standable concerns about gathering and using such data. System suppliers need to make clear to users the implications of providing their personal biometric data; and they need to be transparent in how they might use that data for other means. The FIDO (Fast Identity Online) Alliance advocates that a user's biometric traits should ideally be securely stored on the user's device as opposed to an external database. This is a commonsense approach to avoid the potential breach of a biometric database, such as occurred recently when the fingerprint data of 5.6m US Government employees was stolen[7].

So while the benefits of using ECG for enhanced security are clear, careful security design of a system is paramount. In line with that, systems that utilise a multimodal approach will always offer improved security. Yet despite privacy concerns, data collection is fast becoming the currency we use for connected service convenience. And as we live through a new era of data analysis, the provision of personal data is becoming increasingly accepted. Convenience and value perception will continue to be the main drivers for adoption.

> ***"ECG biometrics offer us greater security and safety in a world of risk, protecting not just our devices, apps and data but even our physical selves"***

Heart of our future?

In summary, ECG biometrics offer us greater security and safety in a world of risk, protecting not just our devices, apps and data but even our physical selves. ECG authentication, especially coupled with other biometric modalities, can provide the most powerful digital security available in the current market. If the value of using internal biometric data as an authenticator can be communicated, we could be looking at a world where your heart is key.

What's more, the potential extrapolation of insight from ECG-based data is arguably more exciting than its authentication usage alone. This data analysis could help us redefine industries and build new markets. The race is now on to harness the disruptive potential of such data and enable us all to benefit from this transformation.

About the authors

Adrian Condon is CTO and Grace Willatt is head of research at B-Secur. B-Secur offers biometric authentication using patented ECG technology which verifies users' identities through their individual unique heartbeat pattern, recognising that this is more secure, convenient and fraud-resistant than passwords, PINs or any external biometric authentication. For more information visit http://www.b-secur.com/.

References

1. George E Forsen, Mark R Nelson and Raymond J Staron Jr. 'Personal Attributes Authentication Techniques'. Pattern Analysis and Recognition Corporation, Rome, NY, US, October 1977. Accessed November 2017. http://www.dtic.mil/docs/citations/ADA047645.
2. Steven A Israel et al. 'ECG to Identify Individuals'. Pattern Recognition, Vol 38, No 1, 2005, pp138-142. Accessed November 2017. http://www.vrphobia.com/library/040521.pdf.
3. Peter Sam Raj and Dimitrios Hatzinakos. 'Feasibility of Single-Arm Single-Lead ECG Biometrics'. Signal Processing Conference (EUSIPCO), 2014.
4. Jim Dearing. 'Electronic Access Control'. IHS Markit Predictions for 2017, 24 January 2017. Accessed November 2017. https://technology.ihs.com/588015/electronic-access-control-ihs-markit-predictions-for-2017.
5. Halle Tecco and Megan Zweig. 'Digital Health Funding 2017 Midyear Review'. Rock Health, 2017. https://rockhealth.com/reports/2017-midyear-funding-review-a-record-breaking-first-half/
6. Annamalai Natarajan, University of Massachusetts Amherst; Kevin S Xu, University of Toledo; Brian Eriksson, Technicolor. 'Detecting Divisions of the Autonomic Nervous System Using Wearables'. Engineering in Medicine and Biology Society (EMBC), August 2016.
7. David Alexander. '5.6 Million Fingerprints Stolen in US Personnel Data Hack: Government'. Reuters, 23 September 2015. Accessed November 2017. https://www.reuters.com/article/us-usa-cybersecurity-fingerprints/5-6-million-fingerprints-stolen-in-u-s-personnel-data-hack-government-idUSKCN0RN1V820150923.

Biometrics becoming must-have for fraud prevention

Charlotte Hill

Charlotte Hill, freelance journalist

Over half of organisations are expected to significantly increase their investment in biometric technologies to prevent fraud and combat organised cyber-crime groups, according to a recent Callcredit Fraud and Risk Report[1].

After questioning 200 UK-based fraud and risk professionals, the report discovered that their biggest concerns are 'professional' cyber-crime, identity fraud, money laundering and social engineering (eg, phishing). Meanwhile, just under half the respondents regard the loss of data by an employee – either accident or intentional – as posing a greater risk than external fraudsters. However, the organisations questioned predict that their concerns are set to change over the next three years, with the majority

John Cannon, Callcredit: "With the major global breaches reported in 2017, leveraging technological advancements has never been more important to instantly verify customers, identify risks, and ultimately stay ahead of the fraudsters."

(55%) citing denial of access as the biggest potential security threat. This is followed by the accidental loss or compromise of data by an employee (50%) and the threat of ransomware (48%).

Sandra Peaston, assistant director of the fraud prevention service Cifas and author of 'Fraudscape', says that it's not surprising that organisations are therefore looking to biometrics to help overcome the problem of fraud. Pointing out that Cifas member organisations are recording hundreds of thousands of cases of identity fraud, she comments in the report: "Clearly, the personally identifiable information (PII) that is still the standard (names, address, birthdates, phone numbers, etc) and the 'what you know' element of the identification/authentication process is in the hands of fraudsters and being exploited."

Best biometrics

So in response to the fraud threat, which specific technologies and methods are organisations planning to adopt? To improve their identity verification procedures over the next three years, the Callcredit report finds that most respondents are looking to introduce more biometric screening techniques (26%), artificial intelligence systems (24%) and voice recognition systems (23%).

John Cannon, Callcredit's commercial director for fraud and ID, welcomes this focus on voice and other biometric ID checking systems: "With the major global breaches reported in 2017, leveraging technological advancements has never been more important for organisations to instantly verify customers, identify risks, and ultimately stay ahead of the fraudsters," he says. "Incorporating biometric and voice recognition technologies into their fraud prevention strategy will strengthen authentication process and reduce risks by allowing the verification of a person rather than just a credential, such as a password."

"The majority of organisations are still struggling to manage the potential conflict between customer acquisition and the need to validate identities when customers interact with them"

Looking into which biometrics measures organisations are planning to implement to combat fraud – and why – the Callcredit report suggests it's too early to accurately predict where, how and in which form reliable biometric services will be delivered. This view is shared by industry expert Alan Goode, managing director of cybersecurity analysis and consulting firm Goode Intelligence. He points out that a wide range of biometric methods are still being implemented across many sectors and across all channels, telling *BTT*: "It is really about matching the right biometric method to the channel. Voice works well in the telephony channel and helps reduce fraud levels and can identify known bad actors. For mobile, we are seeing a mixture of organisations leveraging built-in biometric methods. With fingerprint biometric authentication, Apple TouchID and native Android fingerprinting being prevalent these are the most favoured currently."

Alan Goode, Goode Intelligence: "Biometrics provide convenient frictionless user authentication that is proving very popular to millions of people around the world."

But Goode says that with the arrival of new biometric modalities on next-generation smartphones, we can expect to see multimodal methods, such as iris and face recognition, increasingly being adopted by organisations. "We are also seeing software biometric methods being integrated into authentication platforms, such as EyeVerify's Eyeprint ID being available in the RSA Adaptive Authentication mobile SDK. Biometric authentication provides convenient frictionless user authentication that is proving very popular to millions of people around the world," he says.

Meanwhile, the Biometrics Institute has released its '2017 Biometrics Industry Trend Tracker' survey[3], which offers further critical insights into latest trends in the use of biometrics for fraud prevention and other applications. According to the Institute's CEO, Isabelle Moeller, there will be a shift away from border control/security, mobile payments and device access as development areas. Instead we will move more towards online identity verification, government mobile applications, online payments/e-commerce and healthcare. She adds: "Other findings suggested that face dominates as the biometric thought most likely to be on the increase over the next few years, followed by multimodal and iris – all usurping fingerprint. Behavioural biometrics are also on the increase. Organisations favour these techniques because they strengthen the authentication process and reduce the risk for businesses by allowing the verification of a person rather than just a credential, such as a password."

Speed versus security

One issue stands out across all applications. Callcredit's report finds that the majority of organisations (74%) are still struggling to manage the potential conflict between customer acquisition and the need to validate identities when customers interact with them. Goode points out that biometric technology is aiding this process: "There are a number of very good applications that can verify a new customer's identity based on validating trusted physical identity documents, either by capturing physical print security features off a photo ID or even validating the biometric data held in a passport's chip," he says.

Industry expert Steve Cook, EMEA director of biometric authentication sales at Daon, believes that the issue of convenience versus security remains a hot topic in fraud