ICO Proposes £183m Fine for British Airways GDPR Breach

July 9, 2019

The Information Commissioner's Office ("ICO"), the UK's data protection supervisory authority, has announced that it has issued a notice of its intention to fine British Airways ("BA") £183.39m for infringements of the General Data Protection Regulation ("GDPR"). The fine is the first proposed by the ICO for infringements occurring since the GDPR came into force. If it holds, the penalty would be by a large measure the biggest ever issued by the ICO and the largest by any regulator under GDPR.

Debevoise & Plimpton

The proposed fine arises from an incident which in part involved user traffic to the BA website being diverted to a fraudulent site through which customer details were harvested. It is believed that personal data of approximately 500,000 customers were compromised in this incident. According to a press release issued by the ICO, the investigation has found that a variety of information was compromised by poor security arrangements at BA, including log in, payment card, and travel booking details as well name and address information. While the ICO press release contains few details of the specific security concerns, public sources have previously noted that it may have been the case that the hackers used a cross-site scripting attack, identifying a poorly secured webpage component and injecting their own code into it to alter the victim site's behaviour.

The final decision on the sanction to be imposed has not yet been taken. The ICO has said that BA will have the opportunity to make representations on the proposed findings and sanction. BA has stated publicly that it will vigorously pursue that opportunity, including through appeal stages if necessary.

There has been no suggestion that BA was anything other than the victim of a criminal hack. The ICO announcement does not specify the details of its legal or factual position. But it appears that the ICO is acting on the view – by now familiar among civil regulators – that a corporation that is undisputedly the victim of a cyber crime can nonetheless be held civilly responsible, if its pre-breach security somehow fell short of the "appropriate" level required by GDPR Article 32.

The ICO has been investigating this case as lead supervisory authority on behalf of multiple EU Member State data protection authorities. Representations by other concerned data protection authorities will also be taken into account before the final decision is issued. It is notable that while the ICO has fulfilled the role of lead supervisory authority in this case, had the breach occurred post-Brexit, BA could have faced a separate fine from other EU data protection authorities.

As an intention to issue the first fine in the UK under the GDPR regime, the announcement is highly significant and dispels any doubts over whether the ICO will be prepared to use the new powers available to it. Since the GDPR and the UK's Data Protection Act 2018 came into force in May last year, the ICO has had the power to impose a civil monetary penalty on companies of up to £17m (20m Euro) or 4% of global turnover. It is reported that the proposed fine is around 1.5% of BA's annual turnover.

The announcement also continues the ICO's recent practice of publicising its intention to issue fines before the final decision is made. In June 2018, the ICO published the notice of intention to issue a fine to Facebook for failing to protection users' personal information. The fine itself was issued over four months later, in October 2018, so it may be some time before BA discovers exactly how much it will need to pay. One difference in the approach of the ICO this time around is that it has not published the full notice of its intention to fine BA. The ICO faced allegations of bias from Facebook for, amongst other things, publishing the notice of intention itself before Facebook had an opportunity to respond.

With members of its Cybersecurity & Data Privacy group on both sides of the Atlantic, Debevoise is well-placed to assist EU and non-EU businesses on all areas of GDPR compliance, including cyber incident preparation, incident response, and interaction with data protection authorities.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Stephanie M. Cipolla
smcipolla@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

LONDON

Jane Shvets
jshvets@debevoise.com

Christopher Garrett
cgarrett@debevoise.com

Robert Maddox
rmaddox@debevoise.com

FRANKFURT

Thomas Schürrle
tschurrle@debevoise.com

Friedrich Popp
fpopp@debevoise.com

PARIS

Alexandre Bisch
abisch@debevoise.com