Earlier this year we conducted a YouGov survey to find out more about consumers’ attitudes towards the risk of fraud, and what they deem appropriate when conducting financial transactions online.

Cyber and identity fraud is on the up, with data-driven identity fraud accounting for over 45% of all confirmed frauds identified in the first three quarters of 2014. Add to that an increasing number of services being offered online, we were interested to take a closer look at the perceived risk by the consumer. What is the attitude towards the risk of fraud, and what security measures consumers deem appropriate when conducting financial transactions online?

In February 2015, Equifax commissioned YouGov to conduct a survey around these themes. A general fear of fraud and scamming was a clear thread throughout, especially when it came to using online services. Looking at the results, what can organisations do to reduce this fear and help reassure customers that their accounts and personal details are safe?

Fear of scamming
Many people's fear of scamming appears to revolve around the means of communication with financial services providers. The results show that 32% of UK adults prefer face-to-face contact, while 19% would prefer to speak over the phone and just 15% would opt for contact via the web. While this might not be what the industry wants to hear, as face-to-face interaction is a lot more expensive than phone or web, this illustrates consumers’ fears about managing their finances online.

However, there is no need for financial service providers to rush to open lots of new branches. Interestingly, when asked how they would prefer a financial services provider to get in contact with them, the same percentage of respondents – 29% – said they would prefer to be contacted via email as via post (i.e. letter).

This is, nonetheless, a minority. When asked which contact methods would cause most concern about potential fraud, email communication topped the list, with 58% stating they would worry when contacted via email compared to only 16% who would worry about a letter being an attempted scam. Does this indicate that the perceived risk of email outweighs the convenience?

Increasing education
With this fear of fraud and potential scams in mind, it’s interesting to see that 35% of people feel that their bank doesn’t communicate with them very much (or at all) about the security measures they have in place.

Could a lot of the fear around the perceived risk of using financial services online be eradicated by more or better information? By educating and informing their customers about the security measures they use, and how these help protect them from fraud, organisations could possibly persuade consumers to move away from costly face-to-face interaction.

It’s all about the balance
The survey shows that people are generally happy to answer more security questions for higher value transactions but not so keen when it comes to day-to-day transactions.

Not a surprising result in itself, but it highlights the importance for financial service organisations to continue to find a balance between the risk of fraud (to their business and customers) and the frustration experienced by a customer during the transaction.

One way to do this is to set parameters within an authentication and identity process which adapts the level of security and checks to the relevant transaction, meaning that a customer conducting a small transfer of funds between accounts doesn’t have to go through the same stringent process as a new client applying for a mortgage.

Use of new technology
Respondents did recognise that security measures are necessary: the survey revealed that almost as many people would be happy to use fingerprint recognition (31%) as passwords (32%).

This is reassuring, as we can see that the use of fingerprint recognition and other biometrics, such as facial and voice recognition, is becoming more recognised and more widely used within the industry. Biometric identification will soon become commonplace across multiple payment platforms, as well as phones and NFC payments (contactless cards). We know that many banks are looking to enrol devices at interaction points and use fingerprints to authenticate a person’s identity, helping to secure the consumer without the need to remember multiple passwords and PINs.

Voice biometrics will do the same for call centres, lowering security challenges but raising the standards of security. The key is to make security checks flexible according to the risk or cost of a transaction, while maintaining a level of efficiency to avoid frustrating legitimate law-abiding customers by posing unnecessary security check questions.

However, there is no need for financial service providers to rush to open lots of new branches. Interestingly, when asked how they would prefer a financial services provider to get in contact with them, the same percentage of respondents – 29% – said they would prefer to be contacted via email as via post (i.e. letter).

This is, nonetheless, a minority. When asked which contact methods would cause most concern about potential fraud, email communication topped the list, with 58% stating they would worry when contacted via email compared to only 16% who would worry about a letter being an attempted scam. Does this indicate that the perceived risk of email outweighs the convenience?

Increasing education
With this fear of fraud and potential scams in mind, it’s interesting to see that 35% of people feel that their bank doesn’t communicate with them very much (or at all) about the security measures they have in place.

Could a lot of the fear around the perceived risk of using financial services online be eradicated by more or better information? By educating and informing their customers about the security measures they use, and how these help protect them from fraud, organisations could possibly persuade consumers to move away from costly face-to-face interaction.

It’s all about the balance
The survey shows that people are generally happy to answer more security questions for higher value transactions but not so keen when it comes to day-to-day transactions.

Not a surprising result in itself, but it highlights the importance for financial service organisations to continue to find a balance between the risk of fraud (to their business and customers) and the frustration experienced by a customer during the transaction.

One way to do this is to set parameters within an authentication and identity process which adapts the level of security and checks to the relevant transaction, meaning that a customer conducting a small transfer of funds between accounts doesn’t have to go through the same stringent process as a new client applying for a mortgage.

Use of new technology
Respondents did recognise that security measures are necessary: the survey revealed that almost as many people would be happy to use fingerprint recognition (31%) as passwords (32%).

This is reassuring, as we can see that the use of fingerprint recognition and other biometrics, such as facial and voice recognition, is becoming more recognised and more widely used within the industry. Biometric identification will soon become commonplace across multiple payment platforms, as well as phones and NFC payments (contactless cards). We know that many banks are looking to enrol devices at interaction points and use fingerprints to authenticate a person’s identity, helping to secure the consumer without the need to remember multiple passwords and PINs.

Voice biometrics will do the same for call centres, lowering security challenges but raising the standards of security. The key is to make security checks flexible according to the risk or cost of a transaction, while maintaining a level of efficiency to avoid frustrating legitimate law-abiding customers by posing unnecessary security check questions.
The need for device recognition

Interestingly, 54% of respondents state that they use more than one device to access their personal accounts. With several devices used by over half of the respondents, linking several devices to multiple accounts, the ability to recognise which devices are being used for fraudulent activities is key. The usage of device recognition technology allows organisations to look beyond direct evidence of fraud by identifying whether a device has been associated with fraud on other websites. More importantly, it helps reduce the number of good customers being rejected.

Equifax has launched a new identity and fraud solution using the latest evolution in multi-layered progressive authentication. Equifax Progressive Authentication performs dynamic risk-based authentication in a single process, allowing you to validate genuine customers and screen out fraudsters. For more information on our work in identity verification and fraud prevention, please contact John Marsden on 07789 996557 or email john.marsden@equifax.com.

All figures, unless otherwise stated, are from YouGov Plc.

Idea in brief

THE SITUATION

What are consumers’ attitudes towards the risk of fraud, and what do they deem appropriate when conducting financial transactions online. Earlier this year we conducted a YouGov survey to find out.

THE CHALLENGE

Consumers want to communicate with financial institutions in the way that suits them best and are open to different layers of identity authentication for different levels of purchase.

THE TAKE AWAY

Fraud – and scamming – is still something consumers are concerned about and they’re looking to organisations to better communicate with them to ensure they know how to prevent identity theft but also what steps they’re taking to protect them.

54% of respondents state that they use more than one device to access their personal accounts