing crimes in the world. Biometric technologies, including iris scanning, fingerprints and face recognition have long been touted as a solution to fraud. However, whilst these technologies have their place in the security market, speaker verification, or voiceprint technology, looks poised to be the application that may bring biometrics into widespread corporate use.

### A US\$2 Trillion Problem

Law enforcement agencies in the U.S. estimate that identity-related crime is now a US\$2 trillion problem and doubling every 12 months.

The Australian Institute of Criminology (AIC) estimates that in Australia, identity fraud costs the community between AUD\$2-6 billion a year, with a business losing more to fraud than to employee theft, burglary, armed robbery and vandalism combined. With over one third of all serious crimes involving ID fraud, this cannot only be a problem for law enforcement and national security, as the U.S. and Indian cases make apparent, but also a real problem for victims of ID fraud, both businesses and individuals.

With the trend towards providing services through call centres and the Internet, the opportunity for identity fraud has exploded. Over half of all identity fraud complaints are related to online activities.

In the physical world, establishing identity relies on documents such as driving licences, passports and certificates. With the advent of cheap, high quality copying equipment, relying on documents is increasingly an issue. Establishing identity in the virtual world is even more problematic. Individuals must remember and keep secure passwords and PINs which are notoriously weak forms of security. When they are lost or forgotten, customers must re-establish their identity – most often by calling a call centre and answering a sequence of personal questions. Costly and time consuming, this process does not necessarily establish that the caller is “*who they say they are*”. Furthermore, the call centre agent is also privy to their identity information, and as we have seen in the U.S. and India cases, consequences can be undesirable.

Whilst call centres and the Internet are convenient and effective ways of providing customer self-service, they are also the “*weakest link*” as far as identity fraud is concerned.



raising security to a new dimension

## Voice Authentication – Securing call centres and online services

### Combating Identity Fraud with Voice Biometrics

Voice authentication is one biometric with the potential for widespread use, particularly in call centres and online services. Voice authentication authenticates a person's identity from their unique vocal characteristics. In a nutshell, a person records a spoken password (such as their name or some other easily remembered information). This is analysed to extract their unique voice characteristics, which are then compiled into a "voiceprint", a matrix of parameters that encodes not only the password but the way the person says that password. This is stored in a database for future authentication of the same speaker.

During a transaction, to confirm an identity the person simply says the password information originally spoken during registration. The corresponding "voiceprint" is extracted from the database and the characteristics of each are compared. If they match, identity is confirmed and the transaction can proceed. As voice authentication relies on "voiceprint" information (and not a particular password or phrase), an imposter attempting to gain access to an account may say the correct password but will be rejected as he or she will have the wrong voice quality.

### Voice Authentication - Ubiquitous and Secure

A key benefit of voice authentication is that it works over the telephone - the world's most ubiquitous communications device found in almost every household and business worldwide. In other words, the infrastructure for the widespread rollout of biometric voice authentication is already in place, as one's identity can be authenticated from anywhere in the world simply by dialling a telephone number.

There is no need to invest in special sensors or scanners, or is there any need to invest in special authentication software or data communications technology. More importantly customers do not have to learn to operate new equipment or systems. They simply use the telephone.

These factors all add up to an authentication solution that is more cost effective, easier to implement, easier to manage and faster to deploy than other security options.

Voice authentication also offers enhanced security. As the technology is accessed by telephone, the authentication system can be centrally located in highly secure facilities with no connection to unsecured desktops, laptops and networks. Hence, there is no opportunity for "hackers" to break into the system, providing an extremely secure implementation for identity management and authentication systems.

When voice authentication is deployed in mass market applications, passwords and PINs become unnecessary, and call centre agent intervention becomes obsolete. Removing call centre agents from the identity verification process has the advantage of closing off another avenue for identity theft to occur. An additional benefit of this biometric deployment is automating a core call centre function for voice authentication reduces call centre operation costs.

### FAQs on Voice Authentication

In the past, there have been numerous questions regarding the performance of voice authentication:

- What happens if I have a cold?
- Can mimics break into my account?
- What happens if somebody records my voice?
- Can my password be decoded from the voiceprint?

Recent advances in voice authentication have addressed all of these questions.



raising security to a new dimension

## Voice Authentication – Securing call centres and online services

Studies by the National Centre for Biometric Studies at the University of Canberra confirm research by the UK Communications Electronic Security Group (the Information Security division of the British Government Communications Headquarters) demonstrating that voice authentication outperforms current fingerprint, hand print and face recognition products and has performance standards close to that of iris scanning.

Tests by Edinburgh University's Centre of Communications Interface Research, also covered in the University of Canberra study, showed voice authentication to be 99.9% accurate, which is 100 times better security than using PINs and passwords alone. In 2003, the International Biometrics Group in New York confirmed the highly competitive performance of voice authentication technologies for use in online financial services.

The effectiveness of voice authentication is further reinforced in the University of Canberra study for government call centre applications and online and automated services. In the University of Canberra study, the robustness of voice authentication was also studied to ensure secure operation for every day deployments such as mobile telephones and in high noise conditions.

Extensive testing has also shown that mimics are unable to fool the technology even when they know the passwords and PINs. The technology can also be configured to remain relatively insensitive to colds and flu. Unless highly sophisticated equipment is used, recordings also cannot fool the system.

To further strengthen security, however, voice authentication systems are usually set up to ask questions in a random sequence, thus making each session different from the last - preventing a previously recorded voice from being used. (In fact, speaker verification is now at the point where it is being deployed in highly secure government services and there are at least two vendors certifying their technology for defence applications.)

### Securing the Call Centre

The Australian Government's Office of Strategic Crime Assessment has stated that "*critical to the functioning of the economy is the requirement that stronger systems of proof of identity are developed*".

By applying voice authentication to front-end call centres and online services, there is no need for call centre agents to see or hear clients' personal information, PINs or passwords. Likewise, there is no need for callers to disclose such information to call centre agents. Callers simply authenticate their identity using their voice, and once authenticated, can be passed on to the agent anonymously. As such, the call centre agent can be certain that the caller is who they say they are but need not know any personal or security information about the caller.

Voice as a biometric identifier offers convenience and cost effectiveness in preventing security problems discussed above. By protecting personal information using voice authentication, the "*weak link*" in identity-related fraud in online and call centre services can be effectively addressed.

### About the Author

Dr Clive Summerfield is CEO of 3SH. Clive has been driving the adoption of speech recognition and voice authentication since the 1980s, with a key focus on massively scalable carrier-grade projects.

In 1990 Clive founded Syrinx Speech Systems where he implemented AT&T's USA based Customer Care application as well as applications for Commonwealth Bank's Australian Stock trading system. He introduced voice biometrics to Australian government agencies such as Parliament House and has recently undertaken an evaluation on voice authentication technologies sponsored by Australia's Centrelink.

Please visit [www.3sh.net](http://www.3sh.net) for more information.