ICO fines hotelier Marriott £18.4 million – reduced by around £80 million

The Information Commissioner's Office has fined Marriott International, Inc. £18.4 million – reduced considerably from the circa £99 million fine that the ICO had originally proposed in 2019[1] in relation to a massive data security breach that occurred in 2014, a cyber-attack that compromised the security of the personal data of millions of hotel guests over a four-year period. Before setting a final penalty, the ICO considered representations from Marriott, the steps that Marriott took to mitigate the effects of the breach and the economic impact of Covid-19 on Marriott's business. Even though the scale of the reduction in this case was quite fact-specific, it illustrates the potential value in making representations to the ICO and co-operating openly with an ICO investigation.

Background

In July 2019 the ICO served a Notice of Intent[2] to fine Marriott £99,200,396 for infringements of the General Data Protection Regulation.[3] The proposed fine related to a cyber incident that came from an unknown source and was notified to the ICO by Marriott in November 2018. The incident, which led to the exposure of the personal details of around 339 million guest records across the EEA, was believed to have originated when the Starwood hotel group's systems and guest reservation databases were breached in 2014. Marriott subsequently acquired the Starwood group in 2016, but the breach was not discovered until 2018, when Marriott notified the ICO.

The ICO found that Marriott failed to comply with its obligations under Articles 5(1)(f) and 32 of the GDPR, which imposed obligations on Marriott to ensure that personal data were processed in a manner that ensured an appropriate level of security, using appropriate technical and organisational measures.

As Information Commissioner Elizabeth Denham noted in the course of the investigation, the GDPR makes it clear that organisations must be accountable for the personal data that they hold. The GDPR requirements can include carrying out proper due diligence when making a corporate acquisition and putting in place proper accountability measures to assess not only what personal data have been acquired, but also how such data are protected.

Details of the cyber-attack

In 2014 an unknown attacker installed "web shell" code onto a device in the Starwood system, giving the attacker the ability to install malware and unrestricted access to the device and other devices on that network. Using further tools to gather log-in credentials for network users, the attacker accessed and exported the database storing reservation data for Starwood customers.

The personal data involved would have differed between individual hotel guests, but may have included names, email addresses, phone numbers, unencrypted passport numbers, arrival and departure information, VIP status and loyalty-programme membership numbers. The precise number of data subjects affected was unclear, as there might have been multiple records for an individual guest. In any event, seven million guest records related to UK data subjects.

Liability for the breach

[1] ICO: Action we've taken / Enforcement / Marriott International Inc.

[2] ICO Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach.

[3] EU/2016/679.

The ICO noted that a lack of appropriate monitoring of user accounts and databases contributed to serious security deficiencies, and that there was an insufficient depth in defence of security to protect the systems and to enable swift mitigation of any bypassing of the security controls.

Even though Marriott had outsourced its IT security to Accenture, the ICO noted, in no uncertain terms, that where an organisation "accepts that it is the relevant data controller, and significant failures in its security measures have been identified, the engagement of third parties cannot reduce its degree of responsibility".[4]

Basis for calculating the fine

As noted above, the ICO held that Marriott was in breach of Article 32, the obligation to implement appropriate technical and organisational measures. For a breach of Article 32 the maximum fine is the higher of 2% of worldwide turnover or €10 million.[5]

There is also an obligation under Article 5(1)(f) that imposes a duty to process personal data in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[6] This is one of the seven data protection principles under the GDPR and is known as the "integrity and confidentiality" principle. Breaches of Article 5 are subject to administrative fines up to 4% of total worldwide turnover or €20 million, whichever is higher.[7]

The ICO saw fit to apply the higher cap (although the actual penalty imposed was, in any event, within the lower scale of fine). In assessing this, the ICO based the penalty on the worldwide turnover of the ultimate controller, Marriott International, Inc., rather than looking at turnover applicable to the EEA or to the UK business.

Assessment criteria

Now that the ICO had determined the relevant tier, it had to calculate the appropriate amount of the penalty. In doing so, the ICO had regard to Articles 82(1) and (2) of the GDPR, which set out the principles for compensation of data subjects for breach of the GDPR and controller/processor liability for such breach.

It also applied the five-step approach set out in the ICO's Regulatory Action Policy.[8] The RAP was borne out of a consultation process opened in 2018 on how the Commissioner planned to discharge her regulatory powers under the Data Protection Act 2018. One of the RAP objectives is "to be effective, proportionate, dissuasive and consistent in our application of sanctions, targeting our most significant powers (i) for organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data, and (ii) where formal regulatory action serves as an important deterrent to those who risk non-compliance with the law". In other words, serious penalties are to be reserved for the most serious cases.

RAP five-step analysis

[4] Para 7.28 of the Penalty Notice.

[5] GDPR, Art. 83(4)(a).

[6] GDPR, Art. 5(1)(f).

[7] GDPR, Art. 83(5)(a).

[8] ICO: Regulatory Action Policy.

The five-step test set out in the RAP is as follows:

- 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.
- 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 that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship).

As Marriott had not gained any financial benefit from the breach, Step 1 was irrelevant. In applying Step 2 the ICO considered the fact that, while the infringement was not intentional or deliberate, Marriott was negligent in maintaining vulnerable systems. The ICO noted that "a company of the size and profile of Marriott is expected to be aware that it is likely to be targeted by attackers, sophisticated or otherwise".[9] Accordingly, before making any adjustments under Steps 3-5, the Commissioner considered that a penalty of £28 million would have been appropriate. The ICO did not consider that there were any aggravating factors (Step 3), or that there was an undercurrent of widespread poor practice that warranted imposing a higher penalty to deter such future practices (Step 4).

In accordance with Step 5, the ICO saw fit to reduce the £28 million fine by 20% to £22.4 million to take into account certain mitigating factors, such as the facts that:

- Marriott had, before becoming aware of the breach, confirmed in 2018 a new $19 million security investment for 2019, which raised Marriott's budgeted spend for that year on security to $49.5 million;
- Marriott took immediate steps to mitigate the effects of the breach, such as deploying real-time monitoring and forensic tools on 70,000 devices on the Starwood network, implementing password resets, disabling known compromised accounts and implementing enhanced detection tools; and
- Marriott co-operated fully with the ICO's investigation.

Covid-19

As a result of the Covid-19 pandemic, Marriott also argued that any penalty should be further reduced because of the financial hardship that it would cause. The ICO has published guidance on its regulatory approach during the Coronavirus emergency,[10] the current version of which states: "As set out in the Regulatory Action Policy, before issuing fines we consider the economic impact and affordability. In current circumstances, this is likely to mean the level of fines will be reduced."

Accordingly, considering the impact of the Covid-19 pandemic (on Marriott and more generally), and in light of the ICO's published guidance, the fine was further reduced to £18.4 million. The eventual fine constitutes considerably less than 1% of Marriott's annual turnover in 2017, which was just under $5 billion. As the ICO pointed out, the fine was "accordingly well within the cap imposed by Article

[9] Para 7.17 of the Penalty Notice.

[10] The ICO's updated regulatory approach in response to the coronavirus pandemic.

83(5)".[11] Although Marriott has denied any liability, Marriott has indicated that it does not intend to appeal the final figure.

Marriott's challenges

Marriott submitted that, when proposing the original fine in the Notice of Intent to fine, the ICO had relied on a Draft Internal Procedure for calculating it. The Draft Internal Procedure focussed on the turnover of a controller, and Marriott argued, among other things, that applying this was unlawful. Marriott seems likely to have argued that relying on an unpublished, turnover-based procedure meant that the likely level of fines was not reasonably foreseeable and quantifiable by those liable to such fines, and that the penalty-setting process was therefore ultimately faulty. Although the ICO has not necessarily conceded this point, it nevertheless conceded in a letter dated 6 December 2019 that the Draft Internal Procedure "would not be taken into account in setting any penalty imposed on Marriott".[12] The Commissioner stated instead that she "relied only on Article 83 GDPR, section 155 DPA and the RAP".[13]

Marriott also contested that turnover should not be used as a core metric in cases where the wrongdoer has not profited from the breach.[14] That, argued Marriott, simply punishes a controller for being a large undertaking. The ICO did not accept this and re-emphasised that an organisation's turnover remains a relevant consideration, and that this was consistent with the approach taken to penalties in the GDPR. The ICO explained that, while not the sole factor in determining the penalty, an organisation's financial position remains one of several core metrics to be applied to ensure that the penalty is effective, proportionate and dissuasive. Although denied by the ICO, this subtle shift from its initial focus on turnover may be reassuring for larger undertakings.

Class action

Separately from the ICO fine, it now appears that Marriott will be facing a class action from its customers. Recent filings in the High Court in London reveal that Marriott faces a class action suit for GDPR non-compliance for the same data security breach for which the ICO imposed the fine.

The lawsuit was launched by technology consultant Martin Bryant, represented by international law firm Hausfeld and is being financed by Harbour Litigation Funding. The claim is being brought as a representative action under Rule 19.6 of the Civil Procedure Rules.

If the class action succeeds, Marriott may have to make multiple pay-outs. Although individually such pay-outs could be for small amounts, cumulatively they could be substantial, especially considering that the breach led to the exposure of personal details of about 339 million guest records across the EEA. Even if the class action is unsuccessful, Marriott is likely to incur substantial legal costs in defending it.

Comment

It is worth noting that the fine only relates to Marriott's breach from 25 May 2018, when new rules under the GDPR came into effect, even though the ICO's investigation traced the cyber-attack back to 2014. Also, because the security breach happened before the UK left the EU, the ICO investigated on behalf of all EU authorities as the lead supervisory authority under the GDPR.

[11] Para. 7.57 of the Penalty Notice.

[12] Para 5.6(b) of the Penalty Notice.

[13] Para 7.63 of the Penalty Notice.

[14] Para 7.71 of Penalty Notice.

As this case amply demonstrates, even if IT vulnerabilities of a target company have not been uncovered during due diligence, the buyer will, on completion, become fully responsible for ensuring the security resilience of the entire company. It is also worth noting that, while the ICO will continue to take a hard line on GDPR compliance, it will consider improvements made by the offending entity when taking mitigating factors into account. Besides, as exemplified in this instance, open co-operation appears to be the best policy.

This case also illustrates the daunting scale of the ICO's fining powers and, at the same time, the potential usefulness in challenging an ICO Notice of Intent. Although it is hard to quantify the impact of making such representations in a given case, the potential value in doing so is exemplified by the notable reduction in this case of more than £80 million from the initial notice. Still, Marriott will no doubt have incurred considerable legal fees in the process against an uncertain outcome, and it will ultimately be a question of fact in each case whether there is any realistic scope for significant reduction.

Henry Elkington, Associate Solicitor, Simkins LLP