Data Privacy and Cybersecurity

British Airways data breach: what happened to £163 million of the proposed fine?

By: Kelly Hagedorn

On 16 October 2020, the UK Information Commissioner's Office (ICO) issued a Penalty Notice (the Notice) against British Airways (BA), imposing a £20 million fine in respect of BA's 2018 data breach. This is a significant fine and is substantially higher than any fines previously levied by the ICO. However, it is also significantly less than the £183 million that the ICO indicated it was planning to fine BA when it issued its notice of intent to fine in July 2019. So what happened?

Background

BA notified the ICO in September 2018 that its website had been attacked by a third party, resulting in the personal data of almost 500,000 individuals being exfiltrated by the attacker. This information included credit card details, as well as contact information and booking details.

In July 2019, the ICO indicated that it planned to fine BA £183 million for breaches of the General Data Protection Regulation (GDPR) that led to the attacker being able to access the website and obtain BA customers' personal data. Read further about what the ICO said publicly at that time in our client alert. Had a fine of that size actually been imposed on BA, it would have been the largest fine to date imposed under the GDPR. The final figure of £20 million is still the fourth largest GDPR fine but is clearly significant orders of magnitude less than originally thought.

Why the difference?

The ICO acknowledges that BA made a series of representations to it after the publication of the proposed fine. These representations contained updated factual information about the breach, some of which has weighed in the ICO's decision to impose a smaller fine.

However, the main reason for the reduced amount appears to have been the procedural approach taken by the ICO when setting the proposed fine. As the Notice makes clear, when arriving at the proposed £183 million, the ICO not only took into account its Regulatory Action Policy (RAP) – the published guidance around the ICO's fining policy – but also something known as the Draft Internal Procedure (DIP). As the name suggests, the DIP was both a draft document and one that was internal to the ICO. Although the ICO has not published a copy of the DIP, it appears that it adopts an approach to fine calculation that is based on the relevant controller or processor's turnover. If that is the case, it is not hard to see how using the DIP, the ICO could have arrived at a proposed figure of £183 million.

In its representations, BA complained about the ICO's reliance on the content of the DIP to calculate any fine. The Notice does not provide details of BA's complaints, but it seems that the ICO accepted them. The Notice specifically states that the guidance in the DIP has formed no part of the decision to fine BA £20 million.

How did the ICO arrive at £20 million?

When using only the guidance contained in the RAP, and considering all of BA's representations (many of which are redacted in the Notice for security reasons), the ICO concluded that the appropriate starting point for the calculation of a penalty was £30 million. A discount of £6 million was applied to

account for the mitigating actions BA took, and a further £4 million was deducted under the policy that the ICO has adopted to respond to financial hardship caused by the COVID-19 pandemic. This resulted in a total fine of £20 million.

Does this indicate that ICO fines will be significantly lower than previously thought?

In BA's case, this is what has happened. However, it should not be expected that the trajectory will be for lower fines. On 1 October 2020, the ICO issued draft statutory guidance on the RAP. This document expressly moves towards using a controller or processor's turnover as the starting point for the calculation of a fine. Although the DIP is not available, it appears that the new draft statutory guidance is proposed so as to implement the DIP's approach to fining into a new public document that the ICO will be able to rely on when setting penalties in future.

Although the statutory guidance is in draft and is open for public consultation, it is a signal of the ICO's intention to cement its ability to calculate fines based on the turnover of the relevant organisation. The reduction in the BA fine may well not be a sign of things to come.

Contact Us

Kelly Hagedorn

khagedorn@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower

Chair

dbitkower@jenner.com

Download V-Card

David P. Saunders

Co-chair

dsaunders@jenner.com

Download V-Card