Client Alert: Equifax fined by UK Data Protection Regulator

Date : September 21, 2018

This week the UK Information Commissioner's Office (ICO) issued a monetary penalty of £500,000 to the data broker Equifax Ltd for its part in the data breach at its parent company, Equifax Inc. This wasn't just a fine about the breach however and the case has some additional interesting aspects.

To simplify things in this note we're calling Equifax Ltd Equifax UK and Equifax Inc Equifax US.

What is the background to the case?

The penalty relates to a cyberattack on Equifax US in May and July 2017. Around 146 million customers globally were affected, including many in the UK.

Equifax UK provided services in the UK and it used Equifax US to process some of that data on its behalf.

What did the ICO determine?

The investigation was carried out under the Data Protection Act 1998, rather than the current GDPR or Data Protection Act 2018, as the failings occurred before GDPR came in. The £500,000 fine was the maximum allowed under the previous law.

The ICO carried out an investigation with one of the UK's financial services regulators, the Financial Conduct Authority. The investigation looked at Equifax UK's data handling in a number of areas – this case was not just about data security.

It decided:

1. That although IT systems in the US were compromised, Equifax UK was responsible for the personal information of its UK customers.
2. Equifax UK failed to take appropriate steps to ensure that Equifax US was protecting the information. Equifax US had failings in its IT practices including patch management and audit procedures.
3. Equifax UK contravened five out of the eight data protection principles of the Data Protection Act 1998 including failure to secure personal data, poor retention practices, and lack of legal basis for international transfers of the data. The eight data protection principles in the old law are similar to the six principles in GDPR so this aspect of the case is also useful when looking at how GDPR is likely to be enforced. As an example data was retained on the US system even when that part of the service had been relocated to a UK server. That breached the obligation in data protection law not to keep data for longer than is necessary.
4. A growing trend in data protection cases is regulators taking action when the data controller has not been transparent with data subjects. That was a feature in the recent Emma's Diary case (see http://www.corderycompliance.com/ico-emmas-diary-data-disclosure-failure-case/) and it's a feature of this case too.
5. Equifax US had been warned by the US Department of Homeland Security about a critical vulnerability in March 2017. Sufficient steps to address the vulnerability were not taken.
6. Security is a board level responsibility – the Information Commissioner said when announcing the fine "*Multinational data companies like Equifax must understand what personal data they hold and take robust steps to protect it. Their boards need to ensure that internal controls and systems work effectively to meet legal requirements and customers' expectations*."

The ICO's full decision can be found here: https://ico.org.uk/media/action-weve-taken/mpns/2259808/equifax-ltd-mpn-20180919.pdf

What are the lessons to be learned?

There are many lessons to be learned in this case, both technical and legal. This case was decided under prior data protection law, the Data Protection Act 1998 (DPA 1998) which has now been replaced by the General Data Protection Regulation (GDPR) and in the UK by the Data Protection Act 2018 (DPA 2018).

Lessons to be learned from this case for compliance with the new regime include:

1. GDPR plans are still important – some companies haven't finished their GDPR planning but took a break after the deadline passed. That's unlikely to be a wise decision. Data breaches often shine a light on other issues – such as retaining too much data or not putting steps in place to hold data processors to account. Any GDPR readiness plan needs to be reviewed regularly to check that you're still making progress.
2. Rehearse data breaches regularly – data breaches are inevitable in most organisations. You'll need to do your best to prevent breaches happening but you'll also need to plan what to do when breaches occur. Our Data Breach Academy can help as part of that process and we can tailor data breach rehearsals to match your organisation. There are more details here: http://www.corderycompliance.com/cordery-data-breach-academy/.
3. Victims of a data breach have more power – in this case Equifax US seemed concerned about class actions from victims from the very start. It tried to limit their ability to sue. This is unlikely to work. The BA breach tells us that class action lawyers will be out of the blocks very quickly. Appearing reasonable and responsive to victims is essential. In the UK civil actions like this are on the increase and notable cases include the Home Office spreadsheet case (see here: http://www.corderycompliance.com/uk-appeal-court-ruling-on-spreadsheet-data-breach-damages-case-2/), the Morrisons supermarket case (see here for our article and film: http://www.corderycompliance.com/client-alert-morrisons-data-breach-litigation-succeeds), and the Vidal-Hall/Google case (see here: http://www.corderycompliance.com/vidal-hall-data-protection-class-action-appeal-settled/).
4. Look at intra-group arrangements – part of the fine for Equifax UK was in not having proper measures in place to supervise the data handling of Equifax US. In some cases it might be appropriate to have an external check done on a data processor, even if it's a related entity. There's a little bit about our work in this area here: http://www.corderycompliance.com/assessment-and-review/.
5. Look at transparency – it is important to be clear with data subjects about what you're doing with their data. That might mean you'll want to review privacy policies on a regular basis. Look at other parts of your website too to check you're not making exaggerated claims about how secure data is.
6. The fines in this case were imposed under the DPA 1998 rules where the maximum imposable fine was £500,000. Under the new regime fines for serious breaches may be imposed of up to a maximum of 4% of total annual global turnover or €20 million, whichever is the greater. So, had this case been determined under GDPR the fines would likely have been far greater.
7. You'll need a strategy for transferring data outside of the EEA, even if you're sending the data to an affiliated entity for processing. Our Privacy Shield FAQs have more on some current concerns here: http://www.corderycompliance.com/privacy-shield-faqs/
8. There can be consequences for management – the Information Commissioner made it clear in this case that security is a board level responsibility. Equifax is also facing litigation alleging that its management did not take their responsibilities seriously and has faced calls from investors for the removal of board members – see for example https://www.bizjournals.com/atlanta/news/2018/04/17/iss-recommends-investors-vote-out-5-equifax-board.html

We report about data protection issues, including breaches, here: http://www.corderycompliance.com/category/data-protection-privacy/. For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film
- A template data breach log
- A template data breach plan

- A template data breach reporting form

For more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

For more information please contact Jonathan Armstrong or André Bywater or who are lawyers with Cordery in London where their focus is on compliance issues.