SPECIAL REPORT

Providing security in the electronic age

With traditional authentication methods such as passwords becoming redundant, new systems such as 3D and biometrics are fast developing

Thu, Apr 26, 2018, 00:00

Mimi Murray

With consumers having more on-demand expectations with most services nowadays, including in banking and financial services, it raises concerns about the safety and security of new payment mechanisms.

How safe and secure are new technologies that use authentication methods such as 3D and biometrics? And will these methods of authenticating improve end-user experience?

Tony Hughes, associate director, risk consulting at KPMG, says the on-demand expectation is especially true of the generation coming of age in 2018. They are now consumers, clients and voters and they expect instant payments.

“The idea of the bricks-and-mortar bank is no longer a model. You can go on the internet, create a bank account, authenticate, meet all the money laundering legislation and have a bank account in minutes and within an hour have a loan.”

But the question is, how do you do this in a way that is secure?

“2D is easy to break, we’ve all heard the stories of people holding up a photo to a phone. 3D is a new way to authenticate. One of the most secure methods is retina scanning but someone blowing light in your eye felt very intrusive. Now low-intrusion light does a predefined map of your face – it maps points of congruence,” he says.

Therefore, in the next five years it will not be unusual to see the use of iris scanning, finger-print scanning and facial recognition on mobile phones, he says. The use of a number of these together will provide strong authentication and will make the use of passwords redundant.

“It will then be down to the individual to protect themselves and banks will push risk and responsibility back on to the consumer. In the past, if someone stole your password, the bank would normally provide some remediation. But as biometrics get stronger, the banks will say authentication is so strong, it had to be you [making payment], therefore we take no responsibility.”

Blockchain

Blockchain is another technology being embraced by many. Louise Kidd, head of liability and financial lines at AIG Ireland, says they are using several new technologies, including blockchain, at AIG.

“Working together, AIG, Standard Chartered and IBM converted a multinational policy which required three local policies to be issued in the US, Singapore and Kenya, into a ‘smart contract’ that provides a shared view of policy data an documentation in real time. This whole system allows visibility into coverage, premium payment stages as well as automated notifications to the relevant stakeholders following payment events. It allows the client to possess a ‘single view of the truth’. No doubt, blockchain has a powerful role to play in the future of insurance and we will continue to work with our clients and brokers around the evolvement of blockchain and other technologies.”

Collaboration across sectors can help address concerns about security. The National Cyber Security Centre was develope in 2013 and is responsible for Ireland’s cyber security, with a focus on securing Government networks and assisting businesses and citizens in protecting their own systems.

"They are working on 12 steps to cyber security and that will be sector-neutral so anyone can use it – a major corporation or an SME can use the same model to build up their capability in terms of security.

"In terms of working together intra-sector, in the banking sector they already share information and collaborations are going on and whilst they are still competing in the same space, they share certain information for the prevention of fraud and to protect each others' assets," Hughes says.

Peter Oakes, founder of Fintech Ireland and former director of enforcement at the Central Bank, says there is a strong case for collaboration between incumbent banks and fast-scaling fintech and regtech.

"It is very difficult to incubate ideas critical for innovation and change in an environment as controlling as that of incumbent banks. However, the advent of change and narrower windows for compliance for things like payment services directives, including the European Banking Authority, strong authentication standards, the GDPR and of course network and information systems directive – all addressing cyber security – means that large traditional banks, insurers and investment companies don't have the bandwidth, while battening down the hatches, to look for innovative ways to implement sustainable long-term security technology measures. Plus the environment is changing rapidly, faster than incumbents with legacy systems can ever possibly keep up with.

Duty of care

He says incumbents such as banks owe a duty of care, and therefore must be careful who they let into their core banking platform.

"At the end of the day, it is the regulated bank that will be viewed as responsible for regulatory failures, including cyber security and data protection around their customers' assets – for example, data. More and more, value is moving to electronic form and away from cash and other tangible type assets," he says.

Of the €153 trillion of value of business-to-business transactions which will occur in 2018, 8.5 per cent (or $13 trillion) will be via non-traditional players such as Ireland's TransferMate, which is cited in the recent White Paper on *Big Money B2B Transfer*.

"With fintech players taking a bigger slice of the pie each year from banks, and margins on payments being continually squeezed, traditional banks and incumbents need to collaborate or exit. But it is wrong to think that all banks are sitting twiddling their thumbs. HSBC has launched a voice ID biometric authentication system, together with a selfie-based account registration system. Nonetheless, friction will remain a feature of the collaboration landscape between incumbents and fintech. Without trust, there is no collaboration, without collaboration, cyber security risks will crystallise, thereby eroding the trust of customers – it could be a vicious circle or downward spiral depending on how you look at it," Oakes says.

In terms of the end-user experience, Hughes says for the older generation, it may not enhance their experience at all, as many have not embraced technology.

"To millennials, this will be second nature. This is an enabler for them but for pensioners it will be a challenge," he says.

MORE IN SPECIAL REPORTS

D-day for data protection as penalties to be introduced for breaches of new laws

Ireland difficult to topple as global aviation leader

Chinese firms continue on acquisition trail

Ireland can offer Brexit solutions