What's the PASSWORD?

Ruth O'Toole is a solicitor working as legal counsel in Daon, an Irish company that provides identity software and services globally, including for border control systems for the US and Japan

Biometric technology is seen as a way to improve the security of online banking and payments. But what are the challenges and technology considerations? Ruth O'Toole enters her PIN

The European financial services market is becoming increasingly aware of the need for stronger customer authentication techniques to combat the rising levels of fraud in internet payments. Banks are also tuning into the experience of their customers, who are becoming increasingly frustrated by the need to remember multiple personal identification numbers (PINs) and passwords. Biometric technology is being advocated by the European legislative institutions as a way to improve security, and it is being chosen by customers as a way to improve their security experience.

The most recent European Central Bank figures show that fraud on card internet payments caused €794 million of losses across the EU in 2012 (up 21.2% from 2011). The latest draft of the *Payment Services Directive* (PSD2) introduces a number of measures to address this threat, including the concept of 'strong customer authentication' that includes the use of biometric characteristics as an approved method of authentication.

PSD2 requires payment service providers (PSPs), such as banks, to carry out strong customer authentication to verify customer identity before proceeding with electronic payment transactions (article 87). They must use two or more of the following elements:

- Knowledge – something only the user knows, for example, a password or PIN,
- Possession – something only the user has, for example, smart card or mobile phone, and
- Inherence – something the user 'is', for example, a biometric characteristic such as fingerprint, face or voice.

Just do it

Formal adoption of PSD2 is expected later in 2015, with implementation at national level within approximately two years. In the interim, pursuant to article 16 of the *European Banking Authority Regulation*, the European Banking Authority (EBA) issued *Guidelines on Security of Internet Payments* in December 2014. The guidelines set the minimum security requirements for PSPs across the EU. As one of the key measures to prevent internet fraud, the guidelines require PSPs to carry out strong customer authentication, in the same manner as PSD2, in order to verify customer identities before proceeding with an online payment. The guidelines are applicable from 1 August 2015 until the PSD2 requirements come into force. In accordance with article 16(3) of the *EBA Regulation*, competent authorities and financial institutions must make every effort to comply with the guidelines by incorporating them into their supervisory practices. The May 2015 table of compliance notifications compiled by

at a glance

- The level of fraud in internet payments is increasing
- The latest draft of the *Payment Services Directive* introduces a number of measures to address this threat, including the concept of 'strong customer authentication' that includes the use of biometric characteristics as an approved method of authentication
- There are challenges and technology considerations, but customers are demonstrating that they are ready for an alternative to passwords and PINs, which reflects the way that they use technology today

PIC: iSTOCK

the EBA shows that 24 national authorities, including the Central Bank of Ireland, intend to comply with the guidelines.

Let your fingers do the walking

In addition to improving security, biometric technology can be used to improve customers' experience. Customers are currently expected to remember numerous and complex PINs and passwords for an increasing number of online services. The challenge is compounded by the recommendation of service providers that each set of log-in details be unique and contain a variety of special characters. The Financial Conduct Authority in Britain has identified this as a particular challenge to vulnerable customers, such as the elderly, who have difficulty remembering passwords, and has recommended biometric authentication as a more user-friendly alternative. Instead of numerous PINs and passwords, customers can use their smartphones to authorise payments using their fingerprints, voice and face.

The use of biometric authentication, as provided for in PSD2 and the *EBA Guidelines*, is already a growing trend in the international banking sector. In July 2015, MasterCard announced that it is running a pilot of a service that will allow customers to approve online purchases using facial recognition on their smartphones. Also in 2015, a number of US financial service providers introduced biometric mobile banking apps. USAA Federal Savings Bank introduced a solution that includes face and voice recognition. The adoption figures for the USAA app currently stand at over 800,000. The USAA implementation demonstrates customers enthusiastically embracing a biometric alternative to multiple PINs and passwords. It is interesting to note that 50% of USAA members enrolled are 35 years of age and older and, of those in the older half of adoptees, 15% are over 65. This breakdown of adoptees by age appears to contradict a common assumption that the older generation does not trust, and cannot use, biometric technology. Customers who are now using smartphones and apps to navigate all areas of their lives have shown that, when given a choice, they are able and willing to use authentication techniques that reflect the way that they use technology today.

Challenge everything

There are some challenges associated with the use of strong customer authentication. Firstly, for strong customer authentication systems to be effective, strong customer authentication technologies must comply with recognised standards. The technology of one provider must have the ability to interoperate with the technology of other providers. Article 87 of PSD2 asserts that the EBA shall submit draft regulatory technical standards on the requirements of strong customer authentication to the European Commission within 12 months from the date of entry into force of PSD2. In the interim,


Halt! Who goes there?

the *EBA Guidelines* state that, when assessing compliance with the guidelines, authorities may take into account compliance with the relevant international standards.

In this regard, it is interesting to note the work of the FIDO (Fast IDentity Online) Alliance. This industry consortium of global stakeholders was launched in 2013 to address the lack of interoperability among strong authentication technologies and reduce reliance on passwords. It has developed standards for open, interoperable mechanisms for online authentications. Members include MasterCard, PayPal and Visa, along with a variety of technology providers. In June 2015, it was announced that the US and Britain were the first governments to join the alliance to provide input into the FIDO standards.

Secondly, all security measures must be ready to meet the challenge of attack. Unlike passwords and PINs, biometric systems and technology have the ability to develop and respond to attacks. The security of a biometric authentication system can be increased by:

- Using multi-factor authentication – this combines a variety of biometric techniques such as face, voice and fingerprint in a single authentication, so that the breach of one factor does not compromise the reliability of the others,
- Not permanently storing raw biometrics, such as a photograph or a voice sample – only biometric templates are stored, that is, the raw data is converted into mathematical computer code,
- Encryption of the raw biometric data and biometric templates, and
- Linking the user's mobile device with their authentication to block unauthorised access requests from other devices and locations using GPS.

Biometric technology itself continues to develop. Improvements are made to the hardware used for capturing biometrics (such as cameras and fingerprint readers) and the underlying biometric algorithms (computer formulae). Methods are being developed to differentiate between a live person being authenticated and a picture, video or voice recording of that person being used by someone else to gain unauthorised access.

Here's the science bit

The use of strong customer authentication requires a variety of technology considerations. The following observations are made with particular focus on the definition of 'strong customer authentication' in PSD2.

Firstly, the definition contains the concept of 'privacy by design'. An authentication procedure should be "designed in such a way as to protect the confidentiality of the authentication data".

In this regard, it is interesting to note that biometric authentication may be performed either on a central server or on a user's mobile device. There are competing advantages to each method. When using a central server, biometric data will be stored on the server. The advantages are that the user is only required to enrol once, and that enrolment can be accessed from multiple devices, for example, in a bank branch and on a mobile device. Also, server algorithms tend to be more accurate.

The alternative is that the biometric data remains on the mobile device on which it is captured. The advantage of this method is that, by storing biometric data on the mobile device of the individual being authenticated, rather than in a central data base, the risk of a database breach is eliminated. Any compromise of authentication data on a device is limited to the owner of that device. It cannot lead to a systemic compromise of authentication data of other bank customers. Device-based processing might therefore be considered as a way in which privacy can be designed into the authentication process.

It is important to note, however, that compromise of authentication data on a mobile device would be restricted to accessing the biometric template on that device. This template or conversion of the raw data (such as a photograph) into mathematical code would contain less personally identifiable information than the 'selfies' most users have on their smart phones.

Secondly, the definition of strong customer authentication in PSD2 also contains the concept of mutually independent authentication factors. Authentication factors must be "independent, in that the breach of one does not compromise the reliability of the others".

The classic example in a banking context is 'chip and PIN'. The two authentication elements are possession (chip/smartcard) and knowledge (PIN). The breach or loss of the chip/card is not commonly thought to compromise the reliability of the PIN – that is, if you lose your bank card/chip, your account is not at risk, as no one else can use your card without your PIN. However, it is interesting to note that this banking standard has been challenged by a number of computer scientists, who claim to have identified a flaw in the PIN verification feature of the chip-and-PIN protocol that allows a card to be used without knowing its PIN. It is in this context that the third authentication element of inherence, and the use of biometric technology, may come increasingly to the fore.

> **'Unlike passwords and PINs, biometric systems and technology have the ability to develop and respond to attacks'**

Taking care of business

The level of fraud in internet payments is increasing. The European financial services sector is actively addressing this challenge. Biometric technology is being advocated as an authentication element of choice by the European legislative institutions and the EBA. There are challenges and technology consideration, but customers are demonstrating that they are ready for an alternative to passwords and PINs that reflects the way that they use technology today.

look it up

Legislation:

- *European Banking Authority Regulation* (Regulation (EU) no 1093/2010)
- *Payment Services Directive* (2013/0264/COD)

Literature:

- European Banking Authority, *Guidelines on Security of Internet Payments* (19 December 2014)
- European Central Bank, *Third Report on Card Fraud* (February 2014)