

# INTERVIEW



As a Fraud and Biometrics Specialist for Nuance, Ian McGuire has many years of expertise in the biometrics industry. We spoke to him to find out about the latest trends and what the future holds for this exciting technology...

## **Tell us about how Nuance has grown to date and the changes you expect to see in the future.**

The Security Business within Nuance has grown to become one of the main revenue generators within the business. Over the last few years Nuance security products have become commonplace within the UK banking sector, with all of the major UK banks using Security Suite. Over the next 12 months we are anticipating growth in cloud-based solutions. While it is likely that large organisations will continue to want on-premise solutions (although even there we are seeing movement to cloud) the next tier of organisations are unlikely to want the expense of building and maintaining on-site solutions.

## **What challenges are organisations facing today that you feel biometrics can help to solve?**

I feel there are two primary challenges; customer convenience and combating fraud. Customers have never wanted, and expected, convenience more than they do today. Cumbersome security processes are likely to drive customers away so providing seamless, robust security is becoming the norm. Voice biometrics fits perfectly in addressing this challenge.

Thinking about voice biometric technology, it is clear that all organisations, banks in particular, suffer at the hands of professional, industrial-level fraudsters. We have demonstrated that voice biometrics using watchlists of known fraudsters has a huge impact on reducing fraud losses and disrupting the fraudsters.

## **How do you feel biometric technology can enhance customer experience to deliver great customer service for end-users?**

Customers don't really want to complete security, to them it's a necessary evil. They just want to complete their task, whether that's making a purchase, transferring money, or something else. By focusing on the human, rather than an indirect token (such as a PIN, or OTP generator) biometrics provides a more intuitive and seamless authentication process that will not interfere with the customer achieving their objective.

## **How can biometrics support the increased usage of digital identity?**

The key issue here, I see, is establishing trust! We need to educate, and re-assure people about the robustness of the security, but also, perhaps more importantly, that the creation of a biometric print

doesn't compromise an individual's rights. That is, they understand that a biometric print can't be subverted and used for a purpose beyond that which the person has given permission for. If we can build that confidence in both the reality and perception of security then we, as a society, can start to achieve the full benefits of biometric security. For example, liveness detection is important in building that confidence. People want reassurance that their identity can't be copied, and effectively stolen, by using a voice recording, photograph, etc.

### **How, in your opinion, can new technologies and regulations support authentication and satisfy the greater demand for security and trust?**

There needs to be more communication between technology providers, the organisations using the technology (banks, retailers, government, etc.), and the regulators to ensure that there is clear understanding on the capabilities and limitations of the technology. It is clear from some existing regulations, that the authors of the regulation did not understand what a biometric print is and how it can be used.

### **For those looking to deploy biometric technology in their organisation, or in their products, what are the key things that you would advise them to consider?**

When using biometrics for authentication in particular, an organisation must realise that it is not simply a technology deployment. Authenticating a customer is core to the trust relationship that exists between a customer and the organisation. As such, it must be viewed as a business solution that spans technology, customer experience, business processes, and communication. Simply put, regardless of how good the technology is, if you wrap it in a poor business process, causing a poor customer experience, or if you fail to communicate the benefits to customers, or address any concerns customers have, then your solution will fail.

Nuance Omni-Channel Customer Engagement

## **Biometric authentication and fraud prevention solutions.**

Reduce customer friction and deliver better CX

Powered by AI to detect and prevent fraud

Continuous across voice and digital channels

Trusted by 500+ brands globally with rapid ROI

**Protect your customers and combat fraud with multi-modal voice and behavioral biometrics.**

Learn more about how Nuance can help you protect your customers and your business—and make every customer interaction simpler, email us at [CXexpertsEmea@nuance.com](mailto:CXexpertsEmea@nuance.com).



Nuance and the Nuance logo are registered trademarks or trademarks of NuanceCommunications, Inc. or its affiliates in the United States and/or other countries. All other trademarks referenced herein are the property of their respective owners. Sept. 2019/0499

