ICO flexes its muscles on data protection fines

For some time, we've been waiting for the first substantive fines from the Information Commissioner's Office (ICO) relating to the General Data Protection Regulation (GDPR) or Data Protection Act 2018. To date, the ICO fines have related to old Data Protection Act 1998 breaches (capped at £500,000) or failure to pay data protection fees. Now, the ICO has announced its intention to impose a record-breaking £183m fine on British Airways for personal data breaches.

The build-up

In the lead up to implementation of the GDPR, the higher limits for fines was one of the main headline-grabbers (and certainly got the attention of many boardrooms when allocating time and resource for their compliance projects). The jump from £500,000 to the higher of 4% of worldwide turnover or €20m was a huge one, but many asked if these higher limits would ever realistically be reached. If so, it always appeared likely that the fines would relate (as most do) to either a large data breach or widespread misuse of data.

The French data protection authority (CNIL) has already issued a €50m fine against Google in relation to its use of data for advertising purposes, but until now we haven't had any indication that the UK would follow suit in the size of its fines.

Judgment day

The data breach in question is believed by the ICO to have started in June last year (just after the GDPR, and higher fines, came into force) and affected up to half a million customers' payment details.

The ICO's investigation found that the airline had "poor security arrangements" in place to protect details such as log ins, payment cards, and travel bookings.

The fine amounts to around 1.5% of BA's 2017 turnover. For comparison, the biggest pre-GDPR fine for data security issues was £500,000 imposed on Equifax, in a breach involving the data of up to 15 million UK citizens.

It's difficult to compare the scale and severity of breaches, but if the BA fine is 37.5% of the maximum (£183m compared to a maximum of £488m), for a breach involving 500,000 individuals' data (in circumstances where BA maintains that it found no evidence of fraudulent activity on accounts linked to the theft), it's clear that the ICO's previous fines for companies like Equifax and Facebook would be considerably higher if the GDPR limits applied.

What next?

BA has indicated it will be appealing the level of the fine, and the ICO may well see this as a test case for determining future figures.

It's worth remembering that the ICO will take a number of factors into account when determining the level of a fine. In particular, the fact that a breach has occurred does not necessarily mean there has been a breach of the GDPR/DPA 2018. The ICO in this case found that BA's security measures were not compliant, but some types of breach will always be a threat, even if a company has state of the art security in place.

You can't make yourself completely invulnerable to data breaches, but you can ensure that you have well thought out security policies and procedures which are monitored, tested and updated. If ever there was an effective reminder to look at your security protocols, this is it.

Elliot Fry

Managing Associate