| British Airways (16 October 2020) - £20 Million | |
|---|---|
| **Breach overview** | **Monetary Penalty Notice (MPN) calculation of the penalty**<br><br>**Applying the five-step approach set out in the ICO's Regulatory Action Policy** |
| **Breach:** An external attacker gained access to BA's network initially via a remote access gateway (Citrix) provided to one of BA's suppliers. Once into BA's systems the attacker was able to access other parts of BA's systems. This eventually led to the attacker re-directing customer payment data to a third-party site it controlled called BA.ways.com. In this way, a significant amount of customer data was acquired by the attacker. The attack was not detected for more than two months.<br><br>**ICO finding:** BA ought to have identified weaknesses in its security and resolved them with security measures that were readily available at the time, this would have prevented the attack being carried out in the first place and should have prevented it escalating as it went on.<br><br>**Data:** Personal data of approximately 429,612 customers and staff including:<br><br>• Names, addresses, payment card numbers and CVV numbers; | 1. **<u>STEP 1: An "initial element" removing any financial gain from the breach</u>**<br><br>1.1 BA did not gain any financial benefit, or avoid any losses, directly or indirectly as a result of the breach. Therefore, the Commissioner did not add an initial element under Step 1.<br><br>2. **<u>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)-(4) DPA</u>**<br><br>2.1 **The nature, gravity and duration of the failure (Article 83(2)(a) GDPR)**<br><br>**Nature and gravity**<br><br>2.1.1 The Commissioner considered the nature of the failures to be of serious concern. BA was processing a significant amount of personal data in an insecure manner. BA failed to put in place measures that could have prevented the attack at each stage of its execution. These included: (i) Multi-Factor Authentication (MFA) for remote access by the third-party supplier or other infrastructure such as the use of a Virtual Private Network - BA had failed to follow its own policies and readily available industry guidance in this respect; (ii) once into its systems, BA failed to take sufficient measures to ensure that the remote access was limited to information that it was necessary for the person with that access to see and it was too easy to break out of the remote access to other parts of BA's systems – these risks were widely known and the steps to mitigate them had been highlighted in industry publications; (iii) credit card data should not have been stored at all or was being stored for too long; (iv) the attacker was able to obtain higher level administrator access because the information to do this (including passwords) was stored in plain text rather than being secured eg via encryption; (v) the scope of penetration testing over BA's systems was inadequate; and (vi) monitoring of activity across BA's systems was inadequate meaning that suspicious activity was not detected in real-time as it could have been.<br><br>2.1.2 The failures were especially serious because BA may never have detected the breach unless alerted by a third party. |

| | |
|---|---|
| • Usernames and passwords of employee and administrator accounts;<br><br>• Usernames and PINs of Executive Club accounts.<br><br>**GDPR infringement:** Articles 5(1)(f) and 32 GDPR.<br><br>Link to MPN | 2.1.3 A significant number of individuals (429,612 data subjects on BA's estimate) were affected by the breach.<br><br>2.1.4 Many of these individuals will have suffered anxiety and distress as a result of the disclosure of their personal information. The Commissioner rejected BA's submissions that the individuals would effectively see such loss of control over their data as a commonplace thing and therefore would not be distressed by it, especially as BA had taken measures to protect the individuals (see Step 5 below).<br><br>**Duration**<br><br>2.1.5 The Commissioner took 25 May 2018 (when GDPR came into operation) as the starting point for when infringements under the GDPR commenced and ending on 5 September 2018, when personal data ceased to be transferred to BAways.com. The Commissioner described this as a significant period of time.<br><br>2.2 **The intentional or negligent character of the infringement (Article 83(2)(b))**<br><br>2.2.1 The Commissioner referred to the guidelines provided by the Article 29 Working Party[1] in relation to assessing the character of the infringement.<br><br>2.2.2 The Commissioner said the infringement was not an intentional or deliberate act on the part of BA. However, BA was negligent (within the meaning of Article 83(2)(b) GDPR) in maintaining operating systems which suffered from significant vulnerabilities and shortcomings.<br><br>2.2.3 The Commissioner placed weight on the fact that a company of the size and profile of BA should be expected to be aware that it is likely to be targeted by attackers, sophisticated or otherwise and should therefore do more to prevent this or detect it. In other words, larger organisations may be held to higher security standards.<br><br>2.2.4 The Commissioner rejected the suggestion by BA that it is the attacker who was primarily responsible. The breaches identified in the MPN related to BA's failures to comply with its obligations to put in place appropriate security measures to prevent the attack in the first place or detect it at each stage of its progress. There were multiple failings by BA in this respect.<br><br>2.3 **Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c))** |

[1] ... In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement, although the controller/processor breached the duty of care which is required in the law. It is generally admitted that intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine. The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case.

2.3.1 The Commissioner considered this issue separately under Step 5 in (see below).

2.4 **The degree of responsibility of the controller or processor (Article 83(2)(d))**

2.4.1 The significant inadequacies or deficiencies which the Commissioner identified related to the way in which BA operated its network. They were not caused by inadequacies in the third-party supplier's systems or a problem with applications such as Citrix. The Commissioner therefore considered that BA was wholly responsible for the breaches of Articles 5(1)(f) and 32 of GDPR.

2.4.2 The Commissioner did not treat BA as exclusively responsible for the attack. Nor was the role of the attacker irrelevant. However, that did not alter BA's obligations to have in place appropriate security measures. In fact, the Commissioner said it was the possibility of such attacks by third parties that necessitated compliance with the obligations imposed by Articles 5(1)(f) and 32 of GDPR.

2.5 **Any relevant previous infringements (Article 83(2)(e)) or any previous failure to comply with any enforcement or penalty notices (Article 83(2)(i))**

2.5.1 BA had no relevant previous infringements or failures to comply with past notices.

2.6 **The degree of cooperation with the Commissioner (Article 83(2)(f))**

2.6.1 The Commissioner considered that BA had cooperated fully with the investigation.

2.7 **Categories of personal data affected (Article 83(2)(g))**

2.7.1 The Commissioner considered the loss of control by BA of personal data such as names, addresses and unencrypted payment card data to be particularly serious, because they provide the opportunity for identity theft.

2.7.2 While no "special category data" was affected, this did not mean that the data was not sensitive. CVV card numbers were taken for 77,000 of the 185,000 affected customers. This meant those customers put at a heightened risk.

2.7.3 The Commissioner relied upon the ENISA Guidance entitled "A methodology of the assessment of the severity of personal data breaches", which provides a scoring method to assess the severity of a personal data breach. ENISA is the EU Agency for Cybersecurity. Aggravating factors identified in the ENISA Guidance, and which were present in this case, included where full financial information is disclosed and where there is a high volume of data disclosed.

| | | |
|---|---|---|
| | 2.8 | **Manner in which the infringement became known to the Commissioner (Article 83(2)(h))**<br><br>2.8.1 BA acted promptly in notifying the Commissioner of the Attack and thereby complied with its obligations in this respect (the breach was identified by BA on 5 September and BA informed the Commissioner on 6 September). |
| | 3. | **STEP 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k))**<br><br>3.1 The Commissioner did not consider there to be any other relevant aggravating factors. |
| | 4. | **STEP 4: Adding in an amount for deterrent effect to others**<br><br>4.1 Given BA's size and the scale of its operations, and the fact that the Commissioner decided to impose a penalty that already took those factors into account, as part of the need to ensure that any penalty is proportionate, effective and dissuasive and to reflect the seriousness of the breach, the Commissioner considered that no adjustment was necessary for deterrence to others. |
| | 5. | **STEP 5: Reducing the amount to reflect any mitigating factors, including ability to pay (Articles 83(2)(c) (f) and (k))**<br><br>The Commissioner took the following into account:<br><br>5.1 Upon being alerted to the attack, BA acted promptly to mitigate the potential risk of damage suffered by the data subjects, including by notifying banks and payment schemes, the data subjects, and the Commissioner;<br><br>5.2 BA notified the Financial Conduct Authority, and informed and co-operated with the other regulatory and governmental bodies in the aftermath of the attack. BA also notified other data protection regulators outside the EEA, and 21 State Attorneys General in the USA;<br><br>5.3 BA offered to reimburse all customers who had suffered financial losses as a direct result of the theft of their card details;<br><br>5.4 BA implemented a number of remedial technical measures in order to reduce the risk of a similar attack in future and had indicated that expenditure on IT security would not be reduced as a result of the impact of Covid-19;<br><br>5.5 Having regard to these mitigating factors, the Commissioner reduced the proposed £30m penalty by 20 per cent, ie to £24m; |

| | |
|---|---|
| | 5.6 Having regard to the impact of the Covid-19 pandemic (on BA and more generally), a further reduction of £4m was applied.<br><br>5.7 Accordingly, the final penalty payable by BA was set at £20 million.<br><br>**Application of the fining tier(s) (Articles 84(4) and (f) GDPR)**<br><br>5.8 The infringement of Article 5(1)(f) GDPR falls within Article 83(5)(a) of GDPR, which is the higher category of fines (£17.5M or 20 per cent of annual turnover), whereas a breach of Article 32 falls within Article 83(4)(a) of GDPR, which is the lower level of fines (£8.7M or 10 per cent of annual turnover). The Commissioner decided the appropriate tier is that imposed by 83(5)(a) of GDPR as this was the gravest breach in issue in this case. |
| **Marriott International Inc (30 October 2020) - £18.4 Million** | |
| **Breach overview** | **Monetary Penalty Notice (MPN) calculation of the penalty**<br><br>**Applying the five-step approach set out in the ICO's Regulatory Action Policy** |
| **Breach:** In 2014, an unknown attacker installed code and malware to a device in Starwood Hotels' systems and subsequently acquired privileged access. This meant that they were in a position to take a large amount of guest information stored on Starwood's reservation database. Starwood was acquired by Marriot in 2016, but Marriott failed to detect the breach as it continued. Suspicious activity was not detected until September 2018.<br><br>**ICO finding:** There were failures by Marriott to put appropriate technical and organisational measures in place to protect the personal data being processed on its systems. | 1. **<u>STEP 1: An 'initial element' removing any financial gain from the breach</u>**<br><br>1.1 Marriott did not gain any financial benefit, or avoid any losses, directly or indirectly as a result of the breach. Therefore, the Commissioner did not add an initial element under Step 1.<br><br>2. **<u>STEP 2: Adding in an element to censure the breach based on its scale and severity, taking into account the consideration identified at sections 155(2)-(4) DPA</u>**<br><br>2.1 **The nature, gravity and duration of the failure (Article 83(2))**<br><br>2.1.1 The Commissioner said the failures by Marriott were of significant concern. There were multiple measures that Marriott could have put in place that would have allowed for the detection of, or mitigated, the attack. These included: (i) once in Starwood's systems there was insufficient monitoring to spot suspicious activity – the Commissioner cited commonly available guidelines such as the UK National Cyber Security Centre's guide "10 Steps to Cybersecurity" as relevant and referred to Marriott's own third party investigation report into the breach as illustrating failings; (ii) the logging of activity on Starwood's systems that was undertaken was insufficient and meant the attack went undetected; (iii) particularly sensitive data on Starwood's systems was not subject to additional security measures which the Commissioner would expect to see based on industry standards; (iv) sensitive data, such as passport numbers of guests, should have been subject to |

| | |
|---|---|
| **Data:** Approximately 339 million guest records, though the total number of affected guests was difficult to estimate as there may be multiple records for one guest. The data included names, email addresses, phone numbers, unencrypted passport numbers, arrival/departure information, guests' VIP status and loyalty programme membership numbers.<br><br>**GDPR Infringement:** Articles 5(1)(f) and 32 GDPR.<br><br>Link to MPN | encryption but this was not always the case and there were inconsistencies in Starwood's approach to this issue.<br><br>2.1.2 The Commissioner rejected the submission by Marriott that, as it intended to replace the Starwood systems in the near future then, in the meantime, it did not need to implement the protections which the Commissioner had decided should have been in place but were not.<br><br>2.1.3 A very large number of individuals were affected by the breach, specifically, 339 million guest records, of which - for the purposes of this penalty - 30.1 million were guest records associated with EEA member states.<br><br>2.1.4 Some of these individuals would, depending on their circumstances, have suffered anxiety and distress as a result of the disclosure of their personal information (including payment card information) to an unknown individual or individuals. The fact that 57,000 customer calls were logged to the post-breach call centre established by Marriott was indicative of that distress.<br><br>**Duration**<br><br>2.1.5 Although the attack itself spanned a four-year period, the Commissioner took 25 May 2018 (when GDPR came into operation) as the starting point for when infringements under the GDPR commenced and 17 September 2018 as the end date. The Commissioner considered that to be a significant period of time. Interestingly, this meant that the Commissioner did not consider any failings on Marriott's part to assess Starwood's data security in the course of due diligence around the acquisition of Starwood in 2016. The question of the extent of due diligence required will need to be determined in a future case. The Commissioner said in any event that the need to assess the security of systems and data was not a one-off process and would need to be kept under continual review as circumstances change.<br><br>2.2 **The intentional or negligent character of the infringement (Article 83(2)(b))**<br><br>2.2.1 The Commissioner recognised that the infringement was not an intentional or deliberate act. However, Marriott was negligent (within the meaning of Article 83(2)(b) GDPR) in maintaining operating systems which suffered from significant vulnerabilities and shortcomings.<br><br>2.2.2 As in the BA MPN, the Commissioner placed weight on the fact that a company of the size of Marriott should be expected to be aware that it is likely to be targeted by attackers and should therefore do more to detect it. In other words, larger organisations may be held to higher security standards.<br><br>2.3 **Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c))** |

2.3.1 The Commissioner considered this issue under Step 5.

2.4 **The degree of responsibility of the controller or processor (Article 83(2)(d))**

2.4.1 While the entry of the attacker into Starwood's systems pre-dated Marriott's acquisition of that company, Marriott had an ongoing duty to ensure the safety and security of the systems it was using to process personal data. There were multiple deficiencies in the security measures in place in respect of the Starwood systems, which Marriott continued to operate to process personal data after the GDPR came into force. As a result, the attacker was able to remain present and undetected in the system.

2.4.2 The Commissioner rejected Marriott's suggestion that, as it used a reputable third party to assist it with data security (ie security management services were provided by Accenture), this should be reflected in the level of fine. The Commissioner said Marriott, as controller, could not reduce its degree of responsibility in this way.

2.5 **Any relevant previous infringements (Article 83(2)(e)) or any previous failure to comply with any enforcement or penalty notices (Article 83(2)(i))**

2.5.1 Marriott had no relevant previous infringements or failures to comply with past notices.

2.6 **The degree of cooperation with the Commissioner (Article 83(2)(f))**

2.6.1 Marriott cooperated fully with the Commissioner's investigation and this was taken into account.

2.7 **Categories of personal data affected (Article 83(2)(g))**

2.7.1 The data included in some (but not all) cases unencrypted passport details, details of travel, and various other categories of personal information including name, gender, date of birth, "VIP status", address, phone number, email address, and credit card data.

2.8 **Manner in which the infringement became known to the Commissioner (Article 83(2)(h))**

2.8.1 Marriott notified the Commissioner of the attack on 22 November 2018. The Commissioner was satisfied, after representations from Marriott, that 19 November 2018 was the date when it had become sufficiently clear to Marriott that a breach had occurred, in spite of Marriott first being alerted to this possibility in September 2018. Accordingly, Marriott had complied with its reporting obligations in this respect.

| | | |
|---|---|---|
| | 3. | **STEP 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k))** |
| | 3.1 | The Commissioner did not consider there to be any other relevant aggravating factors. |
| | 4. | **STEP 4: Adding in an amount for deterrent effect to others** |
| | 4.1 | Given Marriott's size and the scale of its operations, and the fact that the Commissioner has decided to impose a penalty that already takes those factors into account as part of the need to ensure that any penalty is proportionate, effective and dissuasive and to reflect the seriousness of the breach, the Commissioner considered that no adjustment was necessary under Step 4. |
| | 5. | **STEP 5: Reducing the amount to reflect any mitigating factors, including ability to pay (Articles 83(2)(c), (f) and (k))**<br><br>The Commissioner took the following into account: |
| | 5.1 | Prior to becoming aware of the attack, Marriott raised their budgeted spend for 2019 on IT security to US$49.5 Million. Subsequent investment decisions raised their forecasted IT security budget for 2020 to US$108 Million; |
| | 5.2 | Marriott took immediate steps to mitigate the effects of the attack and protect the interests of data subjects by implementing remedial measures (eg deployment of real-time monitoring on Starwood devices, implementing password resets, disabling known compromised accounts, implementing enhanced detection tools); |
| | 5.3 | Marriott cooperated fully with the Commissioner's investigation, including responding promptly to requests for information; |
| | 5.4 | The attack and subsequent regulatory action had adversely affected Marriott's brand and reputation, which would have some dissuasive effect on Marriott and other data controllers; |
| | 5.5 | Marriott had also taken steps to: (i) establish a notification and communication regime; (ii) create a bespoke incident website in numerous languages; (iii) send 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; (iv) establish a dedicated call centre; (v) provide web monitoring to affected data subjects; (vi) enhance its data subject rights programme; (vii) engage with card networks; and (viii) improve its technical and organisational measures generally. The Commissioner also noted that Marriott informed a number of other regulatory and law enforcement agencies; |
| | 5.6 | Having regard to the mitigating factors set out above, the Commissioner reduced the £28 Million penalty by 20 per cent, ie to £22.4 Million; |

| | | |
|---|---|---|
| | 5.7 | Having regard to the impact of the Covid-19 pandemic (on Marriott and more generally), and consistently with the Commissioner's published guidance, a further reduction of £4 Million was applied. The final penalty payable was therefore £18.4 Million. |
| **Ticketmaster (13 November 2020) – £1.25 Million** | | |
| **Breach overview** | **Monetary Penalty Notice (MPN) calculation of the penalty**<br><br>**Applying the five-step approach set out in the ICO's Regulatory Action Policy** | |
| **Breach:** Ticketmaster's decision to include a chat-bot, hosted by a third party, on its online payment page allowed an attacker access to customers' financial details.<br><br>**ICO finding:** Ticketmaster failed to assess the risks of using a chat-bot on its payment page; implement appropriate security; and identify the source of suggested fraudulent activity in a timely manner.<br><br>**Data:** Names, payment card numbers, expiry dates and CVV numbers, potentially affecting 9.4 Million customers.<br><br>**GDPR Infringement:** Articles 5(1)(f) and 32 GDPR.<br><br>**Note:** This MPN is under appeal to the First Tier Tribunal (FTT). At present, the FTT proceedings are stayed pending separate High Court proceedings being disposed of which | 1. | **STEP 1: An "initial element" removing any financial gain from the breach** |
| | 1.1 | No gain to Ticketmaster arising from the incident could be identified. The Commissioner did not therefore add an initial element under Step 1. |
| | 2. | **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)-(4) DPA** |
| | 2.1 | **The nature, gravity and duration of the failure (Article 83(2))** |
| | 2.1.1 | The Commissioner found that this was a significant contravention of the GDPR. Amongst the failings relied on by the Commissioner were the following: (i) Ticketmaster failed to take sufficient steps to address security issues when including the third party's chat-bot on its payment pages – such security issues were well-known as was the means of attack used in this case (scraping data from the payment pages), and the ways to prevent it and detect it, but Ticketmaster did not take sufficient steps to address these issues in light of the heightened threat and likelihood of attack; (ii) Ticketmaster's policy of vetting suppliers like this only once every five years was inadequate; (iii) Ticketmaster failed to obtain suitable indications of data security from its supplier or to verify them adequately, in particular, when Ticketmaster first became aware of a potential breach – Ticketmaster should not have assumed, without appropriate oversight or technical measures, that its supplier was capable of ensuring an appropriate level of security; (iv) having been notified of potential issues by numerous third parties, including banks and credit card companies, Ticketmaster failed to act quickly enough to investigate them; (v) the chat-bot was not essential to the operation of the payment pages and Ticketmaster failed to produce evidence that it adequately assessed the benefits and risks of deploying it at the outset or suspending its use when first notified of potential issues; (vi) Ticketmaster had essentially |

| | |
|---|---|
| have been brought against Ticketmaster by customers affected by this incident and as between Ticketmaster and the party who supplied the chat-bot. The FTT appeal is not expected to be heard until late 2023.<br><br>Link to MPN | ceded control over access to data through the chat-bot to its supplier, but had failed to take any steps to control or monitor the interaction between the chat-bot and Ticketmaster's systems.<br><br>2.1.2 The attacker had access to payment card details of approximately 9.4 million customers;<br><br>2.1.3 The Ticketmaster Incident Response Team's instructions for this breach were ineffective in scope and depth and not all of the relevant information was provided initially, meaning that the initial investigations into the incident were too limited;<br><br>2.1.4 Ticketmaster failed to comply with a relevant industry standard, the Payment Card Industry Data Security Standard.<br><br>2.2 **The intentional or negligent character of the infringement (Article 83(2)(b))**<br><br>2.2.1 The Commissioner concluded that Ticketmaster had displayed a lack of consideration in protecting personal data and was negligent for the purposes of Article 83(2)(b).<br><br>2.3 **Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c))**<br><br>2.3.1 Once Ticketmaster removed the chat-bot from its website, the breach ended.<br><br>2.3.2 Ticketmaster created a website where customers and media could receive information about the breach.<br><br>2.3.3 Ticketmaster arranged for 12 months of credit monitoring for individuals affected.<br><br>2.3.4 Ticketmaster forced password resets across all of its domains.<br><br>2.4 **The degree of responsibility of the controller or processor (Article 83(2)(d))**<br><br>2.4.1 Ticketmaster failed in its obligations under Article 5(1)(f) and Article 32 of GDPR and relevant sections of the DPA to have regard to considerations including the state of the art, likelihood of attack, its severity and what appropriate controls were available at the time. Ticketmaster was entirely responsible for this.<br><br>2.5 **Relevant previous infringements (Article 83(2)(e))**<br><br>2.5.1 No other compliance matters or infringements were taken into account when arriving at the amount of the fine. |

| | | |
|---|---|---|
| | 2.6 | **Degree of cooperation with supervisory authority (Article 83(2)(f))** |
| | 2.6.1 | Ticketmaster fully co-operated with the Commissioner during the investigation and provided evidence upon request. |
| | 2.7 | **Categories of personal data affected (Article 83(2) (g))** |
| | 2.7.1 | Ticketmaster provided information that the personal data of approximately 9.4 million customers was potentially affected and was likely to have included basic personal identifiers, identification data, and financial data. |
| | 2.8 | **Manner in which the infringement became known to the Commissioner (Article 83(2)(h))** |
| | 2.8.1 | Ticketmaster reported the incident to the Commissioner on 23 June 2018. The Commissioner noted that banks and other third parties informed Ticketmaster of the potential breach as early as February 2018, but the Commissioner said it had not taken into account any breach of Article 33 of GDPR (failure to report the breach in time) in setting the level of fine. |
| | 3. | **STEP 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k))** |
| | 3.1 | The Commissioner did not consider there to be any other relevant aggravating factors. |
| | 4. | **STEP 4: Adding in an amount for deterrent effect to others** |
| | 4.1 | The Commissioner considered that a fine, accompanied by appropriate public communications by the ICO of its findings, would serve as an effective deterrent to others. |
| | 5. | **STEP 5: Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (Articles 83(2)(c), (f) and (k))** |
| | | The Commissioner concluded: |
| | 5.1 | Once Ticketmaster removed the chat bot from its website, the breach ended; |
| | 5.2 | Ticketmaster forced password resets across all of its domains; |
| | 5.3 | Ticketmaster created a website where customers and media could receive information about the breach; |

| | | |
|---|---|---|
| | 5.4 | The Commissioner had regard to Ticketmaster's failure to answer some questions in relation to costs and failure to provide more general information as to its financial position and the Government support it was receiving; |
| | 5.5 | Taking into account the Commissioner's regulatory approach during the Covid-19 pandemic, an exceptional reduction of the proposed penalty by £250,000 was determined to be proportionate. The fine was therefore set at £1,250,000. |

## Cabinet Office (2 December 2021) – £500,000

| **Breach overview** | **Monetary Penalty Notice (MPN) calculation of the penalty**<br><br>**Applying the five-step approach set out in the ICO's Regulatory Action Policy** |
|---|---|
| **Breach:** In announcing the New Year Honours List in December 2020, the Cabinet Office included the postal addresses of 207 of the 1,000 or so recipients of the awards in the file that was made publicly available.<br><br>**ICO finding:** The Cabinet Office failed to put appropriate technical and organisational measures in place to prevent the unauthorised disclosure of individuals' information.<br><br>**Data:** The unredacted postal addresses of 207 people named in the New Year Honours list.<br><br>**GDPR Infringement:** Articles 5(1)(f) and 32 GDPR.<br><br>Link to MPN | 1. **STEP 1: An "initial element" removing any financial gain from the breach**<br><br>1.1 There were no discernible financial gains identified or losses avoided in relation to the incident. |
| | 2. **STEP 2: Adding in an element to censure the breach based on its scale and severity, taking into account the consideration identified at sections 155(2)-(4) DPA**<br><br>2.1 **The nature, gravity and duration of the failure (Article 83(2))**<br><br>2.1.1 The data breach was caused by or contributed to by the absence of appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing of the data and was a breach of Articles 5(1)(f) and 32(1) of GDPR. The background was that the Honours and Appointments Secretariat (HAS) in the Cabinet office were using for the first time a new IT system for publishing the New Year's Honours list. Postal addresses were included by mistake in a lengthy spreadsheet. This was not noticed when the publication process was tested as the focus was on getting the names of recipients of Honours correct. However, the error was eventually spotted before publication, but it was thought that it could be corrected by a process akin to redaction. However, once uploaded to the Government's website this information would still be visible. Those handling the publication did not understand this. The Commissioner found that the main causes of the breach were: (i) the IT system should never have contained a postal address field; (ii) relevant staff understood that postal address data should not be included but they were not given adequate training in how to effectively do this; (iii) there were insufficient controls in place to sign-off on publication of the file; (iv) in any event, when the error was spotted (twice) before publication it |

should have led to a formal review (as later acknowledged by the Cabinet Office) which would have avoided the publication of the data.

2.1.2 Data was available online for a period of two hours and 21 minutes. During that period, it was accessed 3,872 times from 2,798 unique IP addresses.

2.1.3 The personal data disclosed related to data subjects across the United Kingdom from a broad range of professions and included high profile people. The personal data was published in the public domain and therefore accessible to anyone.

2.1.4 The Commissioner said the data breach was serious and could easily have been avoided. The gravity of the failure was very high.

2.1.5 The data breach caused distress to some of the affected data subjects and gave rise to a possible increase in vulnerability to identity fraud.

2.2 **The intentional or negligent character of the infringement (Article 83(2)(b))**

2.2.1 The infringements were negligent.

2.3 **Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c))**

2.3.1 The Cabinet Office removed the link to the file on the content page and contacted the Government Data Service (GDS) to remove the file from cache. This was completed in a matter of hours.

2.3.2 Affected data subjects were contacted within 48 hours of the breach via email or telephone where possible on 28 and 29 December 2019. The HAS established a rota to answer queries for two weeks following the breach.

2.3.3 The National Police Coordination Centre circulated guidance to all Police forces which could then be provided to individual Honours recipients wanting additional advice.

2.3.4 GDS used analytics to ascertain the extent of access to the data and were commissioned by the Cabinet Office to provide advice on further digital tracking and possible mitigation actions. The Cabinet Office staff monitored social media resulting in a Twitter post (showing a screenshot of the data) being removed.

| | |
|---|---|
| | 2.3.5 GDS undertook a full incident review, including a review of checks on the publisher tool and incident handling. This resulted in a change in policy reducing the caching timeframe from 24 hours to 30 minutes for attachments.<br><br>2.3.6 All employees in the HAS refreshed relevant training after the breach.<br><br>2.3.7 An independent review in the Cabinet Office focusing on data handling policies, processes, practices and culture was completed with recommendations for improvement.<br><br>2.4 **Degree of responsibility of the controller or processor (Article 83(2)(d))**<br><br>2.4.1 No third party was responsible for the breach. The development of the relevant IT system and its operation was all undertaken within Government, as was the process leading to publication.<br><br>2.5 **Any relevant previous infringements (Article 83(2)(e)) or any previous failure to comply with any enforcement or penalty notices (Article 83(2)(i))**<br><br>2.5.1 No relevant previous infringements were identified.<br><br>2.6 **The degree of cooperation with the Commissioner (Article 83(2)(f))**<br><br>2.6.1 The Cabinet Office had been cooperative and responsive to the Commissioner's investigation.<br><br>2.6.2 The initial Personal Data Breach Report for the data breach was submitted in time.<br><br>2.6.3 The Cabinet Office had been open with the Commissioner regarding the failures/factors which contributed to the data breach, including disclosing post-breach investigation reports to the Commissioner.<br><br>**The categories of personal data affected by the infringement**<br><br>2.7 The data disclosed was postal addresses. There were 207 such entries with addresses.<br><br>**The manner in which the infringement became known to the Commissioner**<br><br>The breach became known to the Commissioner as a result of the Cabinet Office submitting a Personal Data Breach Report.<br><br>**Reducing the amount to reflect any mitigating factors, including ability to pay** |

| | | |
|---|---|---|
| | 2.7.1 | The Commissioner did not consider there are any other factors that should lead to a reduction in the fine. |
| | 3. | **STEP 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k))** |
| | 3.1 | The Commissioner determined that there were no additional aggravating factors. |
| | 4. | **STEP 4: Adding in an amount for deterrent effect to others**<br><br>The Commissioner apparently decided that an additional amount should be added to the fine to act as a deterrent. In doing so the Commissioner explained that organisations like the Cabinet Office that have the means to do so should be expected to take the most stringent possible preventative measures to avoid breaches like this and, in doing so, the Cabinet Office would have incurred very little cost in implementing a procedure that could have prevented the breach. |
| | 5. | **STEP 5: Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship) (Articles 83(2)( c) (f) and (k))** |
| | 5.1 | The Commissioner determined that there were no other factors on which to reduce the fine. The Commissioner did not accept that the fine would place undue strain on public finances when the Cabinet Office had an annual budget of £381 Million. |
| | 5.2 | The Commissioner determined that a fine of £500,000 was effective, proportionate and dissuasive. |
| **Mermaids – (8 July 2021) £25,000** | | |
| **Breach overview** | **Monetary Penalty Notice (MPN) calculation of the penalty**<br><br>**Applying the five-step approach set out in the ICO's Regulatory Action Policy** | |
| **Breach:** An internal email group was created by the charity, Mermaids, without appropriate restricted access settings. This meant that approximately 780 pages of confidential emails could be viewable online for a period of nearly three | 1. | **STEP 1: An "initial element" removing any financial gain from the breach** |
| | 1.1 | Mermaids did not gain any financial benefit, or avoid any losses, directly or indirectly as a result of the breach. |
| | 2. | **STEP 2: Adding in an element to censure the breach based on its scale and severity, taking into account the consideration identified at sections 155(2)-(4) DPA** |

| | |
|---|---|
| years by searching via internet search engines.<br><br>**ICO finding:** Mermaids should have applied restricted access to its email group and could have considered pseudonymisation or encryption to add an extra layer of protection to the personal data it held.<br><br>**Data:** Names and email addresses, of 550 people. The personal data of 24 of those people was sensitive as it revealed how the person was coping and feeling, with a further 15 classified as special category data as information relating to mental and physical health and sexual orientation was placed at risk.<br><br>**GDPR Infringement:** Articles 5(1)(f) and 32 GDPR.<br><br>Link to MPN | 2.1 **The nature, gravity and duration of the failure (Article 83(2))**<br><br>**Nature and gravity**<br><br>2.1.1 The breach occurred when an internal email group was established. The way that this was set up meant that it was searchable via internet search engines. This was not deliberate. The email group ceased to be used by July 2017, yet the emails on it remained accessible. Mermaids first became aware of an issue in June 2019 when journalists noticed that information about the individuals Mermaids had been providing its service to was available online if certain searches were undertaken. The Commissioner determined that: (i) the approach to data protection compliance at Mermaids was negligent – there were inadequate data protection policies in place and a lack of adequate training offered to staff, particularly in the context of an organisation handling very sensitive and special category data relating to gender incongruence (the Commissioner said that the fact that the training was inadequate was demonstrated because, when the training took place in 2018, the issue concerning the email group was not recognised); (ii) the email group which was created by the CEO of Mermaids had the least secure settings applied in error; (iii) thereafter, when the email group ceased to be used, nothing was done to secure the data on it - there was no clear documentation to demonstrate how it was created or decommissioned and the email group appeared to have been forgotten about.<br><br>2.1.2 The Commissioner noted that the fact a child or adult may be experiencing gender incongruence is a sensitive issue which can lead to increased vulnerability. The likely increased vulnerability of a data subject in turn increases the risk of damage or distress being caused by any data contravention that reveals that an individual is seeking information about, or support for, gender incongruence.<br><br>2.1.3 In relation to 15 individuals, the emails included special category data, such as details of mental or physical health and/or sex life and/or sexual orientation, with a further 9 individuals whose data could be classified as sensitive. Four of those 24 data subjects were aged 13 or under in June 2019.<br><br>2.1.4 Around 780 pages of confidential emails were visible online, relating to 550 individuals and, apart from the sensitive and special category data referred to above, included data such as names, email addresses, job titles, or employers' names.<br><br>2.1.5 Mermaids could have considered encryption or anonymization/pseudonymization of data as another means to protect it.<br><br>2.1.6 It did not matter that there was no clear evidence that anyone other than the journalists had accessed the email group. It was enough that the data had been placed at risk. |

**Duration**

2.1.7 For the purposes of this MPN, the Commissioner considered that Mermaids was in contravention of the GDPR from the date on which it came into force on 25 May 2018 until the issue was remedied on 14 June 2019.

2.2 **The intentional or negligent character of the infringement (Article 83(2)(b))**

2.2.1 The Commissioner considered that the contraventions were not deliberate, but negligent.

2.3 **Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c))**

Steps taken included:

2.3.1 Immediately taking the email group down and taking proportionate action to ensure any data collected was removed from any archive website;

2.3.2 Taking early steps to transition Mermaids' email service to a more secure email platform;

2.3.3 Contacting (through Mermaids' solicitors) all "sensitive data subjects" to explain the remedial steps which were being taken and keeping them updated on progress;

2.3.4 Notifying the Charity Commission;

2.3.5 Notifying all former trustees and major funders of the incident.

2.4 **The degree of responsibility of the controller or processor (Article 83) (2)(d))**

2.4.1 No other party was responsible for the breaches.

2.5 **Any relevant previous infringements (Article 83(2)(e)) or any previous failure to comply with any enforcement or penalty notices (Article 83(2)(i))**

2.5.1 The Commissioner was unaware of any previous data protection infringements by Mermaids.

2.6 **The degree of cooperation with the Commissioner (Article 83(2)(f))**

2.6.1 Mermaids were co-operative and replied to the Commissioner's enquiries promptly.

| | | |
|---|---|---|
| | 2.7 | **Categories of personal data affected (Article 83(2) (g))** |
| | 2.7.1 | The email addresses identified 550 data subjects, all of whom had been in contact with Mermaids at some point. Due to the nature of the services offered by Mermaids, the Commissioner said that it can be inferred that some of data of those individuals is special category data. |
| | 2.8 | **Manner in which the infringement became known to the Commissioner (Article 83(2)(h))** |
| | 2.8.1 | Mermaids notified the Commissioner of the attack on 14 June 2019, the date it became aware of the breach. |
| | 3. | **STEP 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k))** |
| | 3.1 | An aggravating factor was the duration of the infringement from 2017 to 2019. |
| | 4. | **STEP 4: Adding in an amount for deterrent effect to others** |
| | 4.1 | The Commissioner was mindful that any penalty must be effective, proportionate and dissuasive. However, the Commissioner said nothing specific regarding adding anything to the fine as a deterrence to others. The Commissioner commented that publicity in relation to its findings and national media attention should serve as a deterrent. |
| | 5. | **STEP 5: Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (Articles 83(2)(c), (f) and (k))** |
| | 5.1 | Mermaids immediately adjusted the settings on the Groups.IO website so that the data was no longer accessible to third parties. |
| | 5.2 | Mermaids employed both solicitors and a data protection consultant to review the incident and to oversee any remedial action. Mermaids also instructed a specialist media law firm. |
| | 5.3 | Mermaids updated its data protection policies. |
| | 5.4 | It provided one-to-one training on data protection issues to the CEO. |
| | 5.5 | It also carried out a data security review through an external consultant and implemented their recommendations. |
| | 5.6 | The Commissioner took into account the size of Mermaids and the financial information available about the charity on the Charity Commission website, as well as the representations that Mermaids had made about its financial position. |

| | | |
|---|---|---|
| | | Mermaids' total income rose from £317,580 in the year ending 31 March 2018 to £902,440 in the year ending 31 March 2020. |
| | 5.7 | The Commissioner considered that whilst the fine itself should act as a deterrent, it was important to balance this against ensuring the charity is able to maintain effective provision for its users and not take away donations made by the public. |
| | 5.8 | Taking into account all of the factors set out above, the Commissioner imposed a fine of £25,000. |