大成 DENTONS

Dentons White Paper

Key lessons from the first major GDPR fines for cyber breaches

4TH JANUARY 2021

Contacts

Antonis Patrikios
Partner, London
D +44 20 7246 7798
antonis.patrikios@dentons.com

Monika Sobiecki
Senior Associate, London
D +44 20 7320 6342
monika.sobiecki@dentons.com

Nick Graham
Partner, London
D +44 20 7320 6907
nick.graham@dentons.com

Simon Elliott
Partner, London
D +44 20 7246 7423
simon.elliott@dentons.com

Contents

1. Introduction

The first headlines on the future threat of "mega fines" under the EU General Data Protection Regulation (GDPR) appeared as far back as 2016, when the text of the GDPR was first adopted by the European Parliament. Back then, major cyber and data security breaches were mentioned as prime candidates for mega fines approaching the 4% maximum.

This era seemed to have finally arrived when, in 2019, the UK Information Commissioner's Office (ICO) signalled its intention to levy fines against British Airways plc (BA) and Marriott International, Inc. (Marriott) of £183.39 million and £99.2 million, respectively. These would have been by far the highest data protection fines ever imposed in the UK and EU.

However, in October 2020 the ICO published the final Monetary Penalty Notices (MPN) in relation to each of these two matters.[1] The fines have been reduced massively – in BA's case, to £20 million and, in Marriott's case, to £18.4 million. Nevertheless, they remain the highest data protection fines imposed in Europe for cybersecurity breaches.[2] This was followed in short succession in November 2020 by the (seemingly low) fine of £1.25 million imposed on Ticketmaster UK Limited (Ticketmaster)[3].

The decisions are lengthy but, as the first GDPR fines for cybersecurity breaches, they are seminal. They provide clear pointers concerning the ICO's approach to investigating and enforcing against perceived cybersecurity compliance failures, including how the regulator calculates the amount of fines; the regulator's expectations concerning cybersecurity measures that organisations should have in place; the risks that ICO is prioritising when assessing risk of harm to data subjects; the importance of swift and efficient incident response and breach action; the importance of cooperative but, at the same time, robust liaison with the regulator; and a reminder that the risk of enforcement action is just one of the key adverse consequences of a serious cyber or data security breach. Litigation is likely in these situations and regulatory findings in MPNs may provide ammunition to claimants.

These first fines are likely to form the ICO's "baseline" for cybersecurity and other personal data breach enforcement over the years to come. Despite Brexit, it is likely that EU regulators will be considering ICO's approach and may follow similar approaches when dealing with cybersecurity breaches.

1 The BA MPN is available here: https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf. The Marriott MPN is available here: https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf.

2 Not the highest fine imposed for a breach of the GDPR – see, for example, the French CNIL fine of €50 million on Google in January 2019 for not having a valid legal basis to process the personal data of the users of its services (particularly for ads personalisation), and the French CNIL fines on Google and Amazon of €100 million and €35 million, respectively, for their use of web cookies to track user activities without seeking proper consent.

3 A link to the Ticketmaster decision is available here: https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf.

2. Executive summary

The key takeaways from these MPNs are:

a. **The dramatic reduction of the fine in the BA and Marriott MPNs from the fine originally proposed by the ICO in each Notice of Intent (NoI)**. The crucial factor in the reduction of the fine was not the impact of COVID-19 or the good incident response behaviours displayed by the controllers. It was the successful attack, by the controllers (and their legal counsel), on the application of a draft policy on fines which pegged the level of fines to turnover, and from which the ICO was eventually pushed to depart following robust representations and legal arguments.

b. **The Regulatory Action Policy (RAP) seen in action and ICO's approach to fines and the calculation of quantum**. The ICO worked through the "five-step procedure" in its RAP in a manner which provides a useful template for analysing and assessing future decisions and could help with rough estimates of the possible quantum of fines.

c. **The ICO's expectations concerning technical and organisational cybersecurity measures, which tell us "what good looks like" in the regulator's view**. The ICO was both granular and specific in terms of the standards expected under GDPR Articles 32 and 5(1)(f) to meet the threshold of "appropriateness". Furthermore, this is a useful reminder that cyber incident response is a multidisciplinary effort, in which cyber and Info Sec professionals are the main subject matter experts. It is also clear that, moving forwards, cyber and data protection lawyers will need to ensure that they maintain their technical understanding to be able to advise on compliance and, when things go wrong, on the likelihood of adverse regulatory findings, the risk of enforcement action and the possible size of a fine.

d. **The willingness of the ICO to make findings of negligence**. When assessing the intentional or negligent character of the infringement (i.e. findings under GDPR Article 83(2)(b)), the ICO was open to making, on the face of the decision, findings that the controllers were negligent in their failings to comply with the GDPR. Whilst there is no detailed legal analysis contained within the MPNs themselves, and the MPNs are not binding on the courts, statements to that effect in MPNs can be used by claimants in their claims (whether in court proceedings or in settlement discussions) and will likely have persuasive force in the context of litigation proceedings (noting that group litigation proceedings are currently pending against BA and Marriott). Weighing the likelihood of this sort of finding is going to be crucial in determining the overall cyber breach response strategy, including dealing with data breach litigation.

e. **Unsurprisingly, in all three cases, the main mitigating factor recognised by the ICO was the controllers' swift and efficient incident response and remedial action**. This is a useful reminder that incident preparedness, written and rehearsed incident response plans, awareness and training around incident response are the most essential risk mitigation steps that organisations can take prior to an actual incident.

3. Key background facts

BA

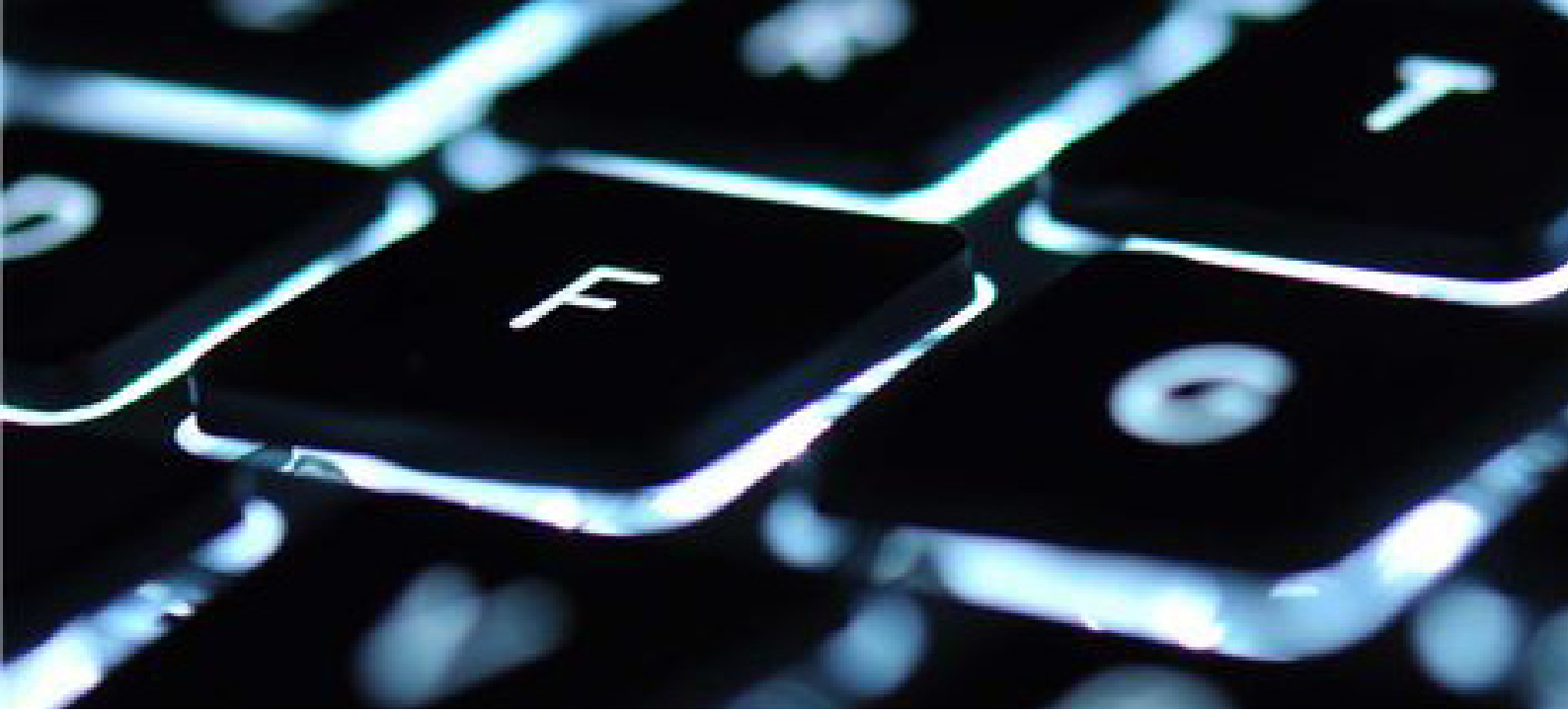
This case is a good example of the risks posed by third party suppliers and incorporating cybersecurity risk through the supply chain.

In June 2018, the attacker was able to access the controller's Citrix Access Gateway (a remote access application that allowed access to the controller's network) using the login credentials of an employee of a provider of cargo services to the controller. The attacker was able to "break out" of the Citrix environment and access a wider range of systems. They obtained access to a file containing login details of a privileged domain administrator, stored in plain text, and so readily available to allow the attacker to escalate its privileged access. In a matter of days, the attacker was able to find further login details of a database system administrator and successfully log in to numerous servers.

Due to an unintended error, a system which processed payment card details for redemption transactions was logging these in plain text (and had been doing so since 2015). This meant that, when the attacker was able to access these log files, they were able to access unencrypted details of 108,000 payment cards.

The attacker was also able to identify files, which contained code for the controller's website. The attacker proceeded to modify the code to redirect customer payment card data from the legitimate website to a bogus website that they had set up.

As a result, the attacker accessed the personal data of approximately 429,612 individuals (the data sets included sensitive financial data, such as card number, CVV number, and usernames and pin numbers relating to 612 executive club accounts).



4. Key background facts **Marriott**

This case centres around incorporating cybersecurity risk by way of a corporate transaction – in this case an acquisition by the controller.

The acquisition brought with it a number of legacy computer systems and an unwelcome guest. The attacker had infiltrated the acquisition target's network in 2014 and installed a web shell on a device within the acquisition target's network. The attacker could remotely access the systems and install Remote Access Trojans (RATs), enabling ongoing administrator control of systems.

Using Mimikatz (a tool which harvests login credentials stored in system memory), the attacker was able to compromise a number of user accounts and ultimately run commands on the acquisition target's reservation databases. In 2015 and 2016, on a number of occasions, the attacker created a number of "dmp" files, which are evidence of the potential exfiltration of data relating to guest reservations.

The controller acquired the target in 2016. After the acquisition, the target's computer systems were kept separate from the acquirer's and remained separate during the relevant period of the attack, which extended beyond the coming into force of the GDPR in May 2018 until the attacker was eventually detected later in 2018.

The attacker was able to access personal data in both encrypted and unencrypted forms. The exfiltrated tables contained unencrypted simple data relating to guests and guest reservations (e.g. guest name, gender, date of birth, VIP status, contact details, specifications as to the room stayed in and certain details of the guest's travel arrangements), 18.5 million passport numbers and 9.1 million payment cards. In total, 339 million guest records were affected by the incident, including 30.1 million EEA records (7 million of which were associated with the UK).

5. Key background facts **Ticketmaster**

The facts of this case are so complex that they are set out in a detailed Chronology contained in an Annex to the MPN. In short, the controller hosted a chat bot to provide customer help on sections of its website, including the payment page. The chat bot was supplied and hosted by a third party software developer. In February 2018, an unknown third party attacker injected malicious code into the chat bot. The malicious code would extract copies of any data submitted on a web page that contained the chat bot. As a result of the controller's choice to host the chat bot on the payment page, the malicious code would extract the payment data which was submitted on that page, including payment card data.

Between February 2018 and April 2018, several banks and credit card providers attempted to alert the controller that there were signs of fraudulent activity and in May 2018 the controller engaged forensic firms to investigate the breaches in Australia. A few days later, a security researcher contacted the controller's establishment in New Zealand to inform them that there was malicious code contained within the chat bot on the website and provide more specific information concerning the malicious code.

After a few more days, the controller raised the issue with the software developer that provided the chat bot and, over the next month and a half (during which members of the public reported to the controller that their personal antivirus software was flagging the chat bot as malicious), the controller instructed forensic firms to expand their search from Australia to all of the controller's geographical domains. However, they did not find any indication of malware. Finally, on further investigation, the chat bot was fully disabled by the controller for all territories in June 2018.

The controller eventually notified 9.4 million data subjects in the EEA as having been potentially impacted by the breach (1.5 million of these were in the UK). A number of banks notified Ticketmaster specifically of card details that had been compromised (one bank noted that 60,000 individual card details were compromised and another replaced 6,000 cards). The controller received 997 complaints alleging financial loss and/or emotional distress.

6. Security measures and cyber learnings: **what does the ICO expect**?

The ICO made a number of factual findings regarding the technical and organisational measures that each of the three controllers had in place at the time of each attack. The findings are relevant as to whether or not the organisations themselves had complied with GDPR Article 5(1)(f) (the data security principle which requires the organisation to ensure the integrity and confidentiality of personal data) and Article 32 (which deals with security of the processing and requires the application of appropriate technical and organisational measures).

The ICO points out that the relevant *standard* in order to comply with each obligation is to ensure that there is *appropriate* security (under Article 5) and *appropriate* technical and organisational measures to ensure an *appropriate* level of security (Article 32). This *appropriateness* is measured by reference to published industry standards, as further set out in the table below. This is a helpful reminder from ICO that, in order to flesh out what "appropriate" means in a particular operational context, controllers should have regard to (among other things, such as the state of the art and the cost of implementation, per the GDPR) the consensus of professional opinion in the field of information and cybersecurity. This is typically enshrined in widely used industry standards (such as the ICO 27000 series or the Payment Card Industry Data Security Standard (PCI-DSS)) and the guidance of centres of excellence, such as the UK National Cybersecurity Centre (NCSC), the European Union Agency for Cybersecurity (ENISA) or the US National Institute of Standards and Technology (NIST).

The ICO confirmed that **a personal data breach does not necessarily amount to a breach of the data security requirements of the GDPR**.[4] This is not new, and was clear under the pre-GDPR regime, but it is useful to have this confirmation from a data protection regulator in a high-profile case like this. The standard is *appropriate* measures, but *appropriate* should not be based on hindsight, it should be appropriate against risks known or that could be reasonably foreseen at the time of the breach. The sophistication of an attacker (for example, APTs, state-sponsored, organised crime) is not a defence where the application of such security measures could have prevented or mitigated the impact of some or all of its actions. The ICO made a clear statement that, in such cases, it does not consider the controller to be solely responsible for the attack, nor does it consider the role of the attacker as irrelevant. However, it appears that the ICO's approach will be directed to whether or not they consider the controller to have met the requirements of Article 32, regardless of the sophistication of the attacker, although broader cybersecurity and GDPR compliance efforts and investment will also be taken into account to assess compliance holistically. Put in its simplest form, whatever the threat vector and the sophistication or complexity of a breach, at the end of the day **a breached organisation wants to be able to demonstrate that a breach happened *despite* the fact that it had in place appropriate security measures, and *not because* it did not have such measures in place** (as the regulator concluded was the position in each of the three cases).

To assess a breach under Article 32, it is necessary to take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk to the rights of data subjects. It is interesting that the ICO's analysis does not methodically consider each of these factors separately, before taking a decision on whether or not the *appropriateness* standard was met. It could be argued that the costs of implementation of, for example, a Security Incident and Event Management (SIEM) system that would cover all of the systems of a global organisation may be prohibitive.

4 Paragraph 6.5 of the BA MPN.

The decisions are replete with major and minor observations from the ICO on "what good looks like" in terms of cybersecurity. We have drawn out the key points/observations and provided our comments on these below, as they provide a useful guide to the UK regulator's expectations concerning the technical and organisational measures that are appropriate to certain cybersecurity risks.

Cyber issue	Which MPN	ICO expectations	Dentons comment
1. Supply chain due diligence	**BA and Ticketmaster**	Supply chain risk should be addressed as an extension of security risk management. **Organisations should have a Security Risk Implementation Plan (SRIP)** in place including: (i) risk scoring contracts; (ii) due diligence of existing suppliers; (iii) audit and compliance monitoring; (iv) mapping upstream and downstream contracts; and (v) contract exit arrangements.[5] In the case of data processors, it is necessary to ensure that they provide sufficient guarantees about their technical and organisational measures.[6] PCI DSS requirements include several provisions regarding relationships with service providers in the field of payment card data processing, which expand on the GDPR requirements for processors. For example: • To ensure that there is a written agreement with service providers that includes an acknowledgement that they are responsible for the security of cardholder data which they process, or to the extent that they can impact their customers' cardholder data environment.[7] • To ensure that there is a programme to monitor service providers' PCI DSS compliance status annually.[8] • To ensure that there are clear definitions of information security responsibilities for personnel[9] and a formal security awareness programme for personnel.[10]	It has been a long-standing principle of data protection law that vendors/service providers who are data processors should be subject to assessment e.g. questionnaire which covers security measures, including those set out in applicable security standards. Look to develop best practice templates for a cybersecurity schedule which forms part of your "standard paper" for vendors to sign up to. This could incorporate measures set out in security standards. Ensure that this is not simply a paper exercise, and suppliers are audited periodically (e.g. annually) during the course of the contract. In BA, the controller had a Third Party System Access Agreement with its service provider, but whilst the ICO recognises that setting security standards for suppliers is commendable, reliance on agreements alone will not be enough to be an effective measure. In Ticketmaster, the controller's contract terms with the chat bot provider required the chat bot to be, amongst other things, free from malware. However, this is not enough to satisfy PCI DSS requirements (nor, for that matter, GDPR requirements) and the contract terms were found to be lacking in several regards, including lack of specific provisions about security of payment card data, the definition of information security responsibilities and annual monitoring of compliance. The lesson here (which is not new) is to ensure that vendor contracts are not rapidly rushed through in order to launch a project or new solution, but are carefully scrutinised, amended and negotiated, particularly where sensitive personal data (including payment card details) will be processed. If a company is unable to complete its due diligence before signing the contract, it should do so as quickly as possible after signature. Furthermore, there is a need for periodic audits to ensure that the service provider remains "secure" after entering into the contract.

5 Paragraphs 6.11 and 6.12 of the BA MPN and *Mitigating Security Risk in the National Infrastructure Supply Chain* (Centre for the Protection of National Infrastructure, Good Practice Guide, April 2015) (https://www.cpni.gov.uk/supply-chain), supplemented by more recent advice published by the NCSC (2018) (https://www.ncsc.gov.uk/collection/supply-chain-security).
6 Paragraph 6.13 of the BA MPN and ICO Guidance on *GDPR Security Outcomes* (2018) (https://ico.org.uk/for-organisations/security-outcomes/).
7 Paragraph 3.48.2 of the Ticketmaster MPN and PCI DSS requirement 12.8.2 (https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1607793567816).
8 Paragraph 3.48.3 of the Ticketmaster MPN and PCI DSS requirement 12.8.4.
9 Paragraph 3.48.4 of the Ticketmaster MPN and PCI DSS requirement 12.4.
10 Paragraph 3.48.5 of the Ticketmaster MPN and PCI DSS requirement 12.6.

Cyber issue	Which MPN	ICO expectations	Dentons comment
2. M&A due diligence	**Marriott**	The ICO did not examine this issue in detail. The controller claimed that during the acquisition they were only able to carry out limited due diligence on the target's data processing systems. The ICO did not make any finding of an infringement specifically in respect of this, as the takeover occurred prior to 25 May 2018. However, the ICO did make findings in respect of the acquirer's securing of the systems post 25 May 2018.	This is likely to be an issue revisited by the ICO in a future matter and reviewing security measures in place should become a priority for all corporate transactions moving forwards. Incorporating cybersecurity risk by way of corporate transaction is not uncommon in our experience. Even so, the amount of due diligence may not protect the acquirer from all security issues. An example on the facts here is that the acquirer relied upon assurances from the target's management on the application of multi-factor authentication (MFA) to systems. Therefore, robustly drafted warranties should be secured where there are any concerns relating to the target. In addition, if the due diligence is not completed prior to the completion of the transaction, it is essential for the acquirer to complete it as soon as possible after that. In any event, the new controller assumes full responsibility for the security of the data. Controllers may derive support from subsequent independent audits of the relevant systems (such as PCI DSS annual assessments), but attention should be paid to the scope of such assessments. Any out-of-scope systems should be assessed separately to plug the gaps.
3. Multi-factor authentication (MFA)	**BA and Marriott**	Companies should appropriately authenticate and authorise users (or any automated functions) that can access personal data. Companies should strongly authenticate users who have privileged access and consider two-factor or hardware authentication measures.[11] Companies should use MFA whenever possible, especially when it comes to their most sensitive data.[12]	MFA is widely available and easily deployed on systems. This has gained new importance in the age of COVID-19 when remote access is more common (e.g. home-working). It has also been cited as a factor in previous ICO decisions, such as the fine levied against Cathay Pacific.[13] It is likely to be considered a baseline security requirement moving forward, which is especially important for authenticating third party users such as contractors and other suppliers.

11 Paragraph 6.14 of the BA MPN and *Supply Chain Security* guidance documents, NCSC (https://www.ncsc.gov.uk/collection/supply-chain-security).
12 Paragraph 6.16 of the BA MPN and *Back to Basics: Multi-Factor Authentication* (NIST, 2016) (https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication).
13 https://ico.org.uk/media/action-weve-taken/mpns/2617314/cathay-pacific-mpn-20200210.pdf

Cyber issue	Which MPN	ICO expectations	Dentons comment
4. Application /server hardening	**BA and Marriott**	The ICO suggests: (a) removing access to features that are not required for the purpose for which access is permitted; and (b) removing or restricting any protocols, software or applications which are similarly not required.[14] Only run the services that are absolutely necessary. This will reduce the number of ways an attacker might compromise systems on the network. If you have services which are publicly accessible and are not being actively used, you are exposing a range of potential attack vectors unnecessarily.[15] There are particular issues with Citrix.[16] The ICO weighs up the scope of systems to which server hardening should have been applied and concludes that it should have included server hardening measures across devices with access to cardholder data, the cardholder data environment itself and any other network devices that could access either large quantities or sensitive categories of personal data.[17]	Reducing the attack surface is a recommended measure for all organisations. This sits alongside the principle of least privilege, which directs organisations to ensure that they allow access rights to specific users which are as limited as necessary (see below). The ICO suggests that there are a range of acceptable means to achieve server hardening (e.g. application whitelisting, application blacklisting).[18] The ICO also points out that the process of server hardening would have been expected to generate server documentation. This could have aided in risk assessments and implementation of whitelists or other measures, e.g. removal of unnecessary applications and/or protocols.[19]
5. Penetration testing	**BA**	The ICO does not specify any particular standard for penetration testing, but points out that the *scope* of the penetration testing performed by the controller was not sufficient.[20] Had more rigorous testing been performed (e.g. a Red Team exercise), then many of the problems identified within the decision were, the ICO deemed, likely to have been identified and addressed.[21]	Regular and comprehensive penetration testing (and, crucially, implementing the recommendations arising from the penetration test) are clearly expected by regulators. Requirements for penetration testing should be set out in a formal policy. It is worth considering whether to attempt to protect the report with privilege. Like forensic reports, the ICO is able to request the results of any penetration tests carried out which are not covered by legal privilege. In the DSG Retail fine decision from the ICO[22], for example, the findings of the penetration test carried out (which had not been acted upon) ended up contributing to the ICO's findings against the organisation.

14 Paragraph 6.44 of the BA MPN.
15 Paragraph 6.44 of the BA MPN and ICO's Guidance on *Protecting personal data in online services: learning from the mistakes of others* (May 2014) (https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf).
16 Paragraph 6.35 of the BA MPN and a Joint White Paper from Citrix and Mandiant entitled *System Hardening Guidance for XenApp and XenDesktop*. (https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/system-hardening-for-xenapp-and-xendesktop.pdf).
17 Paragraph 6.38 of the Marriott MPN.
18 Paragraphs 6.40 to 6.51 of the BA MPN.
19 Paragraph 6.47 of the BA MPN.
20 Paragraph 6.53 of the BA MPN.
21 Paragraphs 6.52 to 6.56 of the BA MPN.
22 https://ico.org.uk/media/action-weve-taken/mpns/2616891/dsg-mpn-20200107.pdf.

Cyber issue	Which MPN	ICO expectations	Dentons comment
6. Hardcoded passwords	**BA**	The use of hardcoded passwords is generally recognised as problematic. If hardcoded passwords are used, it is almost certain that malicious users will gain access through the account in question.[23] Passwords should not be stored in plain text by users or systems, and password hashes should be protected to prevent attackers easily accessing them.[24]	Along with MFA, this is one of the key measures which would limit the efficacy and reach of an attacker, limiting lateral movement across servers and systems. There are a number of approaches which enable the proper protection of passwords (e.g. hashing, encryption) and tools to assist (e.g. see OWASP guidance). Differential security for privileged accounts is also advisable and may deal with concerns about functionality. The ICO's comments make it clear that it is highly unlikely that there will be a satisfactory excuse for an organisation storing passwords in plain text.[25]
7. Privilege management	**BA and Marriott**	Privilege management includes the principle of least privilege, which means that access rights granted to specific users must be limited to those users who reasonably need such access to perform their function and removed when no longer needed.[26] Monitoring activities should prioritise user activity monitoring. Given the high value to an attacker of compromising Identity and Access Management (IAM) systems, they should be given priority for security maintenance. This includes designing access control systems to allow for easy monitoring of account usage and accesses.[27] The ICO commented on the fact that there were no user access monitoring systems to detect the attacker escalating its privileges and setting up guest accounts. One solution, which the ICO suggests, would have been the implementation of a Privilege Access Management (PAM) audit and monitoring tool.[28]	User access management is, as the ICO points out, part of key standards such as NIST and ISO 27001. Large organisations will already be familiar with these information security standards and the fundamental security principle of least privilege. The suggested requirement to implement a monitoring tool as an "appropriate measure" does, however, go above and beyond this. In fact, the size of the organisation is clearly material, but the ICO does not accept that monitoring the controller's IT estate would have been a complex task given its size. This was not accepted as a defence to the non-compliance with the requirement to implement monitoring across a complex estate as an appropriate measure.[29]

23 Paragraph 6.58 of the BA MPN and *Use of Hard Coded Passwords*, The Open Web Application Security Project (OWASP) (https://owasp.org/www-community/vulnerabilities/Use_of_hard-coded_password).
24 Paragraph 6.59 of the BA MPN and *Preventing Lateral Movement*, NCSC (Feb 2018) (https://www.ncsc.gov.uk/guidance/preventing-lateral-movement).
25 See the relevant parts of the BA MPN, in particular paragraph 6.74.
26 Paragraph 6.38 of the BA MPN, and ICO's guidance in respect of *Security Outcomes* (https://ico.org.uk/for-organisations/security-outcomes/).
27 Paragraph 6.16 of the Marriott MPN and *Introduction to Identity and Access Management* (Jan 2018) (NCSC Guidance) (https://www.ncsc.gov.uk/guidance/introduction-identity-and-access-management).
28 Paragraph 6.78 of the BA MPN.
29 Paragraph 6.80 of the BA MPN.

Cyber issue	Which MPN	ICO expectations	Dentons comment
8. Logging / monitoring	**BA and Marriott**	Logging is described by the NCSC as "the foundation on which security monitoring and situational awareness are built". An effective monitoring strategy is required so that actual or attempted security breaches are discovered. Good monitoring is more than simply the collection of logs. It is also the use of appropriate tools and skilled analysis to identify indicators of compromise in a timely manner so that corrective action can be taken.[30] The ICO suggests that logging can be achieved through a number of means, including implementing an SIEM solution or using manual searches[31].	Whilst the ICO points out that logging/monitoring systems would not prevent an attacker from accessing systems in the first place, they may be crucial for detecting an attacker's presence on systems. Good logs will also enable a better understanding of what threat actors carried out while on the network.[32] However, whilst important, implementing monitoring systems may not be entirely straightforward, especially across numerous legacy systems, and the best endpoint monitoring systems can be expensive. There is a tension here, as **the ICO is clearly signalling that it will not consider every logging/monitoring system as *appropriate* and will consider the absence of an adequate form of logging/monitoring system as a failure under Article 32**. One controller appears to have had some logging in place, but this appears to have not included access management logs.[33] By contrast, the other controller had a full SIEM solution in place and an SOC to collect the logs, but did not include sufficient logging of key activities such as user activity or actions taken on databases, therefore rendering the SIEM and SOC ineffective.[34]
9. Code review/code integrity	**BA**	Code review is a software quality assurance activity in which one or several individuals check a program manually by viewing and reading part of its source code. One of the reviewers must not be an author of the code. OWASP describes this as "probably the single-most effective technique for identifying security flaws".[35] The ICO also suggests that file integrity monitoring could have played a role in the detection of changes made to code, in particular the example of the changes to code made in the BA case. PCI DSS also includes provisions around file integrity management: merchants should "deploy file integrity monitoring software to alert personnel to unauthorised modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly".[36]	The controller experienced two separate issues with code: (i) an unintentional error in a script which logged unencrypted payment card details for redemption transactions (then accessible to the attacker); and (ii) the unauthorised modification of the website code by the attacker. Whilst code review/code debugging should be part and parcel of any development process, it is necessary to ensure that internal and external developers of apps for the organisation comply with specified standards for code review. By contrast, file integrity monitoring is crucial, not only in preventing the type of "code modification" attack conducted by the attacker here, but also data integrity attacks. As a core PCI DSS standard, it appears to be called out as a minimum requirement for *appropriate* security under Article 32 GDPR by the ICO.

30 Paragraphs 6.83 and 6.84 of the BA MPN and *Security Monitoring* Guidance published by the NCSC (https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-1-security-monitoring).
31 Paragraph 6.83 of the BA MPN.
32 Paragraphs 6.83 and 6.84 of the BA MPN.
33 Paragraph 6.84 of the BA MPN.
34 Paragraph 6.23 of the Marriott MPN.
35 Paragraph 6.87 of the BA MPN and OWASP *Code Review Guide* (https://owasp.org/www-project-code-review-guide/).
36 Paragraph 6.92 of the BA MPN and PCI DSS (requirement 10.5.5).

Cyber issue	Which MPN	ICO expectations	Dentons comment
10. Encryption	**Marriott**	PCI DSS requires the encryption of cardholder data. There is further guidance from the NCSC to the effect that the use of encryption to protect bulk data should be the norm. In these scenarios, systems architects and designers will need to think carefully about how encryption can be used in a meaningful way.[37]	In this case, payment card data and passport numbers were encrypted by AES-128. Encryption was not applied to other categories of data due to a focus on PCI DSS compliance. The ICO was concerned that, as a result, certain sensitive data (such as passport numbers) ended up unencrypted. There was no rationale recorded for this approach.[38] The ICO **clearly expects a documented risk assessment** which **demonstrates the evaluative judgment** that is arrived at and the rationale for its approach to encryption. Controllers should look to compile such a risk assessment and keep it on record. In addition, the *standard* of encryption should also be examined (as the AES-128 could be decrypted by the attacker).[39] **In practice, good levels of encryption and appropriate key management practices are emerging as key technical and organisational measures in the GDPR era; beyond protecting data In a security sense and providing a possible safe harbour from mandatory breach notification, they are gradually also becoming a key data export control when data is transferred to a country that does not provide adequate levels of privacy protection.**
11. Risk assessments	**Ticketmaster**	PCI DSS requirements include a provision requiring parties who are processing payment card data to implement a risk assessment process that is performed at least annually and upon significant changes to the environment, and identifies critical assets, threats and vulnerabilities.[40]	Whilst it is debatable whether the controller or its third party chat bot provider is more to blame for the incident, the responsibility for introducing the chat bot tool to the payments page rested with the controller – this is not surprising. The controller's own Secure Coding Guidelines required a formal risk assessment, as did PCI DSS requirements, but the controller did not carry out a formal risk assessment of the implementation of the chat bot on the payments page. Non-compliance in breach of own policy is an aggravating factor.[41] In addition, the risks of introducing third party scripts are well known and the ICO determined that the controller should have risk assessed the implementation of third party scripts to its payments page.[42] This is a good example of what appears to be deployment of a seemingly innocuous tool, which itself was not designed to process payment card data, ended up impacting the security of the payments environment. This **highlights the importance of following structured and documented risk assessment processes** and considering the "unintended consequences" of a particular software feature.

37 Paragraph 6.41 of the Marriott MPN and NCSC Guidance on *Protecting Bulk Personal Data* (https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data).
38 Paragraph 6.42 of the Marriott MPN.
39 Paragraphs 6.39 to 6.44 of the Marriott MPN.
40 Paragraph 3.48.1 of the Ticketmaster MPN and PCI DSS requirement 12.2.
41 Paragraph 3.51 of the Ticketmaster MPN.
42 Paragraphs 6.13 to 6.18 of the Ticketmaster MPN.

7. Incident response

In both the BA and Marriott cases, the controllers received **plaudits for their incident response and cooperation with the ICO, with a concomitant reduction in the size of the fine** in each case (see section 8 below for analysis).

In BA, the controller moved swiftly to contain the incident and to notify. They managed to contain the vulnerability within hours of being informed about it by a third party and moved swiftly to deploy additional technical measures, including a top-of-the-range anti-virus and endpoint detection/response tool. The controller notified the ICO, acquirer banks, payment schemes and 496,636 affected customers the day after they became aware of the breach. Further data subjects were notified the following day. The controller offered credit monitoring and compensation for any financial losses to data subjects affected by the breach.

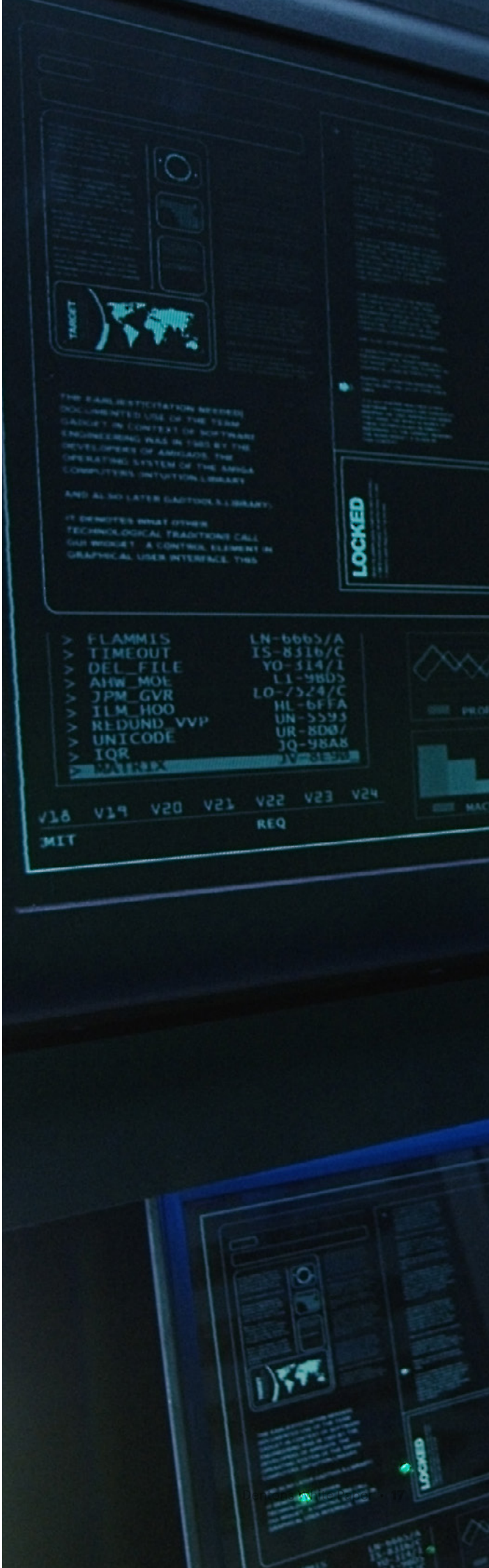
In Marriott, the controller was also, arguably, prompt in notifying (although apparently ICO initially expressed concerns that it took the controller more than two months from initial discovery of the issue to notify the ICO). After being informed by their service provider about the incident, they quickly triggered their Information Security and Privacy Incident Response Plan. A few days later, they deployed monitoring and forensic tools on 70,000 legacy systems of the acquired company. A process of investigation and discovery followed, including terminating the RAT access and discovering evidence of exfiltration of files several weeks later, including a confirmation that the exfiltrated files definitively included documents that contained personal data. The ICO was notified within 72 hours of this evidence coming to light and was kept updated by means of a follow-up report when further personal data breaches were discovered. The controller also issued a press release and set up a dedicated incident website. Finally, a little more than a week from notifying the ICO, the controller also started to email the data subjects, including providing information about the dedicated call centre set up by the controller (although ICO criticised the controller for initially not including in the notification emails the telephone number for the call centre – this was provided on the controller's website).

So, in both cases, the controllers notified the ICO promptly and fully cooperated with the resulting investigation, which involved representations being made by several rounds of correspondence. There was little or no criticism of both the incident response and the level of cooperation with the ICO in both of these MPNs, which led to resulting reductions in the fines (see section 8 below for analysis).

In Ticketmaster, ICO again recognised the good incident response behaviours displayed by the controller as mitigating factors. In particular, **the ICO noted the controller's remedial action** including that, once the chat bot was removed from the controller's website, the breach ended; the controller forced password resets across all of its domains; finally, the controller created a website where customers and media could receive information about the breach and arranged for 12 months of credit monitoring for the affected individuals. However, the ICO criticised the controller for providing inadequate instructions to external forensic specialists.

In short, the ICO's findings across the three MPNs underscore the **overall crucial importance of good incident response in mitigating legal/regulatory risk and brand damage**. Put simply, the way organisations respond to an incident or breach has significant implications from a legal and regulatory liability point of view as regulators will take good incident response, transparency and cooperation with regulators into account as an important mitigating factor. Furthermore, from a brand perspective, appropriate incident/breach response determines, to a large extent, how the incident/breach will be remembered.

This does not mean, however, that an organisation which deals with a breach should simply do as it is told by the regulator. Although the ICO is one of the most pragmatic, sophisticated and prolific (both in terms of guidance and enforcement action) data protection regulators globally, and it is clear from the three MPNs that its sophistication on cybersecurity has increased markedly in recent years, the regulator does sometimes get it wrong. In these cases, **controllers who are confident about their position and strategy should be prepared to put forward robust representations in support of their approach**. The dramatic decrease in the quantum of the proposed fines between the NoI and MPN in each of the Marriott and BA cases is probably the best example regarding the usefulness of a "friendly and cooperative, but assured and robust" approach to regulatory liaison in the aftermath of a serious breach.



8. ICO's approach to calculating the quantum

The ICO's RAP sets out the procedure which the regulator will apply for calculating a fine under Article 83 GDPR. The RAP provides guidance as to the circumstances in which it is appropriate to impose an administrative fine or penalty for breaches of the obligations imposed by the GDPR and draws explicitly on the list of factors which are set out in Article 83(2) GDPR to be taken into account. We have analysed the application of these factors in the three recent MPNs in the table below.

There are a couple of key observations to be made first.

a. Firstly, it is important to note that the fines in both the BA and Marriott cases involve a large reduction compared to the initial NoI. The crucial lesson is that, when appropriate (for instance, when an organisation considers (acting on advice) that the regulator has misunderstood facts, misapplied the law, overreached or got the enforcement action (including the quantum of fines) wrong), it should resist regulatory findings. A carefully planned regulatory liaison strategy, clear positions and solid legal arguments can pay dividends. The analysis in the table below shows that being friendly and cooperative with the ICO will be taken into account in making reductions, but that your organisation should also be assured and robust when appropriate. Good incident response and regulatory liaison handling will make a massive difference to the final enforcement action including, possibly, the quantum of fine, as happened in the BA and Marriott cases. The two are not mutually exclusive: an organisation can reap the benefits of cooperation whilst at the same time taking a robust approach to mitigate legal and regulatory risks. The importance of this is accentuated given that, increasingly, additional risk is posed by legal action and claims brought by the affected persons and/or privacy activists.

b. Secondly, at least in the cases of Marriott and BA, the ICO investigation and final MPNs took two years from notification to publication (including 10 months from notification to ICO issuing the NoI). In other words, regulatory liaison takes time, is expensive and presents opportunities to get it wrong or get it right. However, if you do get it right, the benefits for the organisation may significantly outweigh the costs.

ICO RAP	Application to BA	Application to Marriott	Application to Ticketmaster	Dentons comment
Step 1: an initial element removing any financial gain from the breach	Did not gain any financial benefit or avoid any loss, directly or indirectly. Not relevant.	Did not gain any financial benefit or avoid any loss, directly or indirectly. Not relevant	No gain arising from the incident can be identified.	N/A
Step 2: adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at sections 155(2) to 155(4) DPA (which mirror Art. 83(1) and 83(2) GDPR)	-	-	-	-

ICO RAP	Application to BA	Application to Marriott	Application to Ticketmaster	Dentons comment
• **Nature, gravity and duration of the failure (Art. 83(2)(a))**	Processing a significant amount of personal data in an insecure manner (see findings on cybersecurity measures at section 6 above). The controller was alerted by a third party. Significant number of affected individuals. Individuals will have suffered anxiety and distress as a result of the disclosure of their personal data (including payment cards). The infringement continued for 103 days.	Failed to implement multiple measures that would have allowed detection / mitigation of attack after 25 May 2018. Extremely large number of affected individuals. Mitigating steps will have gone some way to reducing distress. However, it is likely that individuals will still have suffered some anxiety and distress. The infringement continued from 25 May 2018 to 17 September 2018 (a significant length of time).	The controller was unable to identify the breakdown of affected customers accurately. The attacker was potentially able to access 9.4 million customers. Various banks and members of the public had informed the controller that it was the source of a payment card breach. The controller provided inadequate instructions to its external forensic specialists. The controller failed to act in accordance with PCI DSS. The infringement continued from 25 May 2018 to 23 June 2018.	BA argued that the data subjects were not affected by "distress" and that breaches involving payment cards were an "unavoidable fact of life". This was not accepted by the ICO. Marriott similarly argued that distress will only arise in cases where individuals are advised by their banks to cancel payment cards. This was also not accepted as the ICO noted that all personal data is of significance to individuals and loss of control may cause distress (see further section 9 below). The ICO relied on the ENISA Guidance on assessing the severity of data breaches[43] for assessing the risk to the data subjects. In light of this, it is unlikely that arguments regarding the level of distress experienced by the data subjects will be successful, if they are not supported by the ENISA Guidance (see further section 9 below). Marriott argued that the ICO had failed to examine the matter holistically. However, the ICO also rejected this argument and stated that it had looked at a holistic analysis of relevant systems and there had been a failure to ensure multiple levels of security.

43 Recommendations for a methodology of the assessment of severity of personal data breaches (December 2013), European Union Agency for Network and Information Security (ENISA) (https://www.enisa.europa.eu/publications/dbn-severity).

ICO RAP	Application to BA	Application to Marriott	Application to Ticketmaster	Dentons comment
• **Intentional or negligent character of the infringement (Art. 83(2)(b))**	Not an intentional or deliberate act. However, the ICO found that the controller was negligent (within the meaning of Art. 83(2)(b)). In particular, a company the size and profile of the controller is expected to be targeted by attackers. The risks of compromise may have significant consequences for the controller's customers and its business. The ICO would have expected the controller to take a combination of appropriate steps. Therefore, the controller is negligent for failing to do so.	Not an intentional or deliberate act. However, the ICO found that the controller was negligent (within the meaning of Art. 83(2)(b)). Same rationale as in BA.	Not an intentional or deliberate act. However, the ICO found that the controller was negligent (within the meaning of Art. 83(2)(b)). In particular, it was negligent of the controller to presume, without adequate oversight or technical measures, that the third party chat bot supplier would provide an appropriate level of security. In addition, the controller's breaches of PCI DSS were negligent.	The ICO acknowledges that attacks conducted by criminals will not be treated the same as intentional breaches of the law by the controller. However, the regulator rejects the suggestion that the attackers are responsible for the breach. Furthermore, relying on an extensive commitment to Info Sec was not enough. A failure to ensure that all appropriate measures to secure personal data are taken amounts to negligence.
• **Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Art. 83(2) (c))**	This is considered under Step 5.	This is considered under Step 5.	The controller created a website where customers and media could receive information about the breach and arranged for 12 months of credit monitoring.	N/A
• **Degree of responsibility of the controller or processor (Art. 83(2)(d))**	The controller is responsible for the security of its systems and the deficiencies which exposed the network to the attack. Although the fact that the breach was not deliberate (in the sense that the controller was the victim of an attack) is a relevant consideration. It does not absolve the controller of responsibility. If anything, it is precisely the risk of such attacks that necessitates implementation of appropriate measures, per GDPR Articles 5(1)(f) and 32.	The controller is responsible for the security of its systems. While the entry of the attacker into the compromised systems pre-dated the acquisition, the **acquirer has an ongoing duty to secure systems, which extends beyond the completion of the acquisition**.	The controller is responsible for the security of its systems.	N/A

ICO RAP	Application to BA	Application to Marriott	Application to Ticketmaster	Dentons comment
• **Any relevant previous infringements (Art. 83(2)(e)) or any previous failure to comply with any enforcement or penalty notices (Art. 83(2)(i))**	Not relevant.	Not relevant.	Not relevant.	N/A
• **The degree of cooperation with the ICO (Art. 83(2) (f))**	Fully cooperated.	Fully cooperated.	Fully cooperated and provided evidence on request, with one exception.	This is given due credit and weight and will be an important strategic priority when responding to a breach. However, it does not mean that an organisation cannot or should not disagree with the regulator's findings.
• **Categories of personal data affected (Art. 83(2) (g))**	The personal data affected was financial data. Whilst financial data is given a score of 3 (out of a maximum of 4) in the ENISA Guidance, the aggravating factors in this case escalated the incident to a 4.	The personal data included unencrypted passport details, details of travel, various other categories of personal information including name, gender, date of birth, VIP status, address, phone number, email address, credit card data.	The personal data included personal identifiers, usernames and passwords, financial data (e.g. bank details, card details, CVV).	The ENISA Guidance is relied upon by the ICO to assess the risks arising from the data. Therefore, despite being dated 2013, the ENISA guidance remains the most reliable regulatory guidance for risk assessing a personal data breach.
• **Manner in which the infringement became known to the ICO (Art. 83(2) (h))**	The controller acted promptly in notifying the ICO.	The controller complied with its obligations in notifying the ICO.	The controller reported the incident to the ICO who (on reflection) made no finding that the controller was in breach of Art. 33, despite the fact that various banks, card providers and other third parties tried to inform the controller for several months.	Although reporting as quickly as possible (including, in some cases, even if in doubt as to whether the mandatory notification requirements have been actually triggered) will remain the least risky course of action in most cases, the ICO will recognise (consistent with EDPB guidance) that these are not triggered while the controller is investigating whether a personal data breach took place.
Conclusion	An effective, proportionate and dissuasive fine of £30 million.	An effective, proportionate and dissuasive fine of £28 million.	An effective, proportionate and dissuasive fine of £1.5 million.	

ICO RAP	Application to BA	Application to Marriott	Application to Ticketmaster	Dentons comment
Step 3: adding in an element to reflect any aggravating factors (Art. 83(2)(k))	Not relevant.	Not relevant.	Not relevant.	N/A
Step 4: adding in an amount for deterrent effect to others	The ICO determines that it is not aware of widespread issues of poor practice that would be assisted by imposing a higher penalty. No adjustment necessary.	The ICO determines that it is not aware of widespread issues of poor practice that would be assisted by imposing a higher penalty. No adjustment necessary.	The ICO determines that a fine and communications about the fine will be a sufficient deterrent.	In practice, this consideration may be more material for companies / industries / types of data processing where regulators perceive there is systemic non-compliance. One can think of a few areas of privacy (as opposed to cybersecurity) compliance that regulators may perceive as presenting systemic issues.

ICO RAP	Application to BA	Application to Marriott	Application to Ticketmaster	Dentons comment
Step 5: reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship) (Art. 83(2) (c), (f) and (k))	The controller took immediate measures to mitigate and minimise damage to data subjects. The controller promptly informed affected data subjects, law enforcement and regulators. Widespread reporting in the media will have reached other data controllers, having an instructive effect. The impact on the controller's brand and reputation will also have had a dissuasive effect. Offer of reimbursement of financial losses and credit monitoring for data subjects. Remedial IT security measures.	The controller's investment in cybersecurity (immediately prior to the attack, a new US$19 million investment on security bringing total for the year to US$49.5 million, raised to US$108.5 million after the breach was discovered. The controller took immediate steps to mitigate effects of attack and implement remedial measures for data subjects (e.g. password resets, disabling compromised accounts). Full cooperation with investigation. Widespread reporting in the media will have reached other data controllers, having an instructive effect. The impact on brand and reputation will also have had a dissuasive effect. Comprehensive measures for data subjects (e.g. bespoke incident website, 9.2 million emails in EU, dedicated call centre, web monitoring for data subjects, engagement with card networks).	The controller forced password resets across domains. The controller created a website where customers / media could receive information. The controller incurred costs as a result, including 12 months of credit monitoring. The ICO is not aware of any other outstanding compliance issues.	Ironically, if the matter is escalated in the press/worthy of press attention, this appears to play into reducing the fine. Marriott tried to argue that its measures had mitigated distress, but engagement with the call centre (57,000 calls) was taken as evidence of distress (see further section 9 below). Marriott also pointed out how much it had spent on incident response (in excess of US$50 million in customer remediation activities alone). However, the ICO did not consider it appropriate to further reduce the penalty.
Conclusion	Taking account of mitigating factors, reduce penalty by 20% to £24 million.	Taking account of mitigating factors, reduce penalty by 20% to £22.4 million.	No further reduction.	
Impact of COVID-19	With regards to the impact of the COVID-19 pandemic and the ICO's guidance, a further reduction is appropriate and proportionate, to £20 million.	With regards to the impact of the COVID-19 pandemic and the ICO's guidance, a further reduction is appropriate and proportionate, to £18.4 million.	With regards to the impact of the COVID-19 pandemic and the ICO's guidance, a further reduction is appropriate and proportionate, to £1.25 million.	
Final tally	**£20 million.**	**£18.4 million.**	**£1.25 million.**	

9. The law: substantive and procedural points

Both BA and Marriott raised similar points before the regulator. These included substantive, procedural and public law arguments. A number of these arguments were unlikely to succeed (such as an argument that the ICO had applied the wrong fining tier under Article 83 GDPR, or misapplied Article 83(2) altogether) and there is a sense of the proverbial kitchen sink having been thrown at the matter (which presumably was part of the controllers' legal strategy and regulatory liaison tactics).

Furthermore, all three cases raise important legal points, substantive and procedural, that will no doubt be revisited in the future by the ICO and companies under investigation and, if appealed, by the courts. We have addressed some of these legal points above. Below, we look at some additional legal points, which are either novel or most likely to be revisited again in future cases:

a. **No admission of liability for breach of GDPR**. This formed the basis of the controllers' strategy and will, no doubt, be important in the context of defending the ensuing claims. Given the publicity surrounding ICO proceedings, NoIs and MPNs, defending controllers need to be cautious not to inadvertently admit liability, especially in the context of cooperating with the regulators.

b. **Not every instance of unauthorised processing or breach of security will amount to a breach of GDPR Article 5 or Article 3.2**. The success of a cyber attack is not necessarily evidence of breach of the GDPR.[44] As explained above, this is not new but is a useful reminder by the ICO in the context of a serious cyber breach in the GDPR era and can be helpful in practice to controllers who consider that their security controls were appropriate under the GDPR. The standard of compliance with the GDPR security requirements is the implementation of "appropriate" measures, but "appropriate" should not be determined with the benefit of hindsight. Rather, measures should be appropriate to the risks known or reasonably foreseen at the time of the breach.

c. **Mitigating factors help, but do not absolve controllers of responsibility and liability**. Mitigating factors include, for instance, significant investment in cybersecurity and GDPR readiness; the breach being the result of criminal and/or very sophisticated activity; the breach being the result of security failures at partners operating at arm's length, such as suppliers or corporate transaction counterparties; using expert service providers and consultants; good incident response behaviours, including notifications, cooperation with regulators and actions taken to mitigate risk to affected individuals and to remediate the underlying security issue. Even when all these positive behaviours have been displayed, and even if a company has contractual recourse against third parties (such as a supplier or acquired company), the company is not absolved of responsibility for a failure to apply appropriate security measures, if that failure enables, contributes to or fails to mitigate the impact of a breach.

d. **Clear expectation for documented cybersecurity risk assessments**. Consistent with their GDPR accountability obligations and good information security practice, companies should document their security risk assessments, even if they do not result in the identification of appropriate measures (for instance, alternative solutions to MFA). Such risk assessments should be refreshed regularly or when making material changes, should identify alternative solutions or mitigating measures when it is necessary to deviate from the optimal standard, and copies should be kept on file as per GDPR accountability requirements, remembering that these documents may be disclosable to regulators or litigation counterparties.

44 Paragraph 6.54 of the Marriott MPN.

e. **Payment card data is sensitive, but the risk is broader**. In BA, the ICO challenged the controller's submission that the main data that created risk was the payment card details and suggested that attackers may also exploit combinations of other data included in the compromised data set, such as names, user names and passwords. In fact, the ICO considers that the most serious risk is that of identity theft (as opposed to financial loss, anxiety or distress) created by the loss of control of personal data such as names, addresses and unencrypted payment card data.

f. When looking at the risk of harm, the ICO seems to be placing more emphasis on anxiety and distress, rather than the risk of monetary loss or fraud as such, and states that, despite the assurances and mitigating steps taken by the controller (including an offer to reimburse financial loss incurred), individuals will have suffered anxiety and distress until it was clear to them what happened and how they can mitigate risk.[45] In Marriott, ICO held that the act of cancelling payment cards shows that data subjects are likely to have suffered distress; the act of cancelling a card may simply cause inconvenience in itself, but the underlying reason (the risk of loss of data) likely causes distress. High numbers of calls in call centres are seen by the ICO as evidence of distress, even when the number of calls is small compared to the total number of affected data subjects (e.g. in Marriott, 57,000 out of several million). What is more, according to the ICO, loss of any personal data (not just payment card data) is of significance to data subjects and its loss may result in distress.

g. In BA, the ICO also rejected arguments that compromise of payment card data or other personal data is nowadays commonplace and a fact of life, and therefore inherently unlikely to cause distress, especially when third parties (such as banks or credit card issuers) will offer protection or the risk will be mitigated through the risk mitigation steps (such as credit monitoring) offered by the breached controller. The ICO rejected the argument, even for instances where credit card CVV numbers have not been compromised. The fact that more than 10% of affected data subjects (more than 40,000) took up BA's offer of credit monitoring was seen by the ICO as an indication that at least they were sufficiently concerned about the breach.

h. In other words:

   i. where there is evidence of loss of personal data and misuse is possible, especially when the breach affects significant numbers of data subjects, it may be difficult for a controller to support an assessment that the breach is unlikely to result in anxiety or distress, because in the ICO's view this varies from individual to individual;

   ii. mitigating measures (such as notifications, cancellation of cards, refunds, ID fraud protection and credit monitoring) mitigate, but do not eliminate, the risk of harm, as some individuals at the very least will suffer anxiety or distress in the meantime; and

   iii. although convincing arguments to the contrary could be made, including a developing trend of "breach fatigue" and "notified data subject apathy", they may be difficult to substantiate at present. To increase the convincing force of these arguments, it will be necessary to support them by reference to the specific facts of the breach, including the data, the data subjects and the surrounding circumstances. General statements will not suffice.

i. Finally, this is also a useful reminder that, when carrying out their risk assessments, controllers should asses the affected data sets holistically as opposed to just the higher risk items, such as special category data or payment card details. Often, the risk will extend beyond the obvious ones created by the highest risk items (e.g., financial loss in the case of payment cards) into other risks that a combination of data items (e.g. name, email address, postal address and, say, passport number) could create, such as social engineering, identity theft or other fraud.

45 Paragraph 7.12 of the BA MPN.

The numbers of data subjects is an important factor, but is not everything. In BA, ICO also rejected arguments that the breach was not serious given the relatively low numbers compared to other high-profile breaches (i.e. hundreds of thousands as opposed to millions of individuals). This is a useful reminder that, in the eyes of data protection regulators, although numbers of affected individuals are an important factor that must be taken into account when risk assessing a breach, it is not a determinative factor in and of itself. All the circumstances of the breach should be taken into account to determine the risk of harm, even when the numbers of affected data subjects are relatively low.

Your overall exposure may be greater than the sum of the technical breaches. In the event of multiple security failures, the ICO will look at each of them individually, but will also consider their cumulative effect. Put simply, the overall data security risk exposure for the organisation may be larger than the sum of the individual instances of failures to apply appropriate security measures.

When you act reasonably, you may have a defence even if you get it wrong. In Marriott, the ICO considered the reasonableness of the controller's reliance on expert security reports.[46] It reached the view that, even when there is a security failure (in this case, concerning the use of MFA), where the controller reasonably believes that it complies and this belief is corroborated by expert security reports (in this case, two Reports on Compliance obtained by the controller in the context of the annual validations of compliance with PCI DSS), this is not a breach of the GDPR (and, in this case, the ICO did not take the underlying issue concerning the use of MFA as part of the monetary penalty notice or take it into account in calculating the fine).

Near decommissioning is not an excuse. The fact that a system is near decommissioning does not absolve controllers of obligations to protect the data in it with appropriate measures, the implementation of which does not entail disproportionate cost or delay.[47] This is a useful reminder of the risks posed by legacy systems, especially when organisations with limited resources must prioritise investment in securing other systems. The prioritisation is understandable, but will not provide a defence if a legacy system is breached.

Like incident response, regulatory liaison is a multidisciplinary effort. As explained above, across the three cases there was a protracted regulatory liaison process with detailed representations and legal arguments. At the same time, the MPNs provide fairly detailed technical security analysis of specific cybersecurity issues and recommendations for technical security measures. The regulator's technical capabilities have improved noticeably in recent years and, for complex breaches, the regulator has the option to convene a panel of technical advisers (although it did not do so in these cases). There is also a noticeable number of references to ICO security guidance and various external organisations' technical guidance, with the NCSC guidance featuring very prominently. This is a useful reminder of the need for a multidisciplinary approach to personal data security with the controller's DPO, legal and Info Sec working hand in glove at all stages, including risk assessments for compliance purposes, incident response and regulatory liaison post-breach.

46 Paragraphs 6.10 and 6.11 of the Marriott MPN.
47 Paragraphs 6.57 onwards of the BA MPN.

10. Key takeaways for dealing with breaches that may result in a mega fine

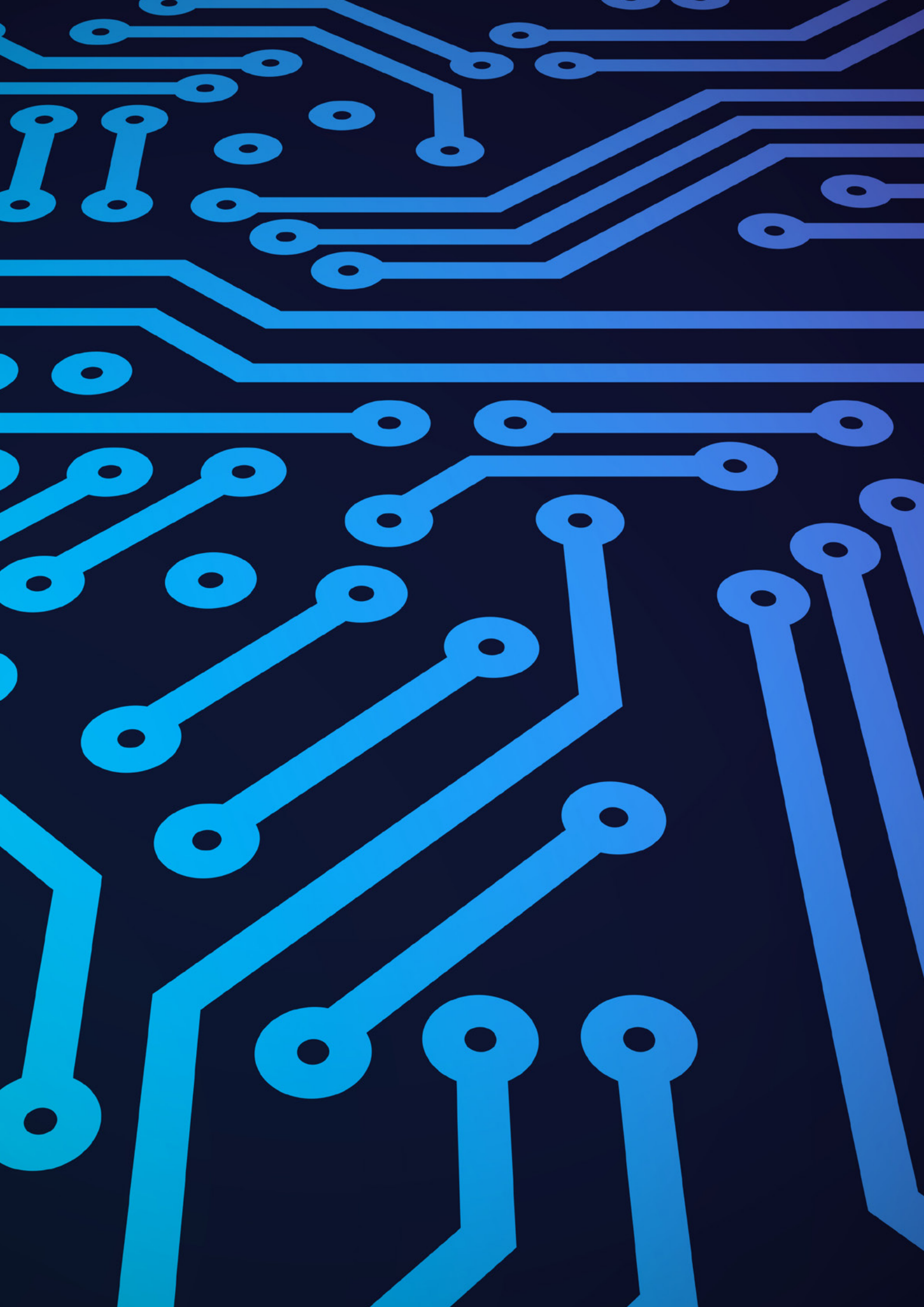
Good operational security is the baseline for mitigating the risk of serious enforcement action and high fines. If organisations fail on this, all other efforts, including significant investment in cybersecurity, appropriate incident response, compliance with notification requirements, carefully crafted and executed legal strategies and comprehensive remediation will mitigate, but will not eliminate, the risk. By contrast, breached companies who can demonstrate that their operational security was appropriate, that they had acted reasonably in their risk assessments and implementation of controls, and that they had documented their evaluative judgment concerning which controls are appropriate may be found *not* to have breached the GDPR (and therefore be subject to fines), even if they suffer a serious breach.

The importance of a robust legal approach to challenging regulatory findings, where appropriate. By mounting sophisticated legal arguments and a resistance to the ICO's draft policy on fines, the controllers achieved significant reductions to the quantum of the fine in both the Marriott and BA cases. Although the precise legal point will not recur in future matters (given that the ICO has now backtracked from this approach), the principle holds as there will potentially be other lines of defence available to organisations potentially facing a substantial GDPR fine. These should be investigated and, where available, pursued robustly in the context of regulatory liaison (with an eye on the litigation risk).

Robust legal approaches should be coupled with productive cooperation with the regulator's investigation. Whilst it is important to challenge the substantive and procedural basis for regulatory approaches and findings where appropriate, it is equally important that the breached organisation acts (and is seen as acting) in a transparent, cooperative and responsive way to requests made by regulators in the course of the investigation, where these requests are reasonable. Non-cooperation will be an aggravating factor (under GDPR Article 83(2)(f)) which may increase the level of the penalty imposed and may also invite further unwanted action, such as an audit. Cooperation, on the other hand, will not just function as a mitigating factor in the regulator's assessment of appropriate enforcement, but will also provide a solid foundation for the breached organisation's PR strategy.

Swift and effective incident response has consistently been found by regulators to be the top mitigating factor. It is striking that each of the controllers in the three cases displayed (and were commended by the ICO for displaying) good incident response behaviours which, in some cases, went above the minimum required standards, including mitigating risks for and communicating with data subjects and implementing comprehensive remedial action. This was also relevant to the ICO's judgment on the level of penalty which would apply. Some evidence of what the ICO will construe as "good practice" is also contained in the MPNs: offering credit monitoring to affected data subjects; setting up a dedicated website for information purposes; a global password reset; speedy assembly of the incident response team and instruction of forensics experts.

Regulatory investigation and action is *not* the end of the story. The imposition of an MPN does not preclude individual and group litigation claims by data subjects whose data has been impacted by the breach. In fact, it may positively encourage it or provide ammunition for it, as the regulator ventures into findings of negligence in the course of its decision, which (whilst not binding) may be persuasive to the courts that are determining those claims. In the Marriott and BA cases, there is high-profile litigation brewing, which we will see play out from 2021 onwards. In the event that either results in a substantial award of compensation, this will provide an epilogue of which data protection practitioners will also have to be mindful when dealing with cyber incidents in the future. Equally, the absence of serious enforcement action or a fine does not necessarily exclude the litigation risk, which may persist in any event, as the Morrisons case, where the controller had to defend the case all the way up to the UK Supreme Court, demonstrates. When dealing with the immediate incident response priorities, such as containment, data subject risk mitigation, notifications and remedial action, companies should have one eye on the risk of litigation, especially when making statements in regulatory representations, notifications and PR statements, and when dealing with incoming data subject queries, requests and complaints. Cyber and data security risk assessments, penetration testing and audit reports, and incident forensic investigation reports should be prepared with this risk in mind.



ABOUT DENTONS

Dentons is the world's largest law firm, connecting talent to the world's challenges and opportunities in more than 75 countries. Dentons' legal and business solutions benefit from deep roots in our communities and award-winning advancements in client service, including Nextlaw, Dentons' innovation and strategic advisory services. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and world-class talent challenge the status quo to advance client and community interests in the New Dynamic.

dentons.com

CSBrand-45350-Whitepaper-GDPR-Cyber breaches-02 — 06/01/2021