UK INFORMATION COMMISSIONER IMPOSES SECOND SIGNIFICANTLY REDUCED GDPR PENALTY

The Information Commissioner (represented by the Information Commissioner's Office, or ICO) has issued a Penalty Notice, fining Marriott International, Inc. (Marriott) the sum of £18.4 million for various infringements of the GDPR, a significant reduction from the £99 million penalty originally proposed.

The Penalty Notice comes just a few weeks after the ICO announced it was reducing to £20 million the size of the penalty imposed on British Airways PLC (BA), down from the £183 million indicated in 2019 (see our analysis of the BA Penalty Notice **here**).

The penalty relates to a cyber incident that began in July 2014 when the IT systems of Starwood Hotels and Resorts Worldwide, Inc. (Starwood) were compromised. Marriott acquired Starwood in 2016, but the compromise of Starwood's systems persisted through to September 2018 when it was detected by Marriott. During that time, the personal data of approximately 339 million individuals worldwide was compromised.

Unlike in relation to BA, the ICO accepted some of Marriott's representation and consequently removed reference in the final Penalty Notice to a number of GDPR infringements included in the ICO's 2019 Notice of Intent to impose of penalty (Notice of Intent). As detailed below, the ICO's discussion of these representations provides useful guidance on how to interpret the GDPR's notification requirements as well as highlighting the significant impact representations can have on the level of penalty ultimately imposed by the ICO. We analyse the decision further below.

Key takeaways

- **Focus on turnover.** Reminiscent of BA's position, Marriott criticised the ICO's prior focus on turnover as the sole metric in determining the level of penalty. The ICO confirmed it would not rely on the Draft Internal Procedure for the purposes of determining the appropriate level of penalty. How the ICO proposes to assess apply its calculation of turnover is relevant to its ongoing public consultation on its draft statutory guidance on taking regulatory action (which can be found **here**).
- **Data due diligence.** The ICO did not make any finding of infringement in respect of the period between Marriott's acquisition of Starwood and the application date of the GDPR (25 May 2018). Accordingly, the ICO did not determine whether or not it was possible for Marriott to conduct adequate due diligence during a takeover. However, in addressing Marriott's statement that it was only able to carry out limited due diligence on the Starwood data processing systems and databases, the ICO acknowledged that there may be circumstances in which in-depth due diligence of a competitor is not possible during a takeover. The ICO appears to be seeking to set a clear expectation that, where drains-up due diligence of data security is not possible pre-acquisition (our observation being that this is, at present, the usual position) such issues must be properly considered following an acquisition to ensure ongoing compliance. Nevertheless, the ICO also stated that due

diligence is *"not time-limited or a 'one-off' requirement … given Marriott's ongoing duty to ensure that the systems it had acquired from Starwood were GDPR-compliant, it is no answer to claim that certain due diligence steps were, or only needed to be, taken in the period immediately after acquisition."*

- **ICO notification period.** Firms who have suffered a cyber incident may be afforded time to determine whether personal data was compromised prior to notifying the ICO. The ICO's Notice of Intent included an infringement of the Article 33(1) GDPR 72-hour breach notification requirement. However, in the final Penalty Notice, the ICO removed this infringement, noting that although Marriott was aware that an incident had occurred in September 2018, it only became aware that personal data had been compromised on 19 November 2018. Marriott's notification to the ICO on 22 November 2018 therefore fell within the 72-hour requirement.
- **ICO notification threshold.** The ICO rejected Marriott's contention that the GDPR requires a data controller to be reasonably certain that a personal data breach has occurred before notifying the ICO. The ICO clarified that a data controller *"must be able reasonably to conclude that it is likely a personal data breach has occurred to trigger the notification requirement".*
- **Data subject notification.** The ICO accepted Marriott's submissions that the actions it took to notify data subjects were sufficient to satisfy its obligations under Article 34 GDPR. Although the Notice of Intent included infringements of Article 34 GDPR, in the Penalty Notice the ICO acknowledged that Marriott emailed affected data subjects where it had an email address available and established a dedicated website and a call centre for affected data subjects.
- **Third party reliance.** Controllers of personal data will be responsible for data breaches even where they have retained third party information security providers to assist them. Marriott argued that the fact it had engaged Accenture to assist in the security management of the Starwood network should be taken into consideration when assessing its responsibility for the incident. However, whilst the ICO acknowledged that Accenture was charged with implementing, maintaining or managing certain elements of the system, it stated that this did not reduce Marriott's ultimate responsibility for the breaches of the GDPR.
- **Focus on information security failures.** Whilst the ICO acknowledged that a 'personal data breach' (as defined in Article 4(12) GDPR) would not necessarily constitute a breach of the GDPR, in the case of Marriott, the ICO identified four avoidable major security failures which enabled the attack (namely the insufficient monitoring of privileged accounts, insufficient monitoring of databases, failure to implement sufficient controls on critical systems (such as sever hardening) and lack of encryption. Interestingly, the ICO reduced the penalty in part due to Marriott's continued and increasing investment in information security.
- **Industry standards.** Significant emphasis was given by the ICO on adherence to industry standards, which the ICO considered as relevant evidence of "the state of the art" (in the context of Article 32 GDPR). The Penalty Notice, for example, makes numerous references to industry standards published by the National Cyber Security Centre (NCSC) and the National Institute of Standards and Technology (NIST). Controllers should be aware of, and implement all such, relevant industry standards. Whilst the ICO acknowledged that Marriott had implemented PCI DSS (payment systems) industry guidance, the ICO noted that *"the fact that Marriott may have complied with certain industry guidance focusing on specific types of personal data does not obviate or reduce its responsibility for the security of all of the personal data it holds."*

BACKGROUND

On 5 July 2019, the ICO issued a Notice of Intent to impose a penalty of £99.2m on Marriott International, Inc. for infringements of the GDPR. We wrote about the background to the GDPR breach and proposed fine **here**.

Summary of the breach

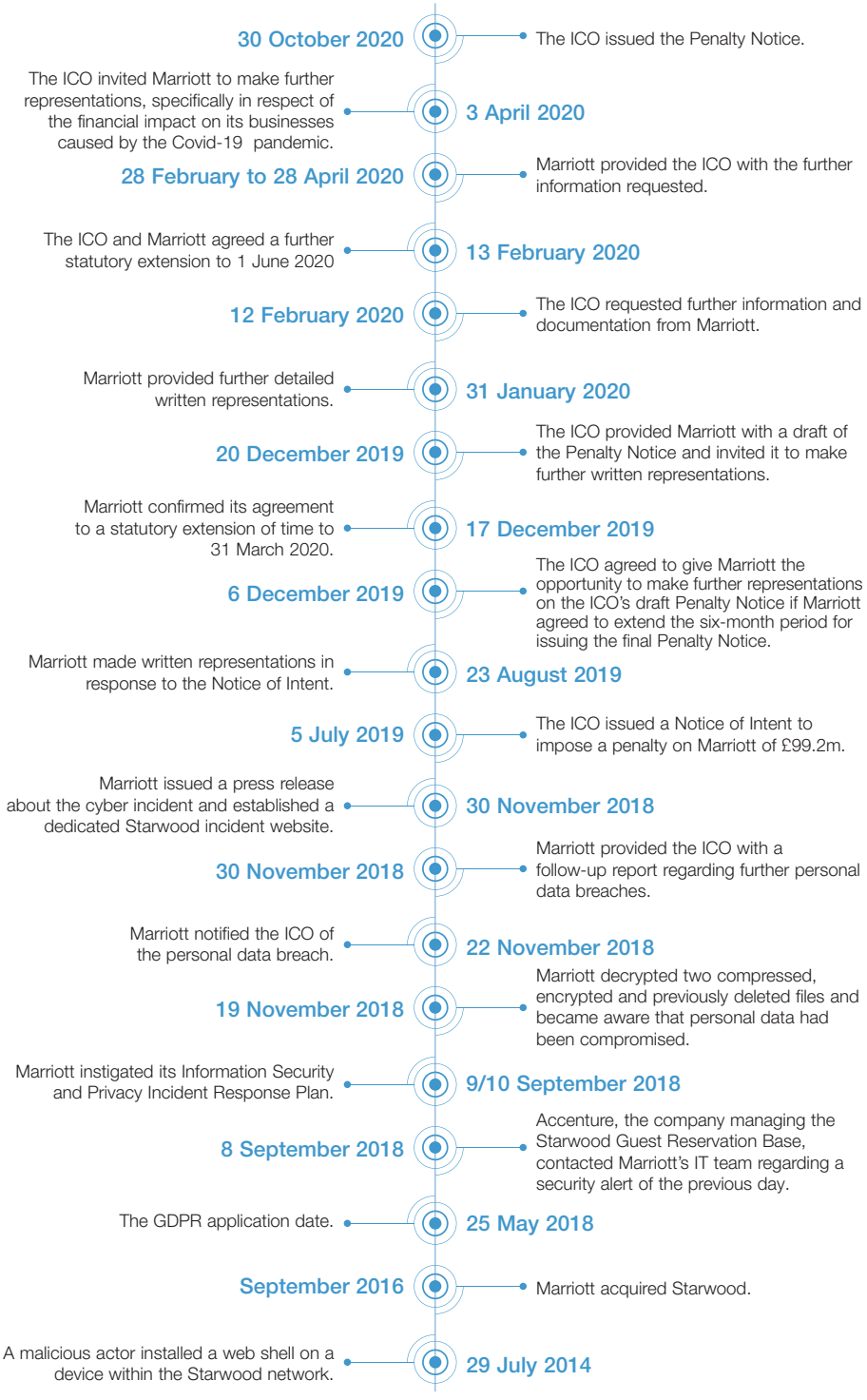
In 2014, the IT systems of Starwood Hotels and Resorts Worldwide, Inc. (Starwood) were compromised by unknown attackers. Two years later, when Marriott acquired Starwood, the historic cyber attack and underlying weakness in Starwood's IT systems went undetected during a limited due diligence exercise carried out on Starwood's data processing systems and databases. The underlying cyber risk had been imported into Marriott's business (although not directly into the Marriott network as the systems accessed by the attacker remained segregated) and remained undiscovered until September 2018, despite the GDPR applying some five months earlier in May 2018.

The Penalty Notice relates only to the period after the GDPR application date of 25 May 2018. Between 25 May and 17 September 2018, the perpetrator of the 2014 Starwood attack was able to move freely within the Starwood internal guest reservation database, accessing a variety of personal data. In September 2018, the exposure was discovered through an internal alert system and in November 2018, following an internal investigation, Marriott learned that the internal data vulnerability could be traced back to the compromised systems of Starwood.

- The attackers are believed to have potentially accessed over 339 million global guest records, 30.1 million of which were EEA records and 7 million of which were associated with the UK.
- The names, email addresses, phone numbers, arrival and departure information, VIP status and loyalty programme numbers of data subjects were thought to have been accessed as a result of the breach.
- Highly sensitive details thought to have been accessed included passport numbers (some of which were in unencrypted format).
- The ICO considered that those data subjects whose personal data was impacted prior to the GDPR application date were affected on an ongoing basis by the attacker's actions after the GDPR application date. This is important because the Penalty Notice concerns only the extent to which, after the GDPR application date of 25 May 2018, Marriott adequately protected the personal data contained within the Starwood systems.

BA enforcement timeline

The key steps in this case were as follows:



The ICO's findings

As was the case with BA, Marriott did not admit liability any the breach of the GDPR. However, in the Penalty Notice, the ICO found that Marriott had failed to process personal data in a manner that ensured appropriate security of personal data, including protecting against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required under Article 5(1)(f) GDPR and Article 32 GDPR.

Specifically, the ICO noted that Marriott failed to:

- Implement sufficient ongoing monitoring of user activity, particularly activity by privileged accounts;
- Adequately monitor the databases within the Starwood Cardholder Data Environment (CDE);
- Maintain control of critical systems and ensure that actions taken on its systems were appropriately monitored; and
- Apply encryption to relevant personal data and be able to explain why it chose to selectively encrypt data.

Calculation of the penalty

Consistent with the ICO's Regulatory Action Policy (RAO), the ICO applied a five-step approach to calculating the penalty:

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 Data Protection Act 2018 (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" per Step 1, as Marriott did not receive any financial benefit from the breach (as might be the case, where, for example, a company has misused personal data for its own commercial benefit).

In applying Step 2, the ICO had regard to the aggravating and mitigating factors listed in Article 83(2) GDPR, including (but not limited to):

- Article 83(2)(a): The nature and gravity (an "extremely large number of individuals were affected by the breach") and duration (the attack having spanned a four year period, although the ICO only takes into consideration the time from the GDPR application date);
- Article 83(2)(b): The negligent character of the infringement ("The Commissioner does, however, consider that Marriott was negligent … in maintaining systems that

suffered from vulnerabilities and shortcomings", although the ICO acknowledged that Marriott's breach was not intentional / deliberate);

- Article 83(2)(d): The degree of responsibility of the controller ("The Commissioner considers that, for the duration of the infringement on which the penalty is based, Marriott is wholly responsible for the breaches of Article 5(1)(f) and 32 GDPR");

At the conclusion of Step 2, the ICO determined that a baseline fine of £28m would appropriately reflect the seriousness of the breach.

As per Steps 3 and 4, 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 5, the ICO considered whether there were any mitigating factors that might reduce the level of the penalty, and specifically noted the following points:

- Marriott had made substantial investments in improving its data security prior to becoming aware of the attack.
- Marriott took immediate steps to mitigate the effects of the attack and protect the interests of the data subjects by implementing remedial measures. Specifically, the ICO noted that Marriott had: (a) established a notification and communication regime; (b) created a bespoke incident website in numerous languages; (c) sent 9.2 million notification emails to data subjects whose country of residence was recorded in the Starwood Guest Reservation Database as being in the EU; (d) established a dedicated call centre; (e) provided web monitoring to affected data subjects; (f) enhanced its data subject rights programme; (g) engaged with card networks; and (h) improved its technical and organisational measures generally.
- Marriott cooperated fully with the ICO's investigation.
- Widespread reporting in the media of the incident is likely to have increased the awareness of other data controllers of the risks posed by cyber attacks and of the need to ensure that they take all appropriate measures to secure personal data.
- The incident and subsequent regulatory action has adversely affected Marriott's brand and reputation, which will have had some dissuasive effect on Marriott and other data controllers.

In light of these mitigating factors, the ICO determined that a 20% reduction of the fine, from £28m to £22.4m, was appropriate.

Finally, the ICO further reduced the fine to £18.4m to account for the impact Covid-19 has had on Marriott's financial position.

APPEALS

Section 162(1) DPA 2018 gives any party the right to appeal the Penalty Notice to the First-tier Tribunal (Information Rights). Marriott has however confirmed that it does not intend to appeal the penalty.

CLIFFORD

CHANCE

AUTHORS

Alice Knowles
Lawyer
T: +44 20 7006 5157
E: alice.knowles@cliffordchance.com

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

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

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

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

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

CONTACTS

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

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

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

2011-000666