CLIFFORD

CHANCE

ICO ANNOUNCES SIGNIFICANTLY REDUCED GDPR FINE FOR BRITISH AIRWAYS

OCTOBER 2020

ICO ANNOUNCES SIGNIFICANTLY REDUCED GDPR FINE FOR BRITISH AIRWAYS

The ICO has issued a Penalty Notice fining British Airways £20m for infringements of the GDPR, a significant reduction of £163 million from the fine originally indicated by the ICO.

In a long anticipated announcement, the Information Commissioner's Office (ICO) has issued a Penalty Notice against British Airways Plc (BA) for infringements of the General Data Protection Regulation (GDPR). Although the ICO had indicated a year ago that it intended to fine BA over £183m, it has announced that the penalty will be only £20m, underscoring the critical role that representations can play in such cases.

The fine relates to a cyber incident, believed to have begun in June 2018, in which the personal data of approximately 500,000 BA customers was compromised.

The proposed £183m fine had equated to 1.5% of BA's global turnover for 2017 (far under the GDPR maximum penalty of 4% of global turnover) – and while the £20m outcome is significantly less than that, it is still the largest penalty levied by the ICO to date.

Whilst the Penalty Notice refutes BA's representations and criticisms of the fine, it does not identify which representations were accepted or the specific factors that resulted in the substantial reduction of the fine.

In addressing BA's procedural criticisms, the ICO concluded, without providing specifics, that "*through issuing the [Notice of Intent], BA was afforded the opportunity to use the consultation process to make meaningful representations which were capable of affecting the outcome of the investigation … The Commissioner rightly took all of the material submitted by BA into account, which necessarily resulted in further clarity being brought to the circumstances of the Attack and a more detailed decision being produced.*"

As explained in detail below, after considering BA's representations, the ICO concluded that a £30m fine was appropriate. This was, however, further reduced by £6m to account for various mitigating factors and by £4m to account for the impact that Covid-19 has had on BA's financial position.

The Penalty Notice highlights the significant impact representations can have on the level of the fine imposed. We analyse the decision further below.

Key takeaways from the case

1. **Cyber security must be prioritised and companies must keep pace with emerging industry expectations.** The ICO stressed that "*it is for the controller to consider what measures are appropriate for securing its system*". The ICO criticised BA for the following errors:
   a. the lack of multi-factor authentication on the relevant system;
   b. the fact that the username and password of a privileged domain administrator account was stored in plain text on a folder on the server; and
   c. the fact that credit card details were being stored as a result of a testing feature error, and were being retained in plain text (as opposed to encrypted form). The ICO pointed out that the Payment Card Industry Data Security Standard guidance makes clear that CVV codes should never be stored.
2. **Any technical response must be swift and decisive.** BA was informed on 5 September 2018 that data was being extracted. Within 90 minutes, BA had adapted the malicious code and contained the vulnerability and 20 minutes later, BA blocked the URL paths. BA's prompt action was referenced by the ICO when calculating the fine.
3. **Once the data breach has been identified, prompt communication with data subjects can help mitigate enforcement exposures**. On 6 September, the day after the incident, BA notified the ICO, acquirer banks and payment schemes and an initial group of 496,636 customers, with a further 39,840 customers being notified on 7 September 2018.
4. **Focus on support of affected data subjects is critical.** BA put in place dedicated support for affected data subjects and considered how their loss and distress might be mitigated; it offered to reimburse financial losses resulting from the attack, and made available a free credit monitoring service. Again, the ICO expressly identified this as a mitigating factor.
5. **Cooperation with the ICO may take some time, but the potential financial benefits of engagement can be significant.** BA provided multiple sets of submissions to the ICO on both technical issues and BA's financial submission. In doing so, BA would have considered carefully the risks of a prolonged process, versus the potential benefits of cooperating fully resulting in a reduced penalty.
6. **Turnover is key, but not the only quantification metric.** The fine originally proposed by the ICO was focussed on BA's turnover. The ICO has stressed that turnover remains "*a core quantification metric*"– amongst other relevant factors. BA focused on those other factors in its representations – including the impact of coronavirus.
7. **Max fine – 2% or 4%?** BA sought to draw a distinction between an infringement of Article 32 of the GDPR (where the maximum fine is 2% of global turnover (Article 83(4))) and of Article 5(1)(f) of the GDPR (where the maximum fine is 4% of global turnover Article 83(5)). The ICO disagreed, highlighting that the two provisions overlap.
8. **No admission of liability**. Notably, BA did not admit liability for the breach of the GDPR. A key factor here is likely to have been the ongoing civil litigation that BA is facing in the English Courts, where BA will have been fully aware that the ICO's decision will be scrutinised by the civil claimants. This underscores the need for a company's enforcement and civil claims defence strategy to be managed in parallel.

BACKGROUND

On 4 July 2019, the ICO issued a Notice of Intent (NOI) to impose what would have been a record-breaking fine of £183.4m on BA for infringements of the GDPR. We wrote about the background to the GDPR breach and proposed fine **here**.

Summary of the cyber attack

Between 22 June and 5 September 2018, BA was the victim of a cyber-attack in which the attacker gained access to an internal BA application through the use of compromised credentials for a Citric remote access gateway:

- The attacker is believed to have potentially accessed the personal data of approximately 429,612 customers and staff. This included names, addresses, payment card numbers and CVV numbers of 244,000 BA customers.
- Other details thought to have been accessed include the combined card and CVV numbers of 77,000 customers and card numbers for 108,000 customers.
- Usernames and passwords of BA employee and administrator accounts, as well as usernames and PINs of up to 612 BA Executive Club accounts, were also potentially accessed.

Statutory process

The ICO is the United Kingdom's designated 'supervisory authority' for the purposes of the GDPR, pursuant to section 115(1) of the Data Protection Act 2018 (DPA). As such, it has the power under Article 58(2)(i) GDPR to fine data controllers/processors for breaches of the GDPR.

Where the ICO is satisfied that a controller or processor has breached its obligations under the GDPR, it can issue a penalty notice under section 155(1)(a) DPA 2018 requiring them to pay a fine (calculated by the ICO in accordance with their fining guidelines).

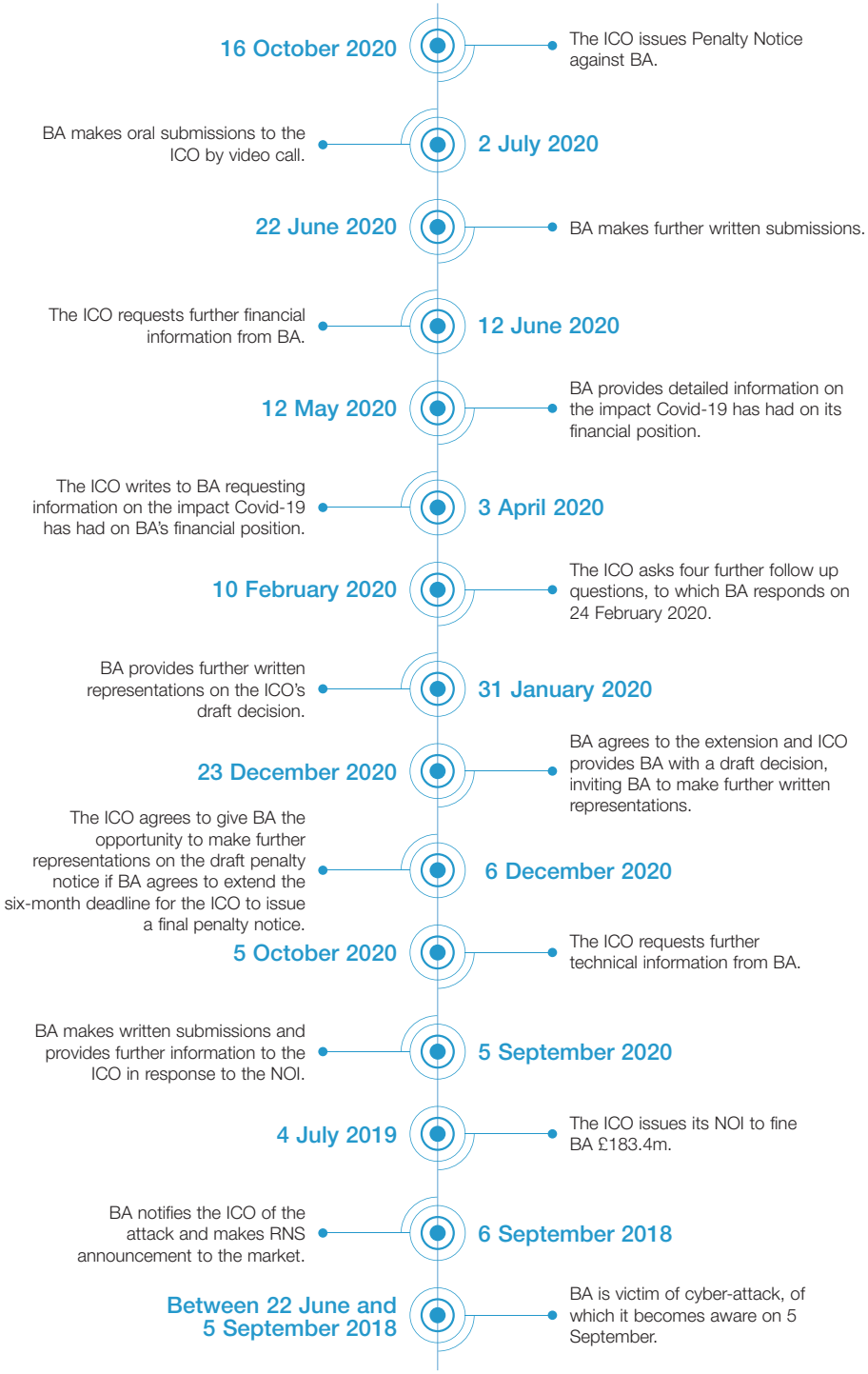
However, before it does so, it must first issue a 'notice of intent' to the relevant party to inform them that it intends to issue a penalty notice (section 155(5) and paragraph 2, Schedule 16 DPA 2018).

In accordance with the ICO's Regulatory Action Policy (RAP), once a notice of intent has been issued, it will take representations from the relevant party relating to the imposition and quantum of any penalty.

The DPA allows the ICO six months within which it should issue a penalty notice following a notice of intent. For BA, that would have required a penalty notice in January 2020. However, paragraph 2(3) of Schedule 16 DPA enables the ICO and the subject of the proposed penalty notice to agree to extend this period.

BA enforcement timeline

The key steps in this case were as follows:



The ICO's findings

Notably, BA does not admit liability for the breach of the GDPR. However, in the Penalty Notice, the ICO found that BA had failed to comply with its obligations under Article 5(1)(f) and Article 32 GDPR by failing to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Specifically, the ICO noted that BA failed to:

- follow industry guidance, including guidance published by the National Institute for Standards and Technology and the National Cyber Security Centre, and failed to take appropriate measures to prevent the initial unauthorised access;
- adequately identify and take measures to mitigate risks associated with remote access, such as limiting access to applications, data and tools to only that which are required to fulfil a user's role;
- take measures to prevent attackers from obtaining privileged access details (e.g. protecting employee and third party accounts with multi-factor authentication – which the relevant BA system did not have in place); and
- undertake rigorous testing, in the form of simulating a cyber-attack, on the business' systems and failed to implement file integrity monitoring, which would have detected malicious action such as that which occurred during the attack.

Calculation of the penalty

The ICO, like some other UK regulators, applied a five-step approach to calculating the BA penalty, which are set out in its RAP:

Step 1	An 'initial element' removing any financial gain from the breach.
Step 2	Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) of the DPA.
Step 3	Adding in an element to reflect any aggravating factors.
Step 4	Adding in an amount for deterrent effect to others.
Step 5	Reducing the amount (except the initial element) to reflect any mitigating factors, including ability to pay (financial hardship).

The ICO did not add an "initial element" as per step one of the procedure as BA did not receive any financial benefit from the breach (as might be the case, where, for example, a company has misused data for its own commercial benefit).

In applying step two, the ICO had regard to the factors listed in Article 83(2) GDPR. In assessing these factors, the ICO noted that BA was negligent in processing a significant amount of personal data in an insecure manner. Moreover, BA was only notified of the data breach by a third party.

At the conclusion of step two, the ICO determined that a baseline fine of £30m would appropriately reflect the seriousness of the breach.

Per steps three and four, the ICO further determined that it would not be appropriate to increase the level of the fine to account for any aggravating factors or as a deterrent.

At step five, the ICO considered whether there were any mitigating factors that might reduce the level of the penalty, and specifically noted the following points:

- BA took immediate measures to mitigate and minimise any damage suffered by the data subjects by implementing remedial measures;
- BA promptly informed the affected data subjects, other law enforcement and regulatory agencies, and the Commissioner, and fully cooperated with the ICO thereafter;
- widespread reporting in the media of the cyber-attack is likely to have increased the awareness of the risks posed by cyber-attacks and the need to ensure that other data controllers take all appropriate measures to secure personal data; and
- the attack and subsequent regulatory action has adversely affected BA's reputation, and will have therefore reinforced the importance of ensuring that personal data is adequately protected.

In light of these mitigating factors, the ICO determined that a 20% reduction of the fine, from £30m to £24m, would be appropriate.

In addition, the ICO considered the impact Covid-19 has had on BA's financial position and noted that "*although the Covid-19 pandemic has had a significant short to medium term impact on BA's revenues and its immediate financial position, the [ICO] considers that the overall financial position of BA and its parent company IAG is such that the imposition of a penalty in the range being considered will not cause financial hardship.*" Nevertheless, the ICO determined that a further £4m reduction in light of the Covid-19 pandemic was appropriate, resulting in the final penalty payable by BA to be £20m.

ICO consultation on DPA penalty calculation

Interestingly, on 1 October 2020, the ICO launched a public consultation on draft statutory guidance that proposes to amend the process by which it calculates penalties under the DPA. Under the proposed guidance, the ICO would calculate penalties using a nine-step process, detailed below.

Step 1	Assessment of seriousness considering relevant factors under section 155 DPA 2018.
Step 2	Assessment of degree of culpability of the organisation concerned.
Step 3	Determination of turnover.
Step 4	Calculation of an appropriate starting point.
Step 5	Consideration of relevant aggravating and mitigating features.
Step 6	Consideration of financial means.
Step 7	Assessment of economic impact.
Step 8	Assessment of effectiveness, proportionality and dissuasiveness.
Step 9	Early payment reduction.

In the Penalty Notice, the ICO noted that it had used an unpublished "draft internal procedure for setting and issuing monetary penalties" when calculating its proposed fine for BA in the NOI. BA criticised this aspect of the fine calculation process and the ICO then "*agreed that the Draft Internal Procedure should not be used in the present case.*"

It may be that the new statutory guidance is an attempt by the ICO to publicise this internal procedure so that it can rely on it in future penalty calculations. The ICO stated that the purpose of its internal policy was to "*provide a guide, by reference to the turnover of the controller, as to the appropriate penalty*," and the statutory guidance, which is still subject to public comment, inserts at step three a determination of turnover.

APPEALS

It has been reported that BA intends to accept the penalty, although section 162(1) DPA gives any party the right to appeal the Penalty Notice to the First-tier Tribunal (Information Rights). If it were to decide to do so, BA must ensure that its appeal is received by the Tribunal within 28 days of 16 October 2020.

CONTACTS

Kate Scott
Partner
T: +44 20 7006 4442
E: kate.scott@
cliffordchance.com

Sam Ward
Partner
T: +44 20 7006 8546
E: samantha.ward@
cliffordchance.com

Alex Sisto
Senior Associate
T: +44 20 7006 4092
E: alex.sisto@
cliffordchance.com

Ellen Lake
Senior Associate
T: +44 20 7006 8345
E: ellen.lake@
cliffordchance.com

Jonathan Kewley
Partner
T: +44 20 7006 3629
E: jonathan.kewley@
cliffordchance.com

Simon Persoff
Partner
T: +44 20 7006 3629
E: Simon.Persoff@
cliffordchance.com

Herbert Swaniker
Lawyer
T: +44 20 7006 6215
E: herbert.swaniker@
cliffordchance.com

Tom Dyer
Lawyer
T: +44 20 7006 5086
E: tom.dyer@
cliffordchance.com

Arnav Joshi
Senior Associate
T: +44 20 7006 1303
E: Arnav.Joshi@
cliffordchance.com

CLIFFORD

CHANCE

2010-001230