Cyber-security breach at Equifax

Thank you for your letter of 11 October 2017 concerning the security breach at Equifax (by which I refer to Equifax Limited, the UK company, as opposed to Equifax Inc. in the US). I have addressed each of your questions below.

I regard this matter extremely seriously given the potential harm caused to consumers. The FCA is carrying out an investigation into the matter and we are constrained by the confidentiality requirement in legislation around information provided to us by the firm. I would add at this stage it is likely that we have not yet discovered all the information that will be relevant to our investigation. That said, we have sought to provide full answers to your questions, and I would be happy to provide a further reply once our investigation is complete.

I would also note that in my view, risks around data security, alongside other cyber-related risks, are increasing in their significance and something that firms and authorities more broadly need to prioritise.

When did Equifax first notify the FCA of the breach?

We first became aware of a breach through media coverage on the morning of Friday 8 September 2017. We immediately contacted the firm to understand the nature of the event and to ensure appropriate steps were being taken to respond. We worked with the Information Commissioner in responding to the news.

Is the FCA satisfied that Equifax Limited has identified all UK individuals affected, and the data that has been potentially compromised in each case?

Equifax Inc commissioned a cybersecurity firm, Mandiant, to investigate the extent of the breach. Equifax reported in a press release of 10 October on the potentially affected data relating to UK persons. It is for a firm, in this case Equifax, rather than the FCA to interrogate data sets in order to identify the number of affected UK customers.

The firm has confirmed that a file containing 15.2 million UK records dating between 2011 and 2016 was attacked. The firm has identified that this number could be sub-divided into different categories of consumer depending on the types of personal data and other records that had been compromised.
The largest of these was a category of 14.5 million records containing a combination of name and date of birth with no other identifying characteristics.

The firm also identified four other categories, totaling 693,665 customers, who had more significant data accessed, including their driving licence numbers and email address associated with their Equifax.co.uk account in 2014.

Our engagement with the firm continues and the protection of all affected UK customers is a matter that we have made clear to the firm must be at the forefront of its considerations consistent with its regulatory obligation to treat its customers fairly.

It is important that the firm uses its best endeavours to ensure it has identified all impacted customers within each of the category breaches. We are aware that where the firm only holds name and date of birth information, making contact will be more difficult.

In summary, and in answer to your question, while the time taken by the firm to establish and report the full facts, is in itself an issue for us, and we are concerned that the firm uses all reasonable steps to make customers aware, we have no reason to challenge the conclusions on identification. That said, our investigation continues.

Is the FCA satisfied with the timescale over which Equifax plans to notify affected individuals, and the means by which it proposes to inform them?

The unauthorised access occurred from mid-May through to July 2017. As noted above, the timing of notification is one subject of our investigation.

We have made it clear to the CEO, as we would to any firm in a similar situation, that we expect contacting affected customers to be the firm’s top priority and that it should use all necessary resources to contact them as quickly as possible. We have also asked the firm to assess whether it is able to share information on affected customers with their banks to enable the banks to target their fraud detection technologies.

Where possible, the firm is writing to consumers whose personal data have been compromised, offering support on the steps that need to be taken to minimise the risk of possible criminal activity. At the same time we have impressed upon the firm that it should take all reasonable steps to ensure that its communications do not give rise to any further data breach. For example, some consumers may be sceptical about any email communications from the firm given the fact email addresses were compromised. Conversely, if it were to become known that Equifax is contacting affected consumers by email, then this may allow those that may have accessed this data to defraud consumers.

Which principles for businesses and FCA rules are engaged by this incident?

Credit reference agency firms are subject to the high level principles of the FCA regulatory regime, which include requirements on treating customers fairly and on ensuring adequate risk management, systems and controls. They are also subject to relevant data protection legislation which is enforced by the Information Commissioner’s Office (ICO). While our investigation is under way, it would be inappropriate at this stage for us to comment publicly on what rules might potentially have been engaged.

Which customers suffered the breach: those of the credit reference agency, those of the credit broker, or both? Would your response change depending on which part of the business was affected?

This particular breach relates to the firm’s credit reference agency activities, rather than credit broking. However, similar rules and principles apply to both activities.
Does the FCA consider that principles, rules or threshold conditions for authorisation may potentially have been breached? Has it appointed investigators and/or issued a Notice of Appointment to Equifax Limited?

Threshold conditions are at all times applied to an authorised firm. The FCA is conducting an investigation, as noted above.

What are the implications for the enforcement options available to the FCA of the fact that the data breach occurred at Equifax Limited’s parent company, Equifax Inc? Did the “process failure” (Equifax’s words) that caused the data on UK individuals to be held by the US parent potentially break any FCA rules, and do such intra-company data transfers compromise the ability of the FCA to meet its consumer protection objective?

If an authorised person outsources an important operational function in relation to customer data to a third party (who may be in the UK or another country), a key feature of FCA regulation is that the authorised person remains fully responsible for discharging all of its obligations under the regulatory system. Firms cannot delegate any part of this responsibility to a third party. In principle, therefore, the fact that an authorised person may have an outsourcing arrangement in place does not alter the effectiveness of the FCA’s toolkit of powers or its ability to secure an appropriate degree of protection for consumers.

If data transfers between companies are adequately controlled and appropriate oversight is applied to them then they should not of themselves compromise our ability to meet our consumer protection objective.

Does the FCA consider that it has powers to establish a consumer redress scheme to compensate affected individuals, were such a scheme to prove necessary?

In general terms, the FCA does have the ability to require a firm to make redress in appropriate cases. This includes the ability to require a firm to conduct a review or take remedial action. In this particular case, our focus at present is on ensuring that appropriate action is taken to protect consumers who are at risk of harm from the data-breach. It would not be appropriate for us to comment at this stage on whether redress or remedial action beyond this is necessary or likely in this particular case.

Has the FCA reached an agreement with the ICO on which body is most appropriate to investigate this matter? Please could you provide a brief account of the division of responsibilities between the FCA and ICO in this case?

The FCA and ICO have an established Memorandum of Understanding in place and have worked co-operatively since we became aware of the data breach on 8 September 2017. As we have different regulatory remits and enforcement options open to us, we would always seek to ensure that the authority with the most applicable regulatory powers leads on that area of exploration or action. This is an approach that would also apply to any potential formal investigatory action.

The implications of such breaches for the future of financial services data sharing initiatives and on the FCA’s supervisory approach under the Second Payment Services Directive.

Data security has been at the forefront of our thinking as we have developed our approach to implementing the Second Payment Services Directive (PSD2).

PSD2 will bring into regulation certain online services which allow customers to access their accounts indirectly through third party providers – account information services (AIS) and payment initiation services (PIS). With the customer’s consent these services can allow the customer to see all their bank accounts in one place in a mobile app or online. They can also be used to pay for things online, as an alternative to using a debit or credit card.
As with other businesses involved in data sharing, FCA regulated businesses must also comply with obligations under data protection law including the General Data Protection Regulation, which comes into effect in May 2018. We have and will continue to engage with the ICO on the matter of PSD2 and the broader implications of increased data sharing in financial services. We will continue to coordinate with the ICO as per our memorandum of understanding which recognises that we have separate but overlapping mandates. We want consumers to enjoy the full benefits that these changes will bring. However, we expect all businesses we regulate to put in place effective procedures to keep customers’ data safe. We recognise that the new opportunities afforded by open banking come with similar data security risks that we see in other sectors. As more customers choose to use and share their financial data, new and existing firms seeking to provide services using these data could become targets for criminals.

PSD2 seeks to address this risk. First of all it brings AIS and PIS into regulation for the first time. Businesses seeking to provide such services must, in respect of those services:

- satisfy us that they have processes in place to file, monitor, track and restrict access to sensitive payment data;
- provide us with a security policy document including a detailed risk assessment and the mitigation measures taken to adequately protect payment service users against risks identified including fraud;
- provide a programme of operations to cover the nature of the service being provided to the customer, how the customer's data will be used, and how the applicant will obtain appropriate consent from the customer; and
- provide their business continuity and disaster recovery plans which should include failure of key systems and the loss of key data.

Once authorised or registered, these firms will be required to meet new FCA reporting requirements which include notifying us within four hours of any major operational or security incidents, including cyber-attacks and providing operational and security risk assessments on an annual basis.

I hope you find this response helpful. If you have any further questions, please do not hesitate to get in touch.

Andrew Bailey
Chief Executive