Information Commissioner's Office

PENALTY NOTICE

Section 155, Data Protection Act 2018

Case ref: COM0783542

British Airways plc
Waterside
PO BOX 365
Harmondsworth
UB7 0GB

16 October 2020

1. INTRODUCTION & SUMMARY

1.1. This Penalty Notice is given to British Airways plc ("**BA**") pursuant to section 155 and Schedule 16 to the Data Protection Act 2018 (the "**DPA**"). It relates to infringements of the General Data Protection Regulation (the "**GDPR**"), which came to the attention of the Information Commissioner ("**the Commissioner**") as a result of an incident that took place between 22 June and 5 September 2018.

1.2. In summary, between 22 June and 5 September 2018, a malicious actor ("the **Attacker**") gained access to an internal BA application through the use of compromised credentials for a Citrix remote access gateway ("**CAG**"). [redacted] After gaining access to the wider network, the Attacker traversed across the network. This culminated in the editing of a Javascript file on BA's website (www.britishairways.com). The edits made by the Attacker were designed to enable the exfiltration of cardholder data from the "britishairways.com" website to an external third-party domain (www.BAways.com) which was controlled by the Attacker. In this Penalty Notice, the events of 22 June to 5 September 2018 are referred to as "the **Attack**".

1.3. BA is a subsidiary of International Airlines Group, which is registered in Spain but has its operational headquarters in the United Kingdom. The data subjects affected by this breach were BA customers in the United Kingdom, in the EU, and in the rest of the world.

1.4. BA was the controller of the personal data of its customers, within the meaning of section 6 DPA and Article 4(7) GDPR, as it determined the purposes and means of the processing of the personal data. By, *inter alia*, collecting, recording, organising, structuring and storing the personal data of its customers, BA was processing that data within the meaning of section 3(4) DPA and Article 4(2) GDPR.

1.5. BA acted promptly in notifying the Commissioner of the Attack on 6 September 2018 and thereby complied with its obligations in this

respect. The Commissioner considers that BA has cooperated fully with her investigation and has taken that into account.

1.6. BA does not admit liability for breach of the GDPR. However, for the reasons set out in this Penalty Notice, the Commissioner has found that BA failed to process the personal data of its customers in a manner that ensured appropriate security of the data, including: protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required by Article 5(1)(f) and by Article 32 GDPR.

1.7. The Commissioner has found that, in all the circumstances of the case and having regard to BA's representations and the matters listed in Article 83(1) and (2) GDPR, the infringements constitute a serious failure to comply with the GDPR and, accordingly, that the imposition of a penalty is appropriate. The amount of the penalty that the Commissioner has decided to impose, having taken into account a range of mitigating factors set out further below and the impact of the Covid-19 pandemic, is £20m.

1.8. Pursuant to Article 56 GDPR, the Commissioner is acting as lead supervisory authority in respect of the cross-border processing at issue in this case.

2. LEGAL FRAMEWORK

GDPR

2.1. On 25 May 2018, the GDPR entered into force, replacing the previous EU law data protection regime that applied under Directive 95/46/EC ("**Data Protection Directive**")[1]. The GDPR seeks to harmonise the protection of fundamental rights in respect of personal data across EU Member States and, unlike the Data Protection Directive, is directly applicable in every Member State.[2]

2.2. The GDPR was developed and enacted in the context of challenges to the protection of personal data posed by, in particular:

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[2] Recital 3.

a. the substantial increase in cross-border flows of personal data resulting from the functioning of the internal market;[3] and

b. the rapid technological developments which have occurred during a period of globalisation.[4] As Recital (6) explains: "*… The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities….*"

2.3. Such developments made it necessary for "*a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market…*".[5]

2.4. Against that background, the GDPR imposed more stringent duties on controllers and significantly increased the penalties that could be imposed for a breach of the obligations imposed on controllers (amongst others).[6]

The relevant obligations

2.5. Chapter 1 GDPR sets out the general provisions. Article 5 of Chapter II GDPR sets out the principles relating to the processing of personal data. Article 5(1) lists the six basic principles that controllers must comply with in processing personal data, including:

> *1. Personal data shall be:*
>
> *…(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*

2.6. Article 5(2) GDPR makes it clear that the "*controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*".

---

[3] Recital 5.
[4] Recital 6.
[5] Recital 7.
[6] See, in particular, Recitals 11, 148, 150, and Article 5, Chapter IV and Article 83.

2.7. Chapter IV, Section 1 addresses the general obligations of controllers and processors. Article 24 sets out the responsibility of controllers for taking appropriate steps to ensure and be able to demonstrate that processing is compatible with the GDPR. Articles 28-29 make separate provision for the processing of data by processors, under the instructions of the controller.

2.8. Chapter IV, Section 2 addresses security of personal data. Article 32 GDPR provides:

> *1. Taking 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 of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
>
> *(a) the pseudonymisation and encryption of personal data;*
> *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
> *(c) …*
> *(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.*
>
> *2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*

2.9. Article 32 GDPR applies to both controllers and processors.

Penalties

2.10. Article 83(1) GDPR requires supervisory authorities to ensure that any penalty imposed in each individual case is "*effective, proportionate and dissuasive*".

2.11. The principle that penalties ought to be effective, proportionate and dissuasive is a longstanding principle of EU law. The Commissioner

is under an EU law obligation to ensure that infringements of the GDPR are penalised in a manner that is effective, proportionate and dissuasive.

2.12. Further, Recital 148 emphasises, *inter alia*, that *"in order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation."* It also records that due regard should be given to the:

> *… nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor…*

2.13. Recital 150 provides as follows:

> *In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of*

administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

2.14. In line with the above, when deciding whether to impose a fine and the appropriate amount of any such fine, Article 83(2) GDPR requires the Commissioner to have regard to the following matters:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, including whether, and if so to what extent, the controller or processor notified the supervisory authority of the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, directly or indirectly from the infringement. [7]

2.15. Article 83(5) GDPR provides that infringements of the basic principles for processing imposed pursuant to Article 5 GDPR will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €20 million or, in the case of an undertaking, up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

2.16. Article 83(4) GDPR provides, *inter alia*, that infringements of the obligations imposed by Article 32 GDPR on the controller and processer will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €10 million or, in the case of an undertaking, up to 2% of its total worldwide annual turnover of the preceding financial year, whichever is higher.

2.17. Article 82(3) GDPR addresses the circumstances in which the same or linked processing operations give rise to infringements of several provisions of the GDPR. It provides that "*... the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*".

2.18. Article 83(8) GDPR provides that the exercise by any supervisory authority of its powers to fine undertakings will be subject to procedural safeguards, including an effective judicial remedy and due process.

Cooperation and consistency

2.19. Where, as here, the processing in issue is cross-border, Article 56 GDPR makes provision for the designation of a lead supervisory authority. In this case, the Commissioner is acting as the lead

[7] See also the Article 29 Data Protection Working Party *Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679*, adopted on 3 October 2017, endorsed by the European Data Protection Board at its first plenary session. These provide a high-level overview of the assessment criteria set out in Article 83(2) GDPR in Section III.

supervisory authority. Chapter VII GDPR establishes the regime for ensuring cooperation between lead and other concerned supervisory authorities, and permitting unified decision-making.[8]

2.20. Article 60 GDPR provides:

> *1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.*
>
> *2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.*
>
> *3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.*
>
> *4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.*
>
> *5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.*

[8] The relevant provisions enacting this regime must be read subject to, in particular, Articles 7, 70 and 127-128 and 131 GDPR.

6. Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7. The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.

8. By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

9. Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.

10. After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned. …

2.21. Article 60(4) refers to the consistency mechanism, which is in Section 2 of Chapter VII GDPR. Article 63 provides that: *"In order*

to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section." Article 65 GDPR provides, insofar as relevant, that:

> ***Dispute resolution by the Board***
>
> *1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:*
>
> > *(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject*
>
> *2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.*
>
> *3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall by adopted by the vote of its Chair.*
>
> *4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.*
>
> *5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the*

Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

DPA

The Commissioner

2.23. Section 115 DPA establishes that the Commissioner is the UK's supervisory authority for the purposes of the GDPR. Section 115 DPA provides, *inter alia*, that the Commissioner's powers under Articles 58(2)(i) (the power to impose administrative fines) and 83 GDPR are exercisable only by giving a penalty notice under section 155 DPA.

Penalties

2.24. Section 155(1) DPA provides that, if the Commissioner is satisfied that a person has failed or is failing as described in section 149(2) DPA, the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

2.25. Section 149(2) DPA provides:

(1) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following –

(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

(b) …

(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors)…

2.26. Section 155 DPA sets out the matters to which the Commissioner must have regard when deciding whether to issue a penalty notice and when determining the amount of the penalty.

2.27. Section 155(2) DPA provides that, subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the matters listed in Article 83(1) and (2) GDPR.

2.28. Schedule 16 includes provisions relevant to the imposition of penalties. Paragraph 2 makes provision for the issuing of notices of intent to impose a penalty, as follows:

(1) Before giving a person a penalty notice, the Commissioner must, by written notice (a "notice of intent") inform the person that the Commissioner intends to give a penalty notice.

(2) The Commissioner may not give a penalty notice to a person in reliance on a notice of intent after the end of the period of 6 months beginning when the notice of intent is given, subject to sub-paragraph (3).

(3) The period for giving a penalty notice to a person may be extended by agreement between the Commissioner and the person.

2.29. Paragraph 5 sets out the required contents of a penalty notice, in accordance with which this Penalty Notice has been prepared.

Guidance

2.30. Section 160 DPA requires the Commissioner to produce and publish guidance about how she intends to exercise her functions. With respect to penalty notices, such guidance is required to include:

(a) provision about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;

(b) provision about the circumstances in which the Commissioner would consider it appropriate to allow a person to make oral representations about the Commissioner's intention to give the person a penalty notice;

(c) provision explaining how the Commissioner will determine the amount of penalties;

(d) provision about how the Commissioner will determine how to proceed if a person does not comply with a penalty notice.

2.31. Pursuant to section 161 DPA, the Commissioner's first guidance documents issued under section 160(1) DPA had to be consulted upon and laid before Parliament by the Secretary of State in accordance with the procedure set out in that section. Thereafter, in issuing any altered or replacement guidance, the Commissioner is required to consult the Secretary of State and such other persons as she considers appropriate. The Commissioner must also arrange for such guidance to be laid before Parliament.

The Commissioner's Regulatory Action Policy

2.32. On 4 May 2018, the Commissioner opened a consultation process on how the Commissioner planned to discharge her regulatory powers under the DPA. The consultation attracted responses from across civil society, commentators, and industry (including the finance and insurance, online technology and telecoms, and charity sectors). The consultation ended on 28 June 2018. Having taken all the views received during the consultation process into account, the Regulatory Action Policy (the "**RAP**") was submitted to the Secretary of State and laid before Parliament for approval.

2.33. Pursuant to section 160(1) DPA, the Commissioner published her RAP on 7 November 2018. Under the heading "Aims", the RAP explains that it seeks to:

- *"Set out the nature of the Commissioner's various powers in one place and to be clear and consistent about when and how we use them";*

- *"Ensure that we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected";*

- *"Guide the Commissioner and our staff in ensuring that any regulatory action is targeted, proportionate and effective…"*[9]

2.34. The objectives of regulatory action are set out at page 6 of the RAP, including:

- *"To respond swiftly and effectively to breaches of legislation which fall within the ICO's remit, focussing on [inter alia] those adversely affecting large groups of individuals".*

- "*To be effective, proportionate, dissuasive and consistent in our application of sanctions",* targeting action taken pursuant to the Commissioner's most significant powers on, *inter alia, "organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data"*.

2.35. The RAP explains that the Commissioner will adopt a selective approach to regulatory action.[10] When deciding whether and how to respond to breaches of information rights obligations she will consider criteria which include the following:

- *"the nature and seriousness of the breach or potential breach";*

- *"where relevant, the categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion";*

- *"the number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy";*

- *"whether the issue raises new or repeated issues, or concerns that technological security measures are not protecting the personal data";*

[9] RAP, page 5.
[10] RAP, pages 6-7 and 10.

- *"the cost of measures to mitigate any risk, issue or harm";*
- *"the public interest in regulatory action being taken (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute)".*[11]

2.36. The RAP explains that, as a general principle, *"more serious, high-impact, intentional, wilful, neglectful or repeated breaches can expect stronger regulatory action".*[12]

2.37. Pages 24-25 of the RAP identify the circumstances in which the issuing of a Penalty Notice will be appropriate. They explain, *inter alia*, that in *"… considering the degree of harm or damage we may consider that, where there is a lower level of impact across a large number of individuals, the totality of that damage or harm may be substantial, and may require a sanction."* The RAP stresses that each case will be assessed objectively on its own merits. However, it explains that, in accordance with the Commissioner's risk-based approach, a penalty is more likely to be imposed in, *inter alia,* the following situations:

- *"a number of individuals have been affected";*
- *"there has been a degree of damage or harm (which may include distress and/or embarrassment);* and
- *"there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it).*

2.38. The process the Commissioner will follow in deciding the appropriate amount of penalty to be imposed is described from page 27 onwards. In particular, the RAP sets out the following five-step process:

a. **Step 1.** An 'initial element' removing any financial gain from the breach.

[11] RAP, pages 10-11.
[12] RAP, page 12.

b. **Step 2.** Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) DPA.

c. **Step 3.** Adding in an element to reflect any aggravating factors. A list of aggravating factors which the Commissioner would take into account, where relevant, is provided at page 11 of the RAP. This list is intended to be indicative, not exhaustive.

d. **Step 4**. Adding in an amount for deterrent effect to others.

e. **Step 5**. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship). A list of mitigating factors which the Commissioner would take into account, where relevant, is provided at page 11-12 of the RAP. This list is intended to be indicative, not exhaustive.

3. CIRCUMSTANCES OF THE FAILURE: FACTS

The Attack

3.1. This section summarises the circumstances of the failures which are the subject of this draft decision. This summary does not seek to provide an exhaustive account of the technical detail involved in each step of the Attack.

3.2. During the course of her investigation, the Commissioner has considered detailed technical reports and information provided by BA, not all of which can be reproduced here. In addition:

a. on 5 September 2019 BA provided written representations in response to the Notice of Intent issued by the Commissioner on 4 July 2019 ("**BA's First Representations**"), which included new information relating to BA's understanding of the facts underlying the incident. The Commissioner's Notice of Intent is referred to as the **"NOI"**;

b. on 11 October 2019 BA provided further information in response to requests for clarification from the Commissioner;

c. on 5 December 2019 BA provided further information in response to a request for further clarification from the Commissioner; and

d. on 31 January 2020, BA provided further detailed written representations in response to the draft notice provided by the Commissioner on 23 December 2019 ("**BA's Second Representations**"), which provided further information about the incident.

3.3. What follows is a summary of the key stages of the Attack, which disclosed the inadequacies in BA's security measures.

Step 1: Initial access

3.4. On 22 June 2018, an individual or individuals (who have not to date been identified), and who are referred to in this Penalty Notice as the Attacker for ease of reference, gained access to BA's IT systems. The Attacker maintained the ability to access BA's systems undetected between 22 June and 5 September 2018.

3.5. The Attacker obtained access to BA's network via the CAG. CAG is a tool that allows users to access a network and applications whilst working remotely. BA's CAG provided access to some of its IT applications so that authorised BA users could remotely log-in and use those applications as if they were in their office.

3.6. The Attack began with the Attacker obtaining access to login credentials that BA had provided for the use of an employee of "Swissport", a third-party provider of cargo services to BA. BA has been unable to determine how the Attacker was able to obtain compromised login credentials of a Swissport employee based in Trinidad and Tobago, although BA has identified that the Attacker compromised five accounts connected to Swissport.

3.7. The CAG was configured to allow access to a specific application on BA's system via the use of a single username and password. The compromised Swissport account was not protected by the use of multi-factor authentication ("**MFA**") (MFA is a system that restricts access to systems to those that can complete a combination of two or more steps. This usually involves the individual having knowledge of a password and possession of a mobile device to which a code is

sent. This code must be input, as well as the password, before access is granted.) Since the Attack, BA has implemented MFA on all remote access accounts.

3.8. By utilising the login credentials of the compromised Swissport account, the Attacker was able to access a set of applications available for Swissport employees in connection with Swissport's provision of services to BA. [redacted] As explained below, the Attacker was then also able to access other parts of BA's network, beyond the access which BA intended to grant to Swissport employees.

Step 2: Breaking out of Citrix

3.9. Having obtained initial access to BA's network, the Attacker was able to 'break out' of the Citrix environment to gain access to parts of BA's network that BA did not intend to be accessed by Swissport employees.

3.10. BA's experts hypothesised that the Attacker was able to break out of the Citrix environment into BA's wider network by [redacted] However, BA's First Representations provided an alternative explanation based on new information.

3.11. BA now believes that [redacted] BA has said that it has not been able to establish conclusively how the Attacker was able to break out of the Citrix environment, but believes that the Attacker may have [redacted] BA has since extended its Group Policy to restrict access [redacted]

3.12. [redacted]

3.13. [redacted]

3.14. BA believes that [redacted] allowed the Attacker to launch tools and scripts that Citrix would ordinarily have blocked, and to bring in tools from outside the Citrix environment. Having successfully copied a number of tools into the Citrix environment from outside the network, the Attacker used these tools to conduct network reconnaissance.

Step 3: Privilege escalation

3.15. During that reconnaissance, the Attacker obtained access to a file containing the username and password of a privileged domain administrator account [redacted]. The login details were stored in plain text, in a folder on the server [redacted]. In theory, any user within the relevant domain would therefore have had sufficient access to be able to open the file and obtain the domain administrator username and password.

3.16. A domain administrator account grants privileged access. In fact, it is an account which grants amongst the most privileged access of any user account in the Windows domain. Access to such domain administrator credentials therefore gave the Attacker virtually unrestricted access to the relevant compromised domain.[13] Due to

[13] The Commissioner has taken into account para 3.2 of BA's Second Representations.

the security risks that arise from the granting of such privileged access, the monitoring of these domain administrator accounts is a vital element of a system's security.[14]

Step 4: [redacted]

3.17. On 26 June 2018, after gaining credentials for [redacted], the Attacker was able to find a database System Administrator username and password [redacted]

Step 5: [redacted]

3.18. According to BA, on 23 June 2018 there were three failed login attempts using System Administrator credentials. On 25 June 2018, the Attacker then logged in successfully to three servers [redacted][16]

Step 6: [redacted]

3.19. [redacted]

[14] See: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-d--securing-built-in-administrator-accounts-in-active-directory and https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-accounts . See further the discussion in Section 6 below.

[15] [redacted]

[16] See para 3.5 of BA's Second Representations. We note that it is not accepted to be necessary for the Commissioner to set out this level of technical detail of each step of the Attack in this document.

[redacted]

Step 7: Personal data breach; XML file

3.20. By this stage the Attacker was in a position within the network where they had [redacted]

3.21. The Attacker then began to log in to different servers, presumably to find out what data was useful or valuable. On 26 July 2018, the Attacker was able to access log files, in plaintext, containing payment card details for BA redemption transactions.

3.22. The logging and storing of these card details (including, in most cases, CVV numbers) was not an intended design feature of BA's systems and was not required for any particular business purpose. It was a testing feature that was only intended to operate when the systems were not live, but which was left activated when the systems went live. BA has explained that this card data was being stored in plaintext (as opposed to in encrypted form) as a result of human error. This error meant that the system had been unnecessarily logging payment card details since December 2015. The impact of this failure was mitigated to some extent by the fact that the retention period of the logs was 95 days, which meant that the only accessible card details were those logged within the preceding 95 days. Nevertheless, the details of approximately 108,000 payment cards were potentially available to the Attacker.

3.23. BA informed the ICO that, around this time, the Attacker began to [redacted]

[17] BA's Second Representations, para 3.6. and BA's letter to the Commissioner, dated 11 October 2019.

Step 8: Personal data breach; payment card data [redacted]

3.24. During searches of BA's systems, the Attacker was able to identify files which contained code for the BA website. [redacted]

3.25. Between 14 August 2018 and 25 August 2018, the Attacker [redacted] to redirect customer payment card data to a different website: "BAways.com". BAways.com was a site owned and controlled by the Attacker. It appears from BA's Second Representations that [redacted] had the effect of copying and redirecting payment card data to "BAways.com" (which BA refers to as "skimming").[19] [redacted] remained active on BA's website for a period of 15 days between 21 August 2018 and 5 September 2018. During this time, when customers entered payment card information into BA's website, a copy was sent to the Attacker, without interrupting the normal BA booking and payment procedure.

Discovery and reporting of the breach

3.26. On 5 September 2018, a third party informed BA that data was being sent from britishairways.com to BAways.com.[20] Within 90 minutes,

[18] BA's Second Representations, para 3.7.
[19] *Ibid.*
[20] In its Second Representations, BA states that this is not correct: "*[the third party] only notified BA that it has identified POST requests to the domain BAways.com*". However, on 1 November 2018 provided the Commissioner with a document entitled "*British Airways Data Incident: timeline of key events*" which states: "*…notification received from [the third party] advising of [confidential] data being sent to BAways.com*". As POST requests are one element of data sharing between websites, the Commissioner does not consider this paragraph to be incorrect.

BA had adapted the malicious code and contained the vulnerability. 20 minutes later, BA blocked the URL paths to BAways.com.

3.27. The following day, 6 September 2018, BA notified the Commissioner, acquirer banks and payment schemes, and 496,636 affected customers about the incident. On 7 September 2018, BA notified an additional 39,480 affected customers.

3.28. BA has determined that 5 September 2018 is the last known date of unauthorised access to personal data within its system because that is the date on which it contained the vulnerability in its system and blocked the relevant URL paths.[21]

3.29. After 5 September 2018, BA implemented additional technical measures, including a next-generation anti-virus and endpoint detection and response tool, called "Crowdstrike Falcon" .

4. PERSONAL DATA INVOLVED IN THE FAILURE

4.1. The Attacker is believed to have potentially accessed the personal data of approximately 429,612 individuals, in particular:

- Name, address, card number and CVV number of BA customers - 244,000 data subjects;
- Card number and CVV only – 77,000 data subjects;
- Card number only – 108,000 data subjects;
- Usernames and passwords of BA employee and administrator accounts; and
- Usernames and pin numbers of up to 612 BA Executive Club accounts.[22].

5. PROCEDURE

5.1. This section summarises the procedural steps the Commissioner has taken. In the Annex to this Penalty Notice, a more detailed chronology is provided.

[21] See, for example, BA's Second Representations, paras 3.10-3.11; and BA's First Written Representations, paras 3.15-3.19.
[22] These accounts had their passwords changed and were checked for fraudulent activity.

5.2. BA notified the Commissioner of the Attack on 6 September 2018. In response, the Commissioner commenced an investigation into the incident. That investigation included various exchanges with BA and considering detailed submissions and evidence.

5.3. On 4 July 2019 the Commissioner issued BA with the NOI, indicating an intention to impose a penalty, pursuant to section 155(1) and Schedule 16 DPA. The proposed penalty was £183.39m.

5.4. BA submitted written representations and provided further information in response to the NOI on 5 September 2019 (BA's First Representations). BA did not request an opportunity to make oral submissions.

5.5. On 4 October 2019, the Commissioner asked BA a number of technical clarification questions as a result of, in particular, the provision of new information in BA's First Representations about how the Attack occurred. BA responded to these questions and provided further information on 11 October 2019 and 18 October 2019. The Commissioner asked further technical clarification questions on 25 November 2019, which BA responded to on 5 December 2019.

5.6. Between July and November 2019, BA and the Commissioner exchanged correspondence about a number of issues, including: (a) whether, and if so when, the Commissioner would be convening the panel of technical advisers ("the **Panel**"); (b) the application of the Commissioner's Draft Internal Procedure, which is discussed further below; (c) the application and/or operation of the Article 60 GDPR consultation process; and (d) BA's request for further opportunities to make submissions or representations prior to and during the Article 60 GDPR process.

5.7. In a letter dated 6 December 2019, the Commissioner:

a. confirmed that she no longer intended to exercise her discretion to convene the Panel;

b. confirmed that the Draft Internal Procedure would not be taken into account in setting any penalty imposed on BA, having considered the detailed representations BA had made on this issue in its First Representations. The letter confirmed that the Commissioner would continue to apply the EU and domestic

legislative framework in conjunction with the Regulatory Action Policy;

c. outlined how the Article 60 consultation process would be conducted in this case; and

d. agreed to give BA the opportunity to make further representations on the Commissioner's draft decision if BA agreed to extend the six-month period for the issuing of a penalty notice prescribed in paragraph 2 of Schedule 16, paragraph 2 DPA. The Commissioner proposed a new deadline of 31 March 2020.

5.8. The Commissioner's position on these issues was informed, in particular, by careful consideration of BA's First Representations, including new factual information provided by BA. Given the length and detail of those representations, the need for further information, and the overall complexity of the case, that consideration took time and considerable resources. That process also resulted in changes and clarifications to the form and content of the draft decision.

5.9. The Commissioner is also especially mindful of the fact that she is acting as lead supervisory authority pursuant to Article 60 GDPR, and that it is important that her investigation and decision be as comprehensive as possible, since the draft decision must be submitted for the consideration of other supervisory authorities pursuant to Article 60(3).

5.10. Although the Commissioner considered that a further opportunity for detailed representations from BA was not required by law, the Commissioner decided to accede to BA's request having regard, in particular, to: (i) the complexity of the case, (ii) BA's representations, and (iii) the fact that this is one of the first major decisions made under the new EU data protection regime. In those circumstances, the Commissioner considered that a further opportunity to make representations was appropriate provided that an agreement could be reached on extending the statutory timetable for the issuing of the decision.

5.11. Following further correspondence, BA confirmed on 23 December 2019 its agreement to a statutory extension of time to 31 March

2020. On the same date, the Commissioner provided BA with a draft decision, inviting BA to make further written representations and to provide any other relevant evidence it wished the Commissioner to take into account.

5.12. On 31 January 2020, BA provided further detailed written representations on the Commissioner's draft decision (BA's Second Representations).

5.13. On 10 February 2020, the Commissioner wrote to BA with four follow-up questions, which arose from her consideration of the Second Representations, to which BA responded on 24 February 2020.

5.14. On 3 April 2020, the Commissioner wrote to BA requesting information regarding the impact of the Covid-19 pandemic on BA's financial position. This letter identified certain financial metrics which the Commissioner suggested were relevant to considering the financial impact of Covid-19 on BA.

5.15. On 12 May 2020, BA provided detailed representations on the impact of Covid-19 on its financial position ("the **Third Representations**").

5.16. Having considered BA's representations, on 12 June 2020 the Commissioner wrote to BA requesting further information on BA's financial position, and reiterated her request for the specific financial metrics set out in the correspondence of 3 April 2020. The Commissioner requested a response by 19 June 2020.

5.17. On 16 June 2020, BA requested an extension until 26 June 2020 and requested an opportunity to make submissions and share financial information via a video call. BA subsequently provided the further information on 22 June 2020 and made oral submissions by video call on 2 July 2020.

5.18. In light of the ongoing exchanges and the circumstances of the Covid-19 pandemic, BA and the Commissioner agreed to a series of further extensions of the statutory deadline to 30 September 2020.

6. CIRCUMSTANCES OF THE FAILURE: BREACHES

BA's failures

6.1. The Commissioner's conclusion is that between 25 May 2018, when the GDPR entered into force, and (at least) 5 September 2018, when BA took action to prevent the transfer of personal data to BAways.com, BA failed to comply with its obligations under Article 5(1)(f) and Article 32 GDPR. BA failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Article 5(1)(f) and Article 32 GDPR.

6.2. This section describes the failures to comply with the GDPR that the Commissioner has identified and responds, where relevant, to BA's First and Second Representations and correspondence in relation to the Commissioner's NOI and draft decision.

The relevant standard

6.3. As set out above, Article 5 GDPR requires that personal data shall be processed in a manner which ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The controller, in this case BA, is responsible for, and must be able to demonstrate compliance with, that requirement.

6.4. Article 32 GDPR concerns the security of processing personal data and, taking 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 of varying likelihood and severity for the rights and freedoms of natural persons, requires a controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Such measures may include encryption of personal data and a process for regularly testing, assessing and evaluating the effectiveness of such technical and organisational measures.[23]

[23] See also Recitals 76, 77 and 83 GDPR.

6.5. Not every instance of unauthorised processing or breach of security will amount to a breach of Article 5 or Article 32. The obligation under Article 5 GDPR is to ensure *appropriate* security; the obligation under Article 32 is to implement *appropriate* technical and organisational measures to ensure an *appropriate* level of security, taking account of 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.

6.6. When considering whether there has been a breach of the GDPR and whether to impose a penalty, the Commissioner must avoid reasoning purely with the benefit of hindsight. The focus should be on the adequacy and appropriateness of the measures implemented by the data controller, risks that were known or could reasonably have been identified or foreseen, and appropriate measures falling within Article 5 and/or Article 32 GDPR that were not, but could and should have been, in place.[24]

6.7. BA has confirmed that it agrees with the description given in paras 6.4-6.5 above regarding the factors to be taken into account to determine an appropriate level of security.[25] Its position remains, however, that the Commissioner has mis-applied the requirements of Articles 5(1)(f) and 32 GDPR. Its submissions in this regard are addressed below.

6.8. Overall, having carefully examined the available evidence, including the material provided: (a) in particular, written submissions provided prior to the issue of the NOI; and (b) BA's First and Second Representations and relevant correspondence, the Commissioner is satisfied that BA failed to put in place appropriate technical or organisational measures to protect the personal data being processed on its systems, as required by the GDPR.

6.9. The principal failures, which are the basis of the Commissioner's decision to impose a penalty, are identified below, by reference to Steps 1-8 of the Attack, described in section 3 above.

[24] At paragraph 3.15 of BA's Second Representations, BA accepts that paragraphs 6.2, 6.4 and 6.5 correctly set out the approach the Commissioner must adopt in this case.
[25] BA's Second Representations, para 3.15.

Step 1: Initial access

6.10. As set out above, initial access was gained to BA's network using the compromised credentials of a user within a third-party supplier to BA, who was accessing BA's network remotely. This is known as a "supply chain attack". There was, before the introduction of the GDPR, guidance in the public domain about the steps that organisations need to take to address the threat of such an attack.

6.11. For example, the Centre for the Protection of National Infrastructure published a Good Practice Guide in April 2015 entitled "*Mitigating Security Risk in the National Infrastructure Supply Chain*", which recommended that organisations view supply chain security risk as being an extension of existing arrangements to mitigate security risks within the organisation. Thus, organisations should have a Security Risk Implementation Plan in place, which includes the following:

- risk scoring contracts to link in with existing risk assessments;
- due diligence / accreditation / assurance of existing suppliers and the adoption, through contracts, of proportionate and appropriate measures designed to mitigate risk;
- audit arrangements and compliance monitoring;
- comprehensive mapping of all tiers of the upstream and downstream supply chains to the level of individual contracts; and
- contract exit arrangements.

6.12. This advice has also been supplemented by more recent advice published by the National Cyber Security Council in January 2018.[26]

6.13. On 9 April 2018, the Commissioner published guidance on *GDPR Security Outcomes*.[27] This document provides guidance to

[26] https://www.ncsc.gov.uk/collection/supply-chain-security
[27] https://ico.org.uk/for-organisations/security-outcomes/. The Commissioner accepts paras 3.23-3.24 of BA's Second Representations which states that these documents are not "*prescriptive requirements*".

organisations on how to put in place appropriate technical and organisational measures, as required by Articles 5(1)(f) and 32 GDPR. It explains that what constitutes *"appropriate"* measures will *"depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation."* Addressing specifically the risks posed by granting third parties / processors access to systems, it explains:

> ***A.4 Data processors and the supply chain***
>
> *[…] understand and manage security risks to your processing operations that may arise as a result of using third parties such as data processors. This includes ensuring that they employ appropriate security measures.*
> *In the case of data processors, you are required to choose those that provide sufficient guarantees about their technical and organisational measures. The GDPR includes provisions where processors are used, including specific stipulations that must feature in your contract.*

6.14. The guidance also refers and links to the NCSC's Supply Chain Security guidance document, referred to above. In relation to the issue of identity and access control, the Commissioner's guidance states: *"You should appropriately authenticate and authorise users (or any automated functions) that can access personal data. You should strongly authenticate users who have privileged access and consider two-factor or hardware authentication measures."*

6.15. There has also been other guidance in the public domain for some time concerning identity access management standards, including the need to ensure that users only have access to software required for their role. For example, OWASP published a list of "Top Ten Proactive Controls 2016", which is described as a *"list of security concepts that should be included in every software development project"*. Control number 6 is the implementation of appropriate access controls, which includes compliance with the principle of least privilege. That privilege is described as follows: *"when designing access controls, each user or system component should be allocated*

the minimum privilege required to perform an action for the minimum amount of time."[28]

6.16. The National Institute for Standards and Technology ("**NIST**") in guidance entitled "Back to Basics: multi-factor authentication" (2016) explained that: "*you should use MFA whenever possible, especially when it comes to your most sensitive data…"*. This is consistent with later guidance published by the NCSC.[29]

6.17. There are a number of appropriate measures that BA could have considered to mitigate the risk of an attacker being able to access the BA network by compromising a single username and password. These measures include, for example, MFA, external public IP address whitelisting, and IPSec VPN. Any one of these options would, in the Commissioner's view, have been appropriate.

6.18. In the first instance, it is for the controller to consider what measures are appropriate for securing its system. BA's own Network Access Control Policy of 7 October 2017 states: *"Multi-factor authentication shall be incorporated for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the network."* It therefore appears that BA itself considered MFA to be an appropriate measure to mitigate the risk of unauthorised remote access via Citrix in the context of its network.

6.19. BA's First Representations indicated that, [redacted][30]

6.20. BA also confirmed to the Commissioner in its response to an Information Notice dated 12 October 2018 that it hosted 243 applications on the Citrix Access Gateway. Of these applications, 13 were not protected by MFA, [redacted].

6.21. BA has not provided a satisfactory explanation as to why Citrix access was the subject of a separate risk assessment process or why

[28] See: https://wiki.owasp.org/index.php/OWASP_Proactive_Controls_2016#6:_Implement_Access_Controls
[29] https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services
[30] BA's First Representations, para 2.28.

it was deemed unnecessary for certain applications, [redacted], to comply with the policy requiring MFA.

6.22. BA has indicated that [redacted][31] However, BA has been unable to provide a copy of that document and, accordingly, the Commissioner has not been able to assess its contents as part of her consideration of whether BA had appropriate measures in place during the relevant period. It is unlikely, moreover, that [redacted] would accurately reflect the full range of cyber security risks in 2018. Further, [redacted] before the enactment of the GDPR in 2016 and its coming into force in May 2018.

6.23. The use of MFA in accordance with BA's own policy, and which BA has since implemented across all remote access users, would have been an appropriate technical measure to implement for users remotely accessing [redacted].

6.24. In a letter dated 11 October 2019, BA responded to the Commissioner's queries[32] about its use of MFA as follows:

[redacted]

[redacted]

[31] Letter from BA to Commissioner of 11 October 2019.
[32] BA's First Representations, paras 2.30-2.31.

[redacted]

6.25. This suggests that BA did not approach its obligations under Articles 5(1)(f) and 32 GDPR correctly. [redacted] Even if BA did not wish to rely upon MFA to secure its remote access for the administrative reasons it has outlined, an alternative option would have been a VPN tool which operated between IP addresses (for example, an IPSec VPN). Such a tool allows remote sites to be connected together in a manner that could have prevented the Attacker from using compromised third-party credentials.[33]

6.26. In its Second Representations, BA claims that since [redacted] did not allow access to personal data, the fact that it was not protected by MFA is consistent with relevant guidance. However, in practice BA's position is that it relied on a risk assessment to depart from the default position, as set out in its policy, that "*all remote network access*" would be protected by MFA. Given how dated the risk assessment is, and that no copy can now be located, it is not possible to say that BA took into consideration the risk, the state of the art, the cost, or the available technical measures when deciding what security was appropriate.

6.27. Moreover, BA has not identified alternative measures it put in place having reached the view that MFA was not necessary in this context.

[33] In response to paras 3.34-3.36 of BA's Second Representations, the Commissioner accepts that Citrix can be regarded as an SSL VPN, and suggests an IPSEC VPN as an alternative to – and not in addition to – the use of MFA-enabled Citrix in its role as an SSL VPN.

At paragraph 6.17 above, the Commissioner has identified alternative appropriate measures that BA could have adopted if the view was properly taken that MFA was not required, which may have justified a departure from its policy position. With respect to whitelisting:

a. BA's First Representations[34] suggested that whitelisting of IP addresses would not have been effective in preventing this step of the Attack because the requests to servers within the network were coming from other servers – which would not have been whitelisted had a whitelist been in place. However, this point only applies once an attacker has gained access to the wider BA network after breaking out of the Citrix gateway. Before then, the use of IP whitelisting would have been an effective measure preventing the Attacker from gaining initial access to the Citrix Gateway. BA could have had whitelisting in place that would have ensured only certain individuals, or organisations, could access it.

b. In its Second Representations, BA argued that it was untenable to suggest that whitelisting was an alternative in practice due to the global spread of its users.[35] However: (i) there is no evidence that BA considered what alternative measures could be put in place as an alternative to MFA, which was the solution identified in its policy; and (ii) even if BA is correct that this solution would not have proven viable, it does not obviate the need to consider appropriate measures or explain why other appropriate measures were not in place, including in particular MFA.

6.28. BA has provided a copy of its Third-Party System Access Agreement in relation to Swissport[36], which included information on general password security. A contractor or third-party access policy is an agreement between two parties regarding access and any security considerations. While the Commissioner recognises that setting security standards for suppliers is commendable, the Commissioner does not consider reliance on such agreements alone to be an effective measure in ensuring that Swissport user credentials, and the access they provided to BA's systems, were appropriately

[34] Para 2.54.
[35] BA's Second Representations, para 3.37.
[36] Annex 9a Swissport Trinidad and Tobago – BA Third Party Systems Access Agreement.

secured.[37] The GDPR requires BA to take appropriate technical measures to ensure that its systems are appropriately secured. BA, through its Network Access Control Policy, appears to accept this, but failed to implement MFA as required by its own policies, or apply appropriate alternative measures.

6.29. For the reasons given above, BA should have ensured that MFA was in use in accordance with its policy for securing access to its network or, having carried out an appropriate risk assessment, put in place appropriate alternatives. MFA and the alternative measures identified above are readily available and mature solutions (i.e. solutions that have been known about in the industry for a long period of time, prior to the Attack), and which could have been implemented by BA without excessive cost.

Step 2: Breaking out of Citrix

6.30. As set out above, in its First Representations BA explained that, based on information it had obtained since receiving the NOI, it believes that the Attacker was able to break out of the Citrix environment by [redacted].[38]

6.31. It is incumbent on BA to identify the risks associated with remote access, and to ensure that those risks are mitigated appropriately. The CAG allows remote access to internal BA applications, its infrastructure and networks. It is important that such access is configured appropriately and tested in order to mitigate against or prevent security risks, including preventing unauthorised or unprivileged users from 'breaking out' from the CAG.

6.32. There is guidance freely available, including from Citrix,[39] which identifies breakout from Citrix as a known security issue and lists effective measures to mitigate this risk.

---

[37] This agreement also referred to the DPA 1998, and had not been updated to take account of the GDPR coming into force. In response to paras 3.41-3.42 of BA's Second Representations, it should be made clear that the Commissioner does not seek to comment on the appropriateness of BA's arrangements with Swissport themselves.

[38] BA's First Representations, paras 2.35-2.38.

[39] https://www.citrix.com/blogs/2019/04/29/citrix-tips-top-10-findings-from-citrix-environment-security-assessments/, see para 8. See also earlier guidance published by Citrix and Mandiant in 2016, entitled *"System Hardening Guidance for XenApp and XenDesktop"* which states at page 2 *"Mandiant continues to observe that one of the commonly overlooked visualization security issues is environment or application jailbreaking."*

6.33. In this respect, BA did not approach its obligations under Articles 5(1)(f) and 32 GDPR correctly. It did not have any up-to-date risk assessment of the CAG, or of the applications (such as [redacted]) that were accessed through the gateway, to ensure that access to these applications was secure and could not be used to 'breakout' from the CAG.

6.34. As described above, [redacted]. However, the risks of attackers using [redacted] to compromise systems is well-documented (and was well-documented long before the Attack).[redacted]

6.35. In the light of these well-established risks, appropriate security measures would have ensured that non-administrator accounts (such as the account used by the Attacker) did not have access to [redacted] or other software not required by such account-holders. For example, in a Joint White Paper from Citrix and Mandiant entitled "*System Hardening Guidance for XenApp and XenDesktop*" (2016)[41], a number of recommendations are set out, including:

> "*Remove all undesired Windows and Citrix functionality – even if there appears to be no direct security threat, it is important to minimize the attack surface by removing unnecessary functionality. This includes removing:*
>
> - *All shortcuts and help keys*
> - *Access to all unused ICA channels*
> - *Unused Windows functionality such as pre-installed applications*
> - *Access to printers or devices that are not absolutely required*
>   - *Especially since this often to file system access via "Print to File"*

[40] [redacted]

[41] https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/system-hardening-for-xenapp-and-xendesktop.pdf

- *Drivers that provide access to devices and services not required…"*[42]

6.36. More specifically, the white paper refers to [redacted]

[redacted]

6.37. In addition, the Commissioner's guidance *A practical guide to IT security: Ideal for the small business* (2016), states: *"each user should use an account that has permissions appropriate to the job they are carrying out at the time".*[43] Although this guidance is aimed at small businesses, it applies *a fortiori* to large data controllers.

6.38. Similarly, the Commissioner's guidance in respect of *Security outcomes*, which applies to all controllers and processors, explains that it is necessary to:

> *… document and manage access to personal data and systems that process this data. Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed. You should undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights.*[44] [Emphasis added]

6.39. That guidance document also explains that a typical example of a measure that can be taken to mitigate the risk of a cyberattack is:

---

[42] https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/system-hardening-for-xenapp-and-xendesktop.pdf, page 4.
[43] ICO Guidance: *"A practical guide to IT security: ideal for the small business"* (2016) page 6.
[44] https://ico.org.uk/for-organisations/security-outcomes/

"minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity."

6.40. With respect to Step 2 of the Attack, there are a number of appropriate measures that BA could have taken, which would have mitigated the risk of the Attacker (or any other attacker / individual) gaining access to [redacted]. It would have been appropriate for BA to put in place at least one of the following measures to secure its network. Each of these options would have aided in preventing this element of the Attack, in accordance with the principle of least privilege described in the guidance above)[45], which the Commissioner expects data controllers to follow.

6.41. First, BA could have implemented application whitelisting. Organisations can configure their networks so that only certain programs or applications can be run by individuals gaining access to the network through a specified route. A whitelisting rule could specify, for example, that access is only granted for use of the [redacted] application. If an attacker then gains access, and seeks to run [redacted] or any other unnecessary software, that tool will be blocked because it is not on the application whitelist.

6.42. At the relevant time, there were various technical means by which BA could implement application whitelisting within the Microsoft Operating System, in accordance with the principle of least privilege, and which would have prevented or mitigated the risk of an attack of this kind.[46] These tools could also be used to alert administrators to attempts by third parties to access tools they do not have permission to use.

6.43. Second, BA could have implemented "BlackLists", which are the inverse of a whitelist and work by blocking certain applications rather than permitting them. A rule could have been put in place to

[45] See also page 3 of the ENISA Guidance entitled "*Indispensable baseline security requirements for the procurement of secure ICT products and services*" (December 2016) which describes the principle of least privilege "… whereby administrative rights are only used when absolutely necessary…" as an "indispensable baseline security requirement".

[46] There are freely available resources that come with Microsoft Server Tech, such as Software Restrictions Policies and App Locker; BA could also have purchased standalone whitelist software to provide more control.

prevent the use of [redacted] or any other software not required for a particular user's role.

6.44. Third, BA could have completed an application/server hardening process, thereby reducing the vulnerabilities on its network. This involves, *inter alia*: (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. Such a process can ensure that users are only granted access to what is necessary. Again, the need to implement such measures is clear from relevant guidance. For example, the Commissioner's Guidance on *Protecting personal data in online services: learning from the mistakes of others*, published in May 2014, states: *"An important principle in network security is to 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."*[47]

6.45. BA has argued that the principle of least privilege was not relevant in this case because while the Attacker gained access to BA's network via a low privilege user account, the Attacker carried out most of its activities using an account with administrator privileges.[48] This argument is misconceived. The point is that the Attacker should not have been able to break out of the CAG using [redacted] having gained accessed using the compromised credentials. It was the absence of necessary server hardening that allowed the Attacker to ultimately gain access to privileged credentials.

6.46. BA has also argued that third-party suppliers accessing [redacted] via Citrix will not be using a BA device, and so device hardening is not a relevant consideration in this case. However, application / server hardening are relevant measures that could have been considered. Rather than [redacted] as an application, it is the

[47] Para 44, https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf
[48] BA's Second Representations, para 3.43.

environment within which [redacted] was accessed, that called for a more rigorous hardening process.

6.47. As part of such application and server hardening BA might also have been expected to generate server documentation. This is a procedural / organisational measure that could have been put in place to aid in risk assessments and implementation of whitelists or other measures. Such documentation may include a list of software, applications and protocols required for an application to work. Such a process can help to indicate, for example, that for [redacted]. This, in turn, aids procedurally and organisationally with the implementation of appropriate security measures such as MFA, VPNs or software whitelisting. It also aids in risk assessment, as organisations can see clearly which pieces of software are available for execution on which systems. Unnecessary applications and/or protocols can be disabled or removed, and the list of applications that are required can be kept under closer review by identifying, for example, whether they are outdated (which can then be addressed). BA has not suggested that any server documentation was in place as part of a process of application and device hardening.

6.48. BA has argued that the Attacker in this case made conscious efforts to avoid detection, for example by [redacted].[49] However, [redacted] is a relatively simple step and this method of avoiding detection would not have been successful if the principle of least privilege, or any of the preventative measures identified above, had been in place. For example, had the Attacker been unable to bring any unauthorised files or programs into the environment, so that the only authorised pieces of software were those required for employee's roles (for example, by whitelisting) then [redacted]. Again, the measures identified above are freely available, and some are provided by Microsoft as part of the operating system used by BA.

6.49. BA had the opportunity to use such controls to prevent unnecessary access to certain tools. As explained above, BA now believes that Group Policies in effect at the time would have prevented the

[49] BA's First Representations, para 2.11.

Attacker [redacted] within the Citrix environment (which was the tool that BA's experts hypothesised may have been used in the Attack). The approach adopted by BA to these other tools is, in effect, a form of blacklist or control policy. But the same approach was not taken to [redacted], notwithstanding the risks that unnecessary access to [redacted] presented.

6.50. BA did disable the ability to right click on an application. This only prevented a person from right clicking it and choosing "open".[50] However, this was inadequate to prevent an attacker or other unauthorised user from opening it. The Attacker would have been able to open applications [redacted] by other methods, for example, by typing [redacted] into the file explorer tab or by selecting 'File' and 'Open' using left click.[51] [redacted]

6.51. Since the Attack, BA has blocked the use of [redacted] by adding them to the Group Policy that is believed to have prevented the use of [redacted] within the Citrix environment.

6.52. Finally, in addition to the above, there were organisational elements of BA's security procedures which allowed the failings discussed here to exist within the system for a significant period.

6.53. One such example is the scope of the penetration testing performed on the BA environment. BA has argued that its testing relied on [redacted][53]

[50] BA, in its Second Representations at para 3.44, states *"It is not clear what the ICO means by 'selecting 'File' and 'Open' using left click".* For the avoidance of doubt, this means from within explorer one clicks on File > Open then browse to the PowerShell location and then double left click on Powershell.exe.
[51] This is a possibility which BA itself recognises at para 2.38 of its First Representations.
[52] BA's Second Representations, para 3.44.
[53] BA's First Representations, paras 2.40-2.42.

6.54. However, there is only evidence of [redacted]. Had this testing been implemented sufficiently, the ability to break out of these remote access systems into the wider network would have been identified.

6.55. Additionally, the Commissioner has only seen evidence of [redacted].

6.56. Had more rigorous testing been performed, or had internal penetration tests been performed (where an attacker with access to the network was simulated), many of the problems identified within this decision are likely to have been detected and appropriately addressed.

Step 3: Privileged escalation

6.57. Having broken out of the Citrix environment, the Attacker was able to obtain privileged access details, i.e. the details of a domain administrator account, because those details were saved in an unencrypted plain text file. This approach to storing passwords in text files is referred to as hardcoding.

6.58. The use of hardcoded passwords is recognised generally as being a problematic practice that increases the risk of and implications of an attack. The Open Web Application Security Project (OWASP) reported in 2016 that:[54]

> *"The use of a hard-coded password increases the possibility of password guessing tremendously.*
>
> ***Consequences***

[54] https://www.owasp.org/index.php/Use_of_hard-coded_password

- *If hard-coded passwords are used, it is almost certain that malicious users will gain access through the account in question.*
- ***Severity:*** *High*
- ***Likelihood of exploit*** *Very high* [Emphasis added]

The use of a hard-coded password has many negative implications - the most significant of these being a failure of authentication measures under certain circumstances."

6.59. There is clear guidance in the public domain that warns about the need to apply particular protections to privileged accounts. For example, the NCSC's Guidance on *Preventing Lateral Movement*[55], published in February 2018, explains:

1. Protect credentials

All credentials on a network, especially those of administrator accounts, should be adequately protected to prevent attackers using them to gain access to devices and systems.

A common type of attack involves stealing a security token to gain access to another device or server. 'Pass the hash' is an example of this, where a stolen hash is used to authenticate the attacker. Passwords should not be stored in plain text by users or systems, and password hashes should be protected to prevent attackers easily accessing them.

…

3. Protect high privilege accounts

Local and domain administrative accounts - with access to most systems and data - are powerful tools in a network. Their use should be tightly controlled and locked down.

Administrators should use separate accounts; one for day-to-day business use (such as web browsing and emails), and a privileged administrator account that should only be used

[55] https://www.ncsc.gov.uk/guidance/preventing-lateral-movement

on separate admin devices. This reduces the risk of an infected device being used for admin purposes.

Administrator accounts should be prevented from browsing the web and accessing emails, and only be used when a task requires elevated permissions.

6.60. There were a range of appropriate measures that BA could have put in place to prevent the Attacker obtaining privileged access.

6.61. First, it is evident from [redacted].

6.62. This same outcome could have been achieved more securely [redacted] The use of this readily available tool would have avoided the hardcoding of the password, and thereby prevented the Attacker from obtaining privileged access.

6.63. Second, BA could have adopted an approach of delegating privileges to specific admins or users (which is recommended by Microsoft[56]). Instead of [redacted], BA could have used this delegation to limit each user's access to the tools, including administrator tools, which the individual user or users requires. This approach again reflects the "least privilege" principle, discussed above. [redacted] using the above method

[56] See https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory

would have been adequate, without increasing the risk by allowing all accounts domain administrator access.

6.64. These features / tools are freely available as part of the Microsoft Operating System used by BA. While they would not have prevented the Attack, they could have mitigated the risks associated with such an attack by permitting early detection. This early detection, if reacted to promptly, could have aided BA in removing the attacker from their network before privileged accounts were compromised and further damage was done within the BA network.

6.65. Generally, the risks associated with storing credentials within scripts can be mitigated with steps such as: (a) monitoring access to the script, (b) requiring the input of credentials on execution of the script, or (c) encrypting the script itself when not in use. The Commissioner accepts that due to the location and functionality of the mapping script these mitigations were not available to BA in this particular circumstance. However, this does not mean that the [redacted] was acceptable or appropriate, as there were other, more secure, methods of achieving the desired outcome, as outlined above.

6.66. Additionally, security testing of the CAG and associated applications may have identified the ability to break out of the Citrix environment. Vulnerability scanning, security testing and internal credential-based penetration testing may have identified issues associated with [redacted].

Step 4: [redacted]

6.67. The risks associated with [redacted] are well-known. [redacted]

[redacted]

6.68. Systems Administrator accounts are generally disabled by default, and systems that use that account are usually legacy systems. It is

reasonable to assume that BA was aware of the security implications of the Systems Administrator account, since a decision would have to have been taken to enable that account.

6.69. As explained above, it is standard practice, in line with the guidance from the NCSC and the Commissioner, that systems should be configured in a way that complies with the principle of "least privilege". In practice, the Systems Administrator account should only have been enabled, when necessary, on a case-by-case basis. [redacted]

6.70. There are a number of appropriate measures that BA could have implemented to prevent or mitigate the risk of an attack of the type which occurred. In particular:

a. BA could have implemented its own policy, which recognised the need to use different passwords for different accounts, when setting up key accounts that gave control of the whole system.

b. BA could have used a different means of [redacted]. This would have avoided the password being saved in hardcode form, and would have avoided the same password being set as the default [redacted].

c. BA could have enabled [redacted]

[redacted]

6.71. Alternatively, BA could have mitigated the risk presented by [redacted] by monitoring access to the relevant files and/or logging access to the file, which could have alerted BA to its misuse.

6.72. None of the above measures would have entailed excessive cost or technical barriers. They are all readily available measures available through the Microsoft Operating System used by BA.

6.73. The Commissioner accepts that, in some cases [redacted] the discovery of credentials was not useful to the Attacker.[58] However, it is still the case that the compromise of [redacted] was a significant step in the early stages of the Attack. For example, the [redacted]

[57] [redacted]

[58] In para 3.4 of its Second Representations BA suggested that [redacted]

[redacted] In its letter to the Commissioner of 12 October 2018, BA explained that:

[redacted]

6.74. Moreover, the Commissioner does not accept that the storage of such credentials in plain text is standard practice or an acceptable way of 'aiding functionality', as suggested by BA. The storage of passwords within scripts and configuration files prevents employees needing to enter these passwords upon the execution of the script(s), as discussed above. If this is why BA stored passwords in this way, that is not an acceptable reason to store passwords in plaintext, when considering the minimal time saving it allows, the high risk it poses, and the alternative methods (such as requiring an input of the passwords to run the script but not storing them as part of the script permanently) available to BA as an organisation. If, on the other hand, these scripts existed as part of an automatic process on the server,[61] this is equally unacceptable. The Commissioner's concern is that the credentials were being stored in plain text, not why that may have been so.

Step 5: [redacted]

6.75. As described above, following failed attempts to access three servers, the Attacker obtained access [redacted]. Having found a hardcoded password file, the Attacker enabled the Guest Account and added it to a local admin group, thereby giving it local administrative control.

6.76. Microsoft's website explains:

> *The Guest account has been disabled by default since Windows 8 because it was determined to be a security risk.*

[60] See BA's letter to the Commissioner, dated 12 October 2018.
[61] See para 3.47 of BA's Second Representations, where it states that "*it is possible that these scripts existed as part of an automated process on the server*".

For that reason, Microsoft asked users not to use the Guest account. When you have guests, have them sign in to a local Standard user account.

6.77. Although the guest account was disabled on BA's system, there was no mechanism in place to detect the unauthorised enabling of that account by the Attacker. There are a number of appropriate measures that could have been put in place to detect that activity:

a. Monitoring of failed attempts to log-in using the Systems Administrator account. Given that such authentication fails should not happen (as access should be carefully restricted to such accounts) the logging of failures to gain access should enable the organisation to detect activity that may be of concern. Email alerts could have been put in place to bring to the organisation's attention that there had been a number of failed login attempts;[62] and

b. Monitoring of the use of guest accounts. The addition of the guest account to the local administrator group should have been identified by monitoring of the system. Guest accounts have been flagged as high risk, even though they have limited access to the system. Local administrators have unlimited access to the relevant system. The addition of a guest account to the local administrator group should have been detected, and would have alerted BA to a problem. But no monitoring was in place (using PowerShell or any alternative tool) that detected the unauthorised activity in this case.

6.78. Another option would have been the implementation of a Privilege Access Management ("**PAM**") audit and monitoring tool to securely manage all privileged accounts across BA's infrastructure. A PAM tool would have secured the issuing and use of a privileged account only to those users or applications that needed them, and when they needed them. The use of specific privilege accounts could have been monitored and audited following their release, to confirm usage and any relevant actions taken. Where appropriate, the account can be

[62] Microsoft information explains how and why to implement these lockout policies, e.g. https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-duration

revoked and its password changed to protect the account from misuse.[63]

6.79. Additionally, user access management is an industry wide methodology, based upon the principle of least privilege. It is identified in standards such as NIST and ISO27001 as a requirement for the management of user privileges and access to system and system resources. It is delivered through several industry recognised tools and the access management process is used to provision users, for example to applications, infrastructure and databases.

6.80. The Commissioner accepts that comprehensive monitoring of an IT estate as large as BA's may be a relatively complex task. However, appropriate measures to both monitor and prevent high risk actions such as the unauthorised creation of administrator accounts were available to BA. BA failed to put in place these measures, which could have prevented, or at least alerted BA, to this Attack.

Step 6: [redacted]

6.81. It is well-known that [redacted] There are a range of measures that can detect such activity.

6.82. The Commissioner notes that in this step of the Attack, the focus must be on detection rather than prevention, as the earlier failures to secure passwords and accounts meant that the Attacker was already able to move freely around BA's system.

6.83. A key detection measure that would have been appropriate is logging. The NCSC describe logging as *"the foundation on which security monitoring and situational awareness are built".*[65] There are a number of ways in which such logging can be implemented, including using a Security Information and Event Managing System

[63] (https://www.cyberark.com/products/privileged-account-security-solution/core-privileged-account-security/)
[64] See [redacted]
[65] NCSC introduction to logging for security purposes as of 08 December 2019 - https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes

or using manual searches of logs to identify concerning activity, focusing on critical servers. [redacted] is an unusual step to take in operating a system, but is a well-known method of attack. It is, therefore, a clear sign that the system may be compromised. Such action may have been detected if it had been accurately logged.

6.84. BA had in place [redacted]. Had it been used to assess access management logs amongst other log files such as network logs or application logs, BA would have been alerted to the creation of or use of privileged accounts or to the elevation of a guest account to an administrator account. It could also have been used to identify brute force attacks and other high-risk actions and, given adequate scope on the network, changes to the BA website code. However, BA were not generating or monitoring logs to a sufficient level to detect these high-risk actions. This is evident, for example, in [redacted][66]

Step 7: Personal data breach; XML files

6.85. A failure to remove administrative or debugging functions will compromise the security of a site. This is an issue identified by, for example, OWASP in its Top 10 Insecure Configuration Management issues of 2004.[67]

6.86. There are a number of measures that BA could have implemented which would have identified the failure to remove the debugging code.

---

[66] See, in particular, the "Security Monitoring" Guidance published by the National Cyber Security Centre at: https://www.ncsc.gov.uk/guidance/c1-security-monitoring, which notes that *"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."*

[67] OWASP Insecure Configuration Management as of 08 December 2019 - https://www.owasp.org/index.php/A10_2004_Insecure_Configuration_Management

6.87. First, an important example of such measures is the use of manual code review. A 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. At least 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. When used together with automated tools and manual penetration testing, code review can significantly increase the cost effectiveness of an application security verification effort."*[68]

6.88. BA has confirmed that some manual code reviews did take place during the movement of code from development to production. These code reviews appear to have been sufficient to ensure that the code would do what it was intended to do. However, these reviews fall short of industry standards in many areas, especially in the review of logging code required under OWASP guidance on code reviews.[69] That guidance states that a review of any logging code should be performed to identify, amongst other things, what information should not be logged, such as sensitive personal data and some forms of personally identifiable information. BA has not suggested that it was undertaking this type of review. While the reviews were appropriate to ensure that the code operated as expected, they were not adequate to ensure that additional, appropriate security measures (such as appropriate logging) were in place.

6.89. Second, whilst the Commissioner accepts that the Payment Card Industry Data Security Standard ("**PCI DSS**")[70] does not require scanning[71], the Commissioner notes that BA appears to have breached ("PCI DSS") (2008) requirement 3.1, which provides: "*Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy."* Moreover, the logging of card details was in error, rather than by design, confirming the absence of any valid business need for the processing.

6.90. The Guidance accompanying PCI DSS requirement 3.1 provides that: "*Extended storage of cardholder data that exceeds business*

[68] https://www.owasp.org/images/d/da/OWASP_Code_Review_Guide_-_V1_1.pdf.
[69] https://www.owasp.org/images/5/53/OWASP_Code_Review_Guide_v2.pdf.
[70] Payment Card Industry Data Security Standard
[71] BA's Second Representations, para 3.30.

need creates unnecessary risk. The only cardholder data that may be stored is the primary account number or PAN (rendered unreadable), expiry date, name, and service code. ***Remember, if you don't need it, don't store it!***" (original emphasis). The Guidance makes it clear that CVV numbers (the majority of which were unencrypted in this case) should not have been logged by BA at all.

6.91. The fact that BA did not identify that the credit card logging feature remained active after its system went live in 2015, including in particular after the GDPR entered into force in May 2018, demonstrates a failure to adopt appropriate technical and organisational measures, including regular testing, assessing and evaluation of its systems, to ensure an appropriate level of protection for customer personal data and compliance with the data protection principles, including data minimisation.

Step 8: Personal data breach; payment card data [redacted]

6.92. Attacks using [redacted] are well-documented as risks to systems and networks.[72] BA could have put in place measures to detect malicious action such as that which occurred during the Attack, in particular file integrity monitoring.[73] This type of monitoring allows the system to detect and alert an organisation to changes being made to its code. While it does not stop an attacker from changing the code, it allows the organisation to detect that changes have been made, and to establish whether they are unauthorised.

6.93. PCI DSS requires (requirement 10.5.5) that merchants "*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.*"[74] PCI

[72] See, for example, [redacted]

[73] Having considered BA's First Representations, the Commissioner no longer refers to traffic monitoring or endpoint monitoring specifically, and considers that the relevant failure by BA was the failure to put in place appropriate file integrity monitoring and events logging on the network.

[74] Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures, Version 3.2.1, May 2018

DSS notes that, without file integrity monitoring a hacker or user with malicious intent could alter file contents or steal data undetected. The requirement set out in PCI DSS para 11.5 reinforces the point: *"Deploy a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorised modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly."*

6.94. BA had established manual change management controls, meaning that if an employee wanted to make any changes to BA's website, code they had to go through a formal change management process to obtain approval for that change. However, BA has not identified any technical or organisational measure it had in place to detect unauthorised changes to its website code. In this instance, BA was only alerted by a third party that significant changes had been made to the website code.

Conclusion on failures under Article 5 / 32 GDPR

6.95. The Commissioner's view is that the personal data stored within and processed by BA's systems, including the BA website, were not being processed in a manner that ensured appropriate security of that personal data, using appropriate technical or organisational measures. BA failed to implement appropriate technical and organisational measures to protect the rights of data subjects and comply with the data protection principles.

6.96. This is demonstrated by the fact that, as set out above, each step of the Attack could have been prevented, or its impact mitigated, by BA implementing one or more of a range of appropriate measures that were open to it.

6.97. The risks created by the way in which BA configured its network ought to have been identified by BA and resolved. Although BA was not required to implement every measure identified above, the Attack exposed BA's failure to secure its systems in an appropriate manner. There was a failure to implement appropriate measures in relation to each of the steps individually outlined above and, in particular when the failures are looked at cumulatively, the

Commissioner considers that BA was in breach of Articles 5(1)(f) and 32 GDPR.

BA's wider arguments

6.98. In addition to the arguments referred to above, BA's Representations raised a number of more general legal and/or factual arguments. This section addresses the following submissions made by BA:

a. **First**, that the Commissioner was wrong to apply Article 25 GDPR in the NOI.[75]

b. **Second**, that the Commissioner erred in her factual findings in the NOI and she could not therefore sustain her finding that BA failed to put in place appropriate measures. In particular, BA contended that the Commissioner erred by applying an *"unduly high standard"* and the benefit of hindsight.[76] BA has advanced similar arguments in its Second Representations in response to the draft decision.[77]

c. **Third**, that the Commissioner applied an unlawful approach by failing to have regard to the whole of BA's security environment.[78] BA expended substantial efforts and applied significant resources to its preparation for the GDPR, which should also be taken into account.[79]

6.99. As part of its wider arguments, BA also made a number of representations on the Commissioner's approach to determining whether to impose a penalty, and the methodology adopted in calculating the proposed penalty in the NOI.[80] These arguments are addressed in section 7, below.

(1) Article 25 GDPR

6.100. In the NOI, the Commissioner provisionally found that BA had infringed Article 25 GDPR as well as Articles 5(1)(f) and 32. BA

[75] BA's first Representations, para 3 of the Executive Summary and paras 2.55-2.60.
[76] BA's First Representations, para 2 of the Executive Summary, and Chapter 2, in particular, paras 2.3-2.192.35-2.38. See also BA's Second Representations, paras 1.3.1, 3.15-4.43.
[77] BA's Second Representations, paras 3.1-3.48.
[78] BA's First Representations, paras 2.20-2.24.
[79] BA's First Representations, Chapter 1.
[80] Specifically, see paras 5.8-5.13, 6.13-6.28, 7.14, and 9.1-9.3 of BA's First Representations.

argued that the Commissioner had misapplied Article 25 GDPR because it was not in force at the time BA designed the relevant data processing systems and/or it should not be relied upon because it is merely duplicative in this context of the obligations applicable under Article 32 GDPR.

6.101. The Commissioner does not agree with BA's interpretation of Article 25 GDPR, which applies *"at the time of the processing itself"* as well as at the point at which the system is designed. The obligation applies on a continuing basis. However, the Commissioner has decided only to make findings of infringement in respect of Articles 5(1)(f) and 32 GDPR. This reflects the Commissioner's central conclusion that BA failed, as a data controller, to apply appropriate security measures meeting, in particular, the basic principles for processing applicable under Article 5 GDPR.

(2) The correct approach / standard

6.102. The Commissioner has considered BA's Representations on her provisional finding that BA breached Articles 5(1)(f) and 32 GDPR and her draft decision to that effect. In particular, BA submitted in both the First and Second Representations that: (a) factual findings were inaccurate; and/or (b) the Commissioner cannot maintain the conclusion that BA failed to take the available appropriate measures to remove or mitigate the risk of an attack of the kind which occurred in this case because she has applied the incorrect standard or approach.[81]

6.103. The Commissioner has clarified certain factual findings that were included in the NOI and/or in the draft decision in the light of: (a) new or additional information submitted by BA, in particular BA's new account of the likely route of the attack (via [redacted]); and/or (b) the submissions or information provided by BA.

6.104. The Commissioner has summarised above her position on the relevant standard, in response to the suggestion by BA that an incorrect or appropriate standard had been applied. For the reasons

[81] BA's First Representations, para 2 of the Executive Summary, and Chapter 2, in particular, paras 2.35-2.38. See also BA's Second Representations, paras 3.14-3.43.

given above, the Commissioner's view is that BA failed to put in place appropriate security arrangements as required by the GDPR.

6.105. As described above, there were a number of appropriate measure(s) available to BA that an organisation of its scale would be expected to take to secure its data operations. In the light of the range of measures identified above that were available to BA, and the nature of BA's processing operations, the Commissioner does not accept BA's argument that she has imposed an unduly high standard under Articles 5(1)(f) and/or 32 GDPR.[82]

6.106. The Commissioner also does not accept BA's suggestion that the airline industry should not be subjected to the same security standards as other industries.[83] The focus should be on whether a particular data controller has taken appropriate steps by reference to the data it is processing. BA failed to take such steps. For the avoidance of doubt, this does not mean, contrary to BA's submission,[84] that the Commissioner is suggesting that the only relevant factor to assessing whether measures are appropriate is the nature of the data to be processed. In carrying out its assessment of whether BA put in place appropriate measures, the Commissioner has had regard to all of the factors listed in Article 32(1) GDPR.

6.107. BA's arguments seek to highlight the apparent sophistication of the criminal attack on its systems.[85] However, sophisticated cyberattacks on global businesses are commonplace. The Attack in this case was not of such a degree of sophistication as to negate BA's responsibilities for securing its system and the personal data processed within it. Many of the steps taken by the Attacker were of a kind that could have been anticipated and addressed, as they were well-known means of attempting to exploit a system.

6.108. In addition to the above, had the principle of least privilege been applied, the sophistication of the Attacker would have been countered. If the files that contained employee credentials had been

[82] BA's First Representations, Chapter 2.
[83] This paragraph responds to a specific claim made by BA in its First Representations, paras 2.3-2.6 and, contrary to the suggestion in BA's Second Representations at para 3.18, does not seek to set out a comprehensive and general approach to the applicable standards.
[84] BA's Second Representations, paras 3.17-3.22.
[85] See, in particular, paras 2.7-2.17 of BA's First Representations.

appropriately secured, and had the tools that allowed the Attacker to perform reconnaissance been unavailable on the network, the Attacker would not have been able to take advantage of the techniques which BA describes as sophisticated.

6.109. The Commissioner's findings do not involve applying the benefit of hindsight in an improper manner. In identifying a range of potential appropriate measures that were available to BA, the Commissioner has found that there were clear weaknesses in BA's system that could have been identified and remedied. The failure to prevent, for example, third party users with access to BA's systems via single factor authentication from being able to access [redacted], was inadequate. Similarly, allowing access to hardcoded administrator passwords created clear and avoidable security risks. There was also an evident failure to put in place adequate monitoring and logging arrangements. The Commissioner does not accept that her approach to assessing the appropriateness and adequacy of BA's security measures is incorrect. Consequently, she does not accept BA's contention that its approach complied with the GDPR.

6.110. In its Second Representations, BA emphasises what it submits is the Commissioner's failure to put herself in BA's shoes and assess the situation as BA did at the time. BA also submits that the Commissioner erred by finding that the fact that each step of the Attack could have been mitigated or prevented because: *"... it is simply not known whether the sophistication of the Attackers was such that it would have enabled them to follow alternative attack vectors had any of the actions they took been prevented or mitigated..."*[86]

6.111. These submissions misunderstand the nature of the Commissioner's findings. The Commissioner does not find that simply because an attack took place BA was in breach of its obligations under the GDPR. Instead, the Attack which did occur exposed the fact that BA had failed to secure its systems in an appropriate manner. This is because looking at the steps of the Attack which occurred, it is clear that there were measures it would have been appropriate for BA to put in place which would have prevented them or mitigated their

[86] BA's Second Representations, paras 3.31-3.32.

impact. The fact that the Attacker may have needed to change course or use different means to attack BA's systems if further measures had been in place does not alter this conclusion.

(3) The totality of the security environment

6.112. The Commissioner has had regard to BA's detailed Representations on the security measures it had in place generally.[87] However, her investigation has identified numerous appropriate measures or steps that should have been taken by BA to address the identified security risks within its system. The Attack, and/or other attacks which could have occurred as a result of the deficiencies in BA's systems mean that, even looked at in the round, BA's technical and organisational data security arrangements, including risk assessment, cannot be regarded as sufficient or appropriate.

6.113. The Commissioner has also had regard to BA's Representations on the steps it took to prepare for the GDPR.[88] It is notable that none of those steps identified the deficiencies in BA's security which were exploited during the Attack, notwithstanding that these could have been easily addressed by BA.

7. REASONS FOR IMPOSING A PENALTY & CALCULATION OF THE APPROPRIATE AMOUNT

7.1. For the reasons set out above, the Commissioner's view is that BA has failed to comply with Articles 5(1)(f) and 32 GDPR. These failures fall within the scope of sections 149(2) and 155(1)(a) DPA. For the reasons explained below, the Commissioner considers it appropriate to impose a penalty in the light of the infringements she has identified.

7.2. In considering whether to impose a penalty, and in calculating the appropriate amount of the penalty, the Commissioner has had regard to the matters listed in Articles 83(1) and (2) GDPR and has applied the five-step approach set out in her RAP.

[87] BA's First Representations, paras 2.20-2.24.
[88] BA's First Representations, paras 1.1-1.4.

The imposition of a penalty is appropriate in this case

7.3. Both the RAP and Article 83 GDPR provide 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.

7.4. Article 83(2) GDPR lists a number of factors that must be taken into account. These are each discussed in detail below in determining the appropriate level of fine, in accordance with the steps outlined in the RAP. The points made below are also relied upon in justifying the Commissioner's decision to impose a penalty, in the light of the findings set out above.

7.5. The RAP provides guidance[89] on when the Commissioner will deem a penalty to be appropriate. In particular, the RAP explains that a penalty is more likely to be imposed where, *inter alia*, (a) a number of individuals have been affected; (b) there has been a degree of damage or harm (which may include distress and/or embarrassment); and (c) there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it).

7.6. As discussed in more detail below, each of those features is present in this case. Taking together the findings made above about the nature of the infringements, their likely impact, and the Commissioner's view that BA failed to comply with its GDPR obligations, the Commissioner considers it appropriate to apply an effective, dissuasive and proportionate penalty, reflecting the seriousness of the breaches which have occurred.

Calculation of the appropriate penalty

Step 1: an 'initial element' removing any financial gain from the breach[90]

7.7. BA did not gain any financial benefit, or avoid any losses, directly or indirectly as a result of the breach. The Commissioner has not, therefore, added an initial element under Step 1.

---

[89] See RAP, pages 24-25.

[90] Removing any financial gain the data controller may have obtained from the infringement is consistent with ensuring that the penalty is effective, proportionate and dissuasive (Article 83(1)), and has regard to Article 83(2)(k), which refers to *"financial benefits gained, or losses avoided, directly or indirectly, from the infringement."*

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

7.8. Sections 155(2)-(4) DPA refer to and reproduce the matters listed in Articles 83(1) and 83(2).

The nature, gravity and duration of the failure (Article 83(2)(a))

7.9. **Nature and gravity of the failures:** The Commissioner considers the nature of the failures to be of serious concern. BA was processing a significant amount of personal data in an insecure manner. As set out above, there were multiple measures that BA could have put in place that would have prevented, or mitigated, the Attack.

7.10. The failures are especially serious in circumstances where it is unclear whether or when BA itself would ever have detected the breach. BA was only alerted to the exfiltration of personal data from its website by a third-party. In the absence of that notification, the number of affected data subjects and any financial harm to them could have been even more significant. Furthermore, the extent of any harm appears to have been limited by the fact that the Attacker appears to have been financially motivated. The Attacker could have used the access for other purposes (such as targeting high-profile individuals, disrupting customer bookings, or perpetrating other forms of fraud).

7.11. A significant number of individuals (429,612 data subjects on BA's estimate) were affected by the breach.

7.12. Notwithstanding the assurances and mitigating steps taken by BA (which are taken into account below), the Commissioner remains of the view that it is likely that many of these individuals will, 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 Commissioner has considered the submissions made by BA in its Representations.[91] She notes the following points:

[91] BA's First Representations, paras 3.11-3.14, and 3.23; BA's Second Representations, paras 4.3 *et seq.*

a. It is not correct that the payment card details are the only data which could arguably have *any* degree of sensitivity. Attackers may exploit combinations of names, usernames and passwords to exploit data subjects.

b. BA's assertions as to the most likely reaction of data subjects to learning that their payment card data or other personal information has been affected do not reflect the Commissioner's experience. It is not, in the Commissioner's experience, *"inherently unlikely"*[92] that consumers will be distressed by learning their payment card data or other personal information has been compromised. Moreover, the fact that consumers can learn how their data may be protected by third parties, such as their credit card issuer, does not remove the likelihood that they suffer distress in the interim while they establish the risks they face and how they might take steps to mitigate these risks. It is unrealistic for BA to suggest that there would not have been such an *"interim"* period between becoming aware of the breach and establishing its impact upon them.[93] It would necessarily take time for individuals to assess the actual risk of harm they face.[94] The fact that BA committed to reimburse financial losses in communicating the breach would not prevent an individual being distressed or concerned about the potential for such loss to occur in the first place.[95] Equally, the fact that one card company indicated that its customers did not need to take action does not mean that relevant customers would have had no concern about the implications of the Attack.[96]

c. The Commissioner does not accept that payment card breaches, at least of the type involved here, are *"an entirely commonplace phenomenon"* and therefore an *"unavoidable fact of life"*, as BA claims.[97] These statements trivialise what was a serious failure on BA's part. The fact that data subjects were able to book flights online does not mean they are so *"tech savvy"* that they would be unaffected by being told that BA has lost control of their personal data as a result of its security

[92] BA's First Representations, para 3.11.
[93] BA's Second Representations, para 4.3(c).
[94] BA's Second Representations, para 4.3(c).
[95] BA's Second Representations, paras 4.3(c)-4.3(d).
[96] Contrary to para 4.3(e) of BA's Second Representations.
[97] BA's First Representations, para 3.11.

failings. The Commissioner does not comment on BA's assertions that *"claimant law firms will, for entirely self-serving purposes, use the word "distress" very liberally, essentially with the aim of garnering thousands of potential claimants on no-win-no-fee agreement…"*[98] The Commissioner applies that term in accordance with the legislation, when the circumstances under consideration warrant it.

d. As set out below, over 40,000 data subjects took up BA's offer of free credit monitoring, demonstrating that they were at least sufficiently concerned about the breach to take that precautionary step.

e. BA's suggestion that the infringements found in this case are not serious because hundreds of thousands of data subjects were affected, rather than millions of data subjects as in other breaches to which it refers, is not accepted.[99] Given the totality of the facts and circumstances set out above, the Commissioner remains of the view that the infringements in this case are significant, and affected a substantial number of data subjects. For the reasons set out further below, BA's reliance on penalties imposed under the superseded Data Protection Act 1998 ("**DPA 1998"**) regime is misplaced.

f. The Commissioner accepts the point in BA's Second Representations[100] that there was a category of individuals whose CVV numbers were not compromised and that it is possible that for these individuals the risk of incurring any financial damage would be reduced compared to the category of individuals whose CVV numbers were compromised. However, the risk was not removed for such individuals. By way of example, some retailers (such as Amazon) accept card payment without CVV numbers. In any event, individuals are likely to have been distressed by the fact that their personal data had been used unlawfully.

7.13. **Duration:** In the NOI and draft decision, the Commissioner found that the infringement in issue lasted from 25 May 2018 (when the

[98] BA's First Representations, para 3.11.
[99] BA's First Representations, para 3.23.
[100] BA's Second Representations, para 4.8(b).

GDPR came into force and ended on 16 November 2018. The Commissioner remains of the view that it was reasonable to treat 16 November 2018 as the appropriate end date.

7.14. As BA notes in its Second Representations, the Commissioner's Lead Technical Investigation Officer asked BA in his letter of 18 February 2019 to indicate the date on which: *"the final technical measure was put in place as a result of this incident, i.e. the latest date that technical vulnerabilities brought to light as a result of this attack were fixed".* BA responded confirming that the relevant date was 16 November 2018, when its endpoint monitoring tool 'Crowdstrike Falcon' was fully deployed. Given the importance of endpoint monitoring as an appropriate measure that ought to have been in place, the date of 16 November 2018 was deemed appropriate as an end date.

7.15. However, the Commissioner has considered BA's submissions[101] and decided that the infringement in issue should be regarded as continuing until 5 September 2018.

7.16. Thus, for the purposes of deciding whether to impose a penalty, and for calculating the appropriate amount, the Commissioner proceeds on the basis that the infringements under the GDPR commenced on 25 May 2018, when the GDPR entered into force, and ended on 5 September 2018, when personal data ceased to be transferred to BAways.com. This is a significant period of time (103 days) during which unauthorised access to, and in some cases subsequent exfiltration of, personal data went undetected by BA.

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

7.17. The Commissioner has had regard to the guidelines provided by the Article 29 Working Party in relation to assessing the character of the infringement in issue. It explains that:

> *… 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*

[101] BA's First Representations, paras 3.15-3.19; and BA's Second Representations, paras 3.10-3.11, and 4.2.

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…[102]

7.18. The Commissioner recognises that the infringement was not an intentional or deliberate act on the part of BA.

7.19. The Commissioner has, however, found that BA was negligent (within the meaning of Article 83(2)(b) GDPR) in maintaining operating systems which suffered from the significant vulnerabilities and shortcomings identified in sections 3 and 6 above.

7.20. In making this determination, the Commissioner places some weight on the relevant context: a company of the size and profile of BA is expected to be aware that it is likely to be targeted by attackers, sophisticated or otherwise. BA must be aware that the nature of its business involves processing large volumes of personal data, including sensitive personal data. The risk of any compromise of that information may have significant consequences for BA's customers and its own business. In view of these factors, the Commissioner would expect BA to have taken appropriate steps or a combination of appropriate steps to secure the personal data of its customers; and considers that BA was negligent (within the meaning of Article 83(2)(b)) in failing to do so.

7.21. BA relies upon its "*extensive commitment to information security*" in its First and Second Representations.[103] The Commissioner accepts that BA has been able to demonstrate commitment to certain aspects of information security, however in relation to the specific shortcomings identified in this Penalty Notice which were exploited by the Attackers, BA was negligent (under Article 83(2)(b)) in failing to ensure that it had taken <u>all</u> appropriate measures to secure personal data.

---

[102] Pp.11-12.
[103] BA's First Representations, para 2.22; and BA's Second Representations, para 4.8.

7.22. The Commissioner acknowledges that the Attack was carried out by criminal third parties. However, the Commissioner rejects the suggestion that it is the Attackers who are primarily responsible for the breaches of the GDPR identified in this Penalty Notice. The breaches identified relate to BA's failures to comply with its obligations to put in place appropriate security measures.[104] These failures were exposed by the Attack. This penalty decision does not proceed on the basis that the fact of an attack justifies imposing a penalty.

7.23. While this penalty decision only takes into account failures under the GDPR during the period between 25 May 2018 and 5 September 2018, it is clear that the deficiencies in BA's systems were present for some time. The advent of the GDPR should have prompted a careful review of BA's systems and security arrangements. This, contrary to BA's suggestion in its Second Representations,[105] was evidently appreciated by BA. The Commissioner has noted that BA put in place a programme to prepare its systems for the introduction of the GDPR. However, that programme failed to identify and address the deficiencies in BA's security that were highlighted by the Attack. The Commissioner does not accept BA's argument that it did not act negligently or otherwise in breach of Articles 5(1)(f) and 32 GDPR.[106]

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

7.24. The Commissioner has carefully considered BA's submissions to the effect that Steps 1 and 5 of the RAP are duplicative, such that BA could not discern how the mitigation action it took in response to the Attack has been taken into account.[107]

7.25. The Commissioner remains of the view that it makes no difference to the ultimate decision on what, if any, penalty to impose whether the action taken by the controller to mitigate the damage is taken into account here, or under Step 5. However, she has decided to consider this issue separately under Step 5 in this Penalty Notice.

---

[104] BA's First Representations, paras 3.28-3.29; and BA's Second Representations, para 4.10.
[105] BA's Second Representations, para 4.8.
[106] BA's First Representations, para 3.29.
[107] BA's Second Representations, paras 5.42-5.44.

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

7.26. As a controller, BA is responsible under the GDPR for the security of its systems and the protection of personal data stored within those systems. It is required by the GDPR to implement security measures to reduce the vulnerability of those systems, and the vulnerability of the personal data processed within those systems, to attack. Although the initial access was gained to BA's systems through the Citrix remote access port, which was used to permit third party access to [redacted], it is clear that there were numerous deficiencies in BA's security measures and network which the Attack exposed.

7.27. The Attacker was able to exploit the deficiencies in BA's security, ultimately gaining access to personal data that should not have been accessible using the third-party remote access system. The significant inadequacies or deficiencies which the Commissioner has identified relate to the way in which BA operated its network. They were not caused by inadequacies in third-party systems or a problem with applications such as Citrix.

7.28. The Commissioner therefore considers that BA is wholly responsible for the breaches of Articles 5(1)(f) and 32 GDPR described above.

7.29. Contrary to BA's Representations, the Commissioner does not treat BA as exclusively responsible for the Attack.[108] Nor has she dismissed the role of the Attacker as being irrelevant.[109] The Commissioner appreciates that the Attacker engaged in criminal activity. She is also conscious that the Attacker gained access as a result of compromised access granted to a Swissport employee. BA did not intend anyone at Swissport to have access to the personal data processed by BA. These points do not, however, alter BA's obligations to have in place appropriate security measures. In fact, it is the possibility of such attacks by third parties that necessitate compliance with the obligations imposed by Articles 5(1)(f) and 32 GDPR. While BA submitted in its Representations that the access granted to Swissport was to a *"carefully curated set of BA applications"*,[110] that does not appear to reflect what happened in

[108] BA's First Representations, paras 3.39-3.45.
[109] BA's Second Representations, paras 4.10-4.11.
[110] BA's First Representations, para 3.41.

practice. As described above, once onto the BA system the Attacker was able to [redacted] and thereafter move through BA's network, because of inadequacies in BA's security measures. It is these inadequacies for which BA is accountable.

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

7.30. BA has no relevant previous infringements or failures to comply with past notices.

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

7.31. The Commissioner considers that BA has cooperated fully with her investigation and has taken that into account.

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

7.32. In the initial stages of the Attack, the data categories affected were: (a) username and passwords of contractors and employees; and (b) username and passwords of members of the Executive club. Once the malicious script was added, the categories affected were: (a) customer names and addresses; (b) unencrypted payment card data including card numbers; and (c) CVV numbers and expiry dates. The Commissioner considers the loss of control by BA of personal data such as names, addresses and unencrypted payment card data to be particularly serious, allowing as they do the opportunity for identity theft.

7.33. As noted above, while no "special category data" was affected, this does not mean that the data was not sensitive. CVV numbers were taken for 77,000 of the 185,000 customers who had their payment card data compromised. This meant that 77,000 customers had sensitive financial data taken, which put them at a heightened risk. The Commissioner does not agree with BA's submission that she has *"severely overstated"* the sensitivity of the data affected by the Attack or that she is treating the compromise of this sensitive data as *"commensurate with a breach of special category data"*.[111]

[111] See BA's First Representations, para 3.46 and BA's Second Representations, paras 4.4-4.6.

7.34. The Commissioner relies upon the ENISA Guidance entitled "*A methodology of the assessment of the severity of personal data breaches*"[112], which provides a scoring method to assess the severity of a personal data breach. Whilst financial data is given a score of 3 (out of a maximum of 4), the presence of an aggravating factor can elevate financial data to a score of 4. Aggravating factors identified in the ENISA Guidance, and which were present in this case, include where full financial information is disclosed and where there is a high volume of data disclosed. Therefore, the Commissioner is entitled to regard the disclosure of financial data in this case as a cause for significant concern.

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

7.35. BA acted promptly in notifying the Commissioner of the Attack and thereby complied with its obligations in this respect.

Conclusion at Step 2

7.36. Taking into account: (a) the matters set out in Sections 2-4 and 6 above; (b) the matters referred to in this section; and (c) the need to apply an effective, proportionate and dissuasive fine in the context of a controller of BA's scale and turnover, the Commissioner has determined that, in principle, a penalty of £30m would be appropriate, before adjustment in accordance with Steps 3-5 below and the application of the Commissioner's Covid-19 policy. This amount is considered appropriate to reflect the seriousness of the breach and takes into account the need for the penalty to be effective, proportionate and dissuasive.

Step 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k))

7.37. The amount of the penalty, as identified at Step 2, may be increased where there are 'other' aggravating factors.[113] In this case, the Commissioner does not consider there to be any other relevant aggravating factors. The Commissioner has not, therefore, adjusted the penalty level determined at Step 2.

---

[112] Dated 20 December 2013.
[113] In accordance with article 83(2)(k) GDPR and section 155(3)(k) DPA and page 11 of the RAP.

Step 4: Adding in an amount for deterrent effect to others

7.38. The Commissioner is under an obligation to impose a penalty which is *"dissuasive"*. The need for the penalty to be dissuasive in relation to BA itself is addressed by the analysis at Step 2. Having regard to the amount of the penalty identified under Step 2, the Commissioner does not consider it necessary to increase the penalty further under Step 4 to dissuade others.[114]

7.39. The Commissioner is not aware of widespread issues of poor practice that may be particularly deterred by the imposition of a higher penalty. Given BA'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 considers that no adjustment is necessary under Step 4.

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))

7.40. As explained above, in principle, other relevant mitigating factors could be taken into account under Step 2 or Step 5 of the RAP. Previously the Commissioner considered such matters in the round under Step 2 of the RAP, taking into account the factors in Article 83 GDPR and section 155(3)DPA 2018. However, in light of BA's representations, for the purposes of this Penalty Notice the Commissioner has considered relevant mitigating factors under Step 5.

7.41. Following the guidance set out at page 11 of the RAP, and having considered BA's representations, the Commissioner considers it appropriate to take into account the following mitigating factors:

[114] This makes, in particular, the points made by BA at para 6.26 of its Representations irrelevant. However, it is noted that the Commissioner does not accept that she should take into account in determining whether a fine should be increased to secure a deterrent effect that a controller may have suffered reputational damage / exposure to civil claims as a result of its infringement of the GDPR. Moreover, the Commissioner does not accept that as a matter of general principle concerns about deterrent effect should be limited to deliberate breaches. It is also important to deter data controllers from acting negligently.

a. BA took immediate measures to mitigate and minimise any damage suffered by the data subjects by implementing remedial measures;

b. BA promptly informed the affected data subjects, other law enforcement and regulatory agencies, and the Commissioner, and fully cooperated with the Commissioner's enquiries thereafter;

c. Widespread reporting in the media of the Attack is likely to have increased the awareness of other data controllers of the risks posed by cyber attacks and of the need to ensure that they take all appropriate measures to secure personal data;

d. The Attack and subsequent regulatory action has adversely affected BA's brand and reputation, which will have had some dissuasive effect on BA and other data controllers.

7.42. The Commissioner has taken into account the fact that, 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.[115] In particular, the Commissioner has considered the information provided by BA about the action it took in paras 3.30-3.38 of its Representations. These included, *inter alia*, issuing a press release to 5,000 journalists and commentators, and being active on television, social media and in the press about the Attack.

7.43. It is also noted that BA notified the FCA, and that BA informed and co-operated with the following other regulatory and governmental bodies in the aftermath of the Attack: the UK Police, the Civil Aviation Authority, HMRC, Department of Transport, the National Crime Agency, and the National Cyber Security Centre. BA also notified other data protection regulators outside the EEA, and 21 State Attorneys General in the USA.[116]

7.44. The Commissioner has also taken into account the fact that BA offered to reimburse all customers who had suffered financial losses as a direct result of the theft of their card details. The offer was

[115] Referred to, in particular, in para 3.35 of BA's First Representations.
[116] BA's First Representations, para 3.47(c).

made on 7 September 2018 and is maintained on BA's website. BA also made free credit monitoring available.[117]

7.45. The Commissioner acknowledges that the steps above will have gone some way to reassuring BA's customers, and therefore may have reduced or mitigated any likely distress that may otherwise have been caused by the breach. The Commissioner does not accept, however, BA's suggestion that the action taken to mitigate the impact of the Attack would have immediately addressed all concerns on the part of data subjects about their data being in the hands of criminals and/or otherwise outside of BA's control.[118] It is not the Commissioner's role to investigate and establish the extent of any damage that may have been caused to any particular data subject.

7.46. The Commissioner notes that BA has also implemented a number of remedial technical measures so as to reduce the risk of a similar Attack in future, and has indicated that expenditure on IT security will not be reduced as a result of the impact of Covid-19. The remedial measures include, in particular:

a. [redacted]

b. [redacted]

c. [redacted]

d. [redacted]

7.47. Having regard to the mitigating factors set out above, it is appropriate to reduce the proposed £30m penalty by 20%, i.e. to £24m.

[117] Referred to at paras 3.34 and 3.36 of BA's First Representations.
[118] Contrary to paras 3.37-3.38 of BA's First Representations.
[119] BA's First Representations, paras 3.47-3.48.

7.48. As a result of the Covid-19 pandemic, BA has argued that any penalty should be significantly reduced, or not imposed at all because of the financial hardship it would cause.

7.49. The Commissioner has carefully considered BA's Third Representations and oral representations, and the evidence that BA has provided. Although the Covid-19 pandemic has had a significant short to medium term impact on BA's revenues and its immediate financial position, the Commissioner considers that the overall financial position of BA and its parent company IAG is such that the imposition of a penalty in the range being considered will not cause financial hardship.

7.50. The Commissioner has published guidance entitled *"The ICO's regulatory approach during the Coronavirus public health emergency"*.[120] That guidance indicates that *"As set out in the Regulatory Action Policy, before issuing fines we take into account the economic impact and affordability. In current circumstances, this is likely to mean the level of fines reduces."* While the proposed penalty will not cause financial hardship for BA, the Commissioner considers it appropriate to reduce the penalty that would otherwise have been imposed, in light of the current public health emergency and associated economic consequences. This is addressed further below, separately from Step 5.

7.51. The Commissioner has carefully considered BA's submissions that there are other additional mitigating factors that should be taken into account in this case.[121] However, none of the points raised justify a further reduction of the appropriate penalty beyond the discounts set out above. In particular:

a. The Commissioner has recognised that the Attack involved persistent criminal activity. But this does not alter the fact that the security of BA's network was inadequate in a number of respects, and that those failings could and should have been addressed on a prospective basis through the implementation of appropriate measures. It is BA's breaches of Articles 5(1)(f)

[120] Version 2.1, 13 July 2020.
[121] BA's First Representations, para 3.47.

and 32 GDPR that are being penalised, not the actions of third parties.

b. The Commissioner does not accept BA's assertion that no harm or damage was caused by the failings identified in this decision. It is not the Commissioner's role to investigate and establish the extent of any damage that may have been caused to any particular data subject. To the extent that BA relies on the steps it took to mitigate the impact of the Attack on data subjects, those have been taken into account.

c. To the extent that BA relies on other factors such as the steps it took to publicise the attack, inform relevant authorities, and the steps it has now taken to mitigate the threat of a repeat attack, those have all been taken into account in calculating the penalty and any discount.

d. The Commissioner does not consider it appropriate to reduce the penalty by reference to the costs to BA of taking measures to rectify or mitigate the impact of its infringement, including the cost to BA of appointing external forensic consultants or legal advisers.[122] The fact that BA may have suffered financial losses as a result of the Attack, such as the cost of providing credit monitoring for customers or appointing external advisers, is not directly relevant to the amount of any penalty. The fact that mitigating measures were taken, in accordance with BA's obligations as a controller, has already been taken into account in calculating the overall level of penalty including any discount, and in considering whether a penalty is proportionate.

e. BA's preparations for the introduction of the GDPR are noted.[123] However, these do not undermine the Commissioner's conclusions on BA's failure to implement appropriate security measures.

7.52. Accordingly, having carefully considered the mitigating factors raised by BA, which are relevant to the assessment of the appropriate level of any penalty, the penalty payable by BA would

[122] See BA's First Representations, para 3.49.
[123] As relied upon at para 3.50 of BA's First Representations.

be £24 million, subject to the application of the Covid-19 policy as set out below.

Application of the Covid-19 Policy

7.53. As described above, having regard to the impact of the Covid-19 pandemic (on BA and more generally), and consistently with the Commissioner's published guidance, a further reduction of £4m is appropriate and proportionate. The final penalty payable by BA will therefore be £20 million.

Application of the fining tier(s) (Articles 84(4) and (f) GDPR)

7.54. The infringement of Article 5(1)(f) GDPR falls within Article 83(5)(a) GDPR, whereas Article 32 falls within Article 83(4)(a). The appropriate tier is therefore that imposed by Article 83(a) as this is the gravest breach in issue in this case.

7.55. In any event, for the year ended 31 December 2017 BA has confirmed that its worldwide annual turnover was £12,226,000,000 (£12.26bn). The penalty the Commissioner has decided to impose on BA is the sum of £20 million. This is considerably less than 4%, indeed considerably less than 1%, of BA's total worldwide annual turnover, and accordingly well within the cap imposed by Article 83(5) GDPR.

BA's other representations on the decision to impose a penalty and the appropriate amount Penalty amount

7.56. BA submitted detailed representations in response to: (a) the Commissioner's decision to impose a penalty at all; and (b) the proposed penalty amount, as indicated in the NOI and the draft decision. The Commissioner has carefully considered those representations and, to the extent they have not already been addressed above, responds to them below.

7.57. In summary, BA submitted as follows:

a. **First,** the Commissioner misapplied Article 83(2) in deciding to impose a fine and in determining the appropriate level of penalty. A proper application of that Article should result in no

fine being imposed or, in the alternative, should result in only a low penalty.[124]

b. **Second,** the Commissioner: (i) unlawfully applied an unpublished internal document, entitled "*Draft Internal Procedure for Setting and Issuing Monetary Penalties*", in setting the proposed penalty on BA included in the NOI;[125] and (ii) calculated the revised penalty in the draft decision in a manner which was tainted by the original proposed penalty in the NOI;[126]

c. **Third**, a turnover-based approach, as adopted by the Commissioner in calculating the proposed penalty on BA included in the Notice, has no statutory basis, and is a fundamentally flawed way of achieving penalties which are effective and proportionate. The Commissioner is wrong to treat turnover as the *"core quantification metric"*;[127]

d. **Fourth**, the Commissioner has applied the wrong fining Tier under Article 83 GDPR in calculating the proposed fine;[128]

e. **Fifth,** the Commissioner has acted contrary to the RAP because a proper application of that policy and/or compliance with its 'spirit' would not have resulted in a fine being issued at all, or, alternatively, would have resulted in a much lower fine.[129] In particular, BA contends that the breach in this case:

   i. cannot be considered to be a *"most severe breach"*, necessitating the imposition of a penalty, because its actions were not wilful or deliberate, the incident did not involve repeat breaches, harm to individuals, no special

[124] BA's First Representations, Chapter 2; and BA's Second Representations, paras 1.3.2, and 4.14-4.17.
[125] BA's First Representations, para 6 of the Executive Summary, and paras 4.1-4.12; and BA's Second Representations, paras 2.2-2.8.
[126] BA's Second Representations, paras 1.1, 1.3.3, 1.4, 2.7, 5.2-5.7.
[127] BA's First Representations, para 7 of the Executive Summary, and paras 5.1-5.7; and BA's Second Representations, paras 1.3.3, 5.8-5.15.
[128] BA's First Representations, para 8 of the Executive Summary, and paras 5.8-5.13; and BA's Second Representations, paras 1.3.3, 5.16-5,21.
[129] BA's First Representations, paras 9-10 of the Executive Summary, and paras 6.1-6.12, with specific representations on the application of the five-step procedure at paras 6.13-6.28 of BA's Representations. See also BA's Second Representations, paras 5.22-5.24.

category data was affected, and BA did not make financial gains as a result of the breach;[130] and

ii. applying the guidance in the RAP, the criteria justifying the imposition of a higher or very significant penalty do not arise in this case;[131]

f. **Sixth**, the Commissioner's penalty regime lacks legal certainty or any *"rational basis"*.[132] As a result, the Commissioner should continue to take the approach to fining under GDPR that she took in past decisions issued under the DPA 1998.[133] Alternatively, she should impose a fine of a level equivalent to that imposed by other European authorities under GDPR and/or impose a fine which is consistent with other decisions she has issued under the GDPR;[134]

g. **Seventh**, the amount of the fine is not "effective" because issuing large fines is likely to be counterproductive;[135]

h. **Eighth,** the Commissioner has failed to comply with BA's rights because: (i) the NOI failed to provide BA with adequate and clear reasoning such that a decision to proceed to impose a penalty would be unlawful because it would be contrary to BA's rights of defence[136]; and (ii) her conduct post the issuance of the NOI undermined due process and therefore BA's right of defence;[137]

i. **Ninth,** the Commissioner ought to have convened the Panel of Technical Advisers;[138]

j. **Tenth**, in agreeing to the extension proposed by the Commissioner, BA was not given a genuine choice;[139]

---

[130] BA's First Representations, paras 6.5-6.6.
[131] BA's First Representations, paras 6.11-6.12.
[132] BA's First Representations, Executive Summary, para 11, and paras 7.1-7.23; and BA's Second Representations, paras 1.2, 1.3.3, 5.1-5.4, 5.32-5.53.
[133] BA's First Representations, Executive Summary, paras 11-12, and paras 8.1-8.24; and BA's Second Representations, paras 5.54-5.60.
[134] BA's First Representations, paras 8.16-8.24; and BA's Second Representations, para 1.3.3.
[135] BA's First Representations, paras 10.1-10.5.
[136] BA's First Representations, Executive Summary paras 13-14, and Chapter 11.
[137] BA's First Representations, Chapter 12; and BA's Second Representations, paras 1.4, 2.2, 2.9-2.30.
[138] BA's Second Representations, paras 2.13-2.16.
[139] BA's Second Representations, paras 2.2, 2.17-2.30.

k. **Eleventh,** the Commissioner has failed to comply with its statutory obligations to: (a) act in a manner which is transparent, accountable, proportionate and consistent; and (b) take into account the desirability of promoting economic growth in ensuring its actions are proportionate.[140]

(1) Application of Article 83(2)

7.58. The Commissioner has described above how the factors listed in Article 83(2) apply to the facts of this case. In its First Representations, BA criticised the Commissioner's provisional findings in the NOI. It then advanced further criticisms in its Second Representations of the Commissioner's application of Article 83(2) as set out in the draft decision. Where necessary, BA's criticisms have been addressed under each step of the analysis set out above.

7.59. BA submits that any penalty regime engages the fundamental rights of controllers, including their fundamental right to property as provided for under Article 1 of Protocol 1 of the European Convention on Human rights, and Article 17 of the EU Charter of Fundamental Rights. The Commissioner recognises that in imposing a penalty on a controller, she must comply with relevant fundamental rights that are engaged, including under the ECHR or the EU Charter. However, it is not accepted that a penalty should only be imposed in the narrow circumstances identified by BA. Whether or not a penalty is appropriate and proportionate is a matter of judgment for the Commissioner applying, in particular, the considerations set out in Article 83 GDPR.

(2) Draft Internal Procedure

7.60. Prior to issuing the NOI in this case, the Commissioner had developed a Draft Internal Procedure for calculating proposed penalties, as a supplement to the RAP. Its purpose was to provide a guide, by reference to the turnover of the controller, as to the appropriate penalty. As the GDPR is a new regime, this additional tool was intended to assist the decision-makers in applying Article 83 GDPR and the RAP.

[140] BA's Second Representations, para 1.3.4, and Section 6.

7.61. BA submitted detailed representations on this issue.[141] The Commissioner has considered those representations in deciding how to approach the calculation of the penalty to be imposed in this Penalty Notice.

7.62. The Commissioner remains of the view that the controller's turnover is a relevant consideration in determining the appropriate level of penalty, and this is addressed further below. However, before issuing the draft decision to BA, the Commissioner agreed that the Draft Internal Procedure should not be used in the present case. Therefore, in deciding the appropriate penalty in this case no reference has been made to the Draft Internal Procedure. The Commissioner has instead relied on Article 83 GDPR, section 155 DPA and the RAP. The approach taken to the calculation of the penalty for the purposes of this Penalty Notice is set out above.

7.63. Notwithstanding the fact that the Commissioner had decided no longer to rely upon the Draft Internal Procedure, BA stated in its Second Representations that the Commissioner's approach is nevertheless "*tainted*" by reliance upon the Draft Internal Procedure, "*given the repeated references in the DPN to the initial figure of £183 million*".[142] The Commissioner does not accept this.

7.64. This Penalty Notice, and its earlier iteration refer (or allude) to the figure of £183 million on four occasions.[143] One reference forms part of the factual background, and the others are by reference to the fact that the proposed penalty has been reduced taking into account BA's First and Second representations. That the proposed penalty is less than the initial proposed penalty as a result of BA's Representations is simply a fact, and not an indication that the penalty calculation exercise took the initial figure as a starting point.[144] The process by which the Commissioner calculated the proposed penalty is set out above. The level of penalty that the Commissioner proposed to set in the past is not treated as the starting point for that consideration or factored into it.

7.65. BA submitted in its Second Representations that it is incumbent on the Commissioner to explain whether the she has any intention of

[141] See paras 4.1-4.12 of BA's First Representations in particular.
[142] BA's Second Representations, paras 2.7, and 5.5-5.7.
[143] Draft Penalty Notice, dated 23 December 2019, paras 5.2, 7.32, 7.43, 7.68(d).
[144] BA's Second Representations, paras 5.2, 5.5-5.7 and 5.36-5.37.

retaining the principles behind the Draft Internal Procedure going forward.[145] The Commissioner has made plain in the draft decision and this Penalty Notice that turnover remains a relevant factor in assessing whether a penalty should be imposed and, if so, at what level. The Commissioner has also made plain however that the Draft Internal Procedure has not been taken into account in setting the level of penalty proposed in the draft decision or in this Penalty Notice.

7.66. Further, the Commissioner does not accept that the use of the Draft Internal Procedure has in any way delayed her investigation.[146] BA, in its First Representations in particular, provided a large volume of additional factual and technical information which the Commissioner was obliged to take into account when calculating the revised proposed penalty. That calculation exercise would have been re-visited in the light of BA's extensive representations in any event. This process of consultation is part of ensuring the procedural fairness of the Commissioner's decision-making.

(3) The Use of a Turnover-Based Approach

7.67. BA makes two submissions at paras 5.1-5.7 of its First Representations in respect of the Commissioner having adopted a turnover-based approach.

7.68. The first submission is that the Commissioner should not have relied on turnover-based 'bands' defined in the Draft Internal Procedure in calculating the proposed penalty. As set out above, the Commissioner has not applied the Draft Internal Procedure in making her final decision on the appropriate penalty in this case.

7.69. The second submission is that the Commissioner is not entitled to use turnover-based approach at all because such an approach is inconsistent with the requirement that fines be effective, proportionate and dissuasive, and conform to the GDPR's aim of consistent and homogenous application of the rules.

[145] BA's Second Representations, para 2.5.
[146] BA's Second Representations, para 2.7.

7.70. In its Second Representations, BA maintains that the Commissioner continued to err in her draft decision by relying on turnover as a "*core quantification metric*".[147]

7.71. In the circumstances of this case, turnover is one of several core quantification metrics for the following reasons:

a. A turnover-based approach is consistent with the approach taken to penalties in GDPR. The Data Protection Directive did not prescribe the level of fines that Member State authorities should impose for data breaches. The GDPR departs from that approach. In doing so, it expresses the maximum penalty in terms of a percentage of turnover. Turnover is therefore a relevant factor in determining the appropriate level of penalty to be imposed. This is also reflected in the Recitals, which make clear that the economic position of the controller is relevant even where the controller is a private person and not an undertaking: *"… Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine."*

b. Further, and in any event, the Commissioner is obliged to ensure that any penalties imposed are "*effective, proportionate and dissuasive*". Having regard to a data controller's turnover complies with this principle by ensuring that the level of any penalty is not only proportionate but is also likely to be an effective and dissuasive deterrent for the undertaking on which it is imposed, and other equivalent controllers. It is self-evident that imposing the same penalty on an undertaking with a turnover of billions of pounds as would be imposed on a small or medium sized business would not be effective, proportionate or dissuasive. Comparable regulatory regimes that share the GDPR's emphasis on deterrence, such as under competition law, also take turnover into account in setting penalties.

7.72. The Commissioner does not, therefore, accept BA's contention that relying on turnover as a metric in calculating the appropriate penalty

[147] BA's Second Representations, paras 5.8-5.15.

is "*entirely arbitrary*" because "*it bears no meaningful relationship to the wrong in issue*"[148], nor is it the case that such an approach will necessarily result in disproportionate fines[149]. Turnover is a relevant metric for assessing whether any fine is proportionate and dissuasive.

7.73. Consequently, in calculating the penalty in this case, the Commissioner has taken into account a number of core metrics for quantification, including turnover. Turnover is one key factor to be taken into account in the round, by reference to the particular facts at issue in the case.

7.74. However, it is noted that BA's primary criticism in its First Representations relates to the use of turnover bands as the starting point of the penalty calculation, and this has been addressed by the Commissioner's decision not to rely on the Draft Internal Procedure. At para 5.4 of its First Representations and paras 5.10-5.12 of BA's Second Representations, BA accepted that the overall financial position of an organisation may be a factor to be considered when deciding whether a fine is effective and proportionate, and/or to avoid undue hardship. BA instead emphasises that the person's financial position should be treated only as one consideration amongst others.

7.75. The Commissioner agrees that a person's financial position is a relevant factor, though not the sole factor, in determining the overall penalty. She is obliged to consider, and does consider, *inter alia*, the scale and severity of the breach and its effect on data subjects, as part of the analysis to ensure that any penalty is proportionate. However, for the reasons explained above, when considering whether a penalty is dissuasive and effective, it is also necessary for the Commissioner to consider the scale and turnover of the controller, reflecting the undertaking's overall financial position. The appropriate penalty has to be assessed by the Commissioner in the round, applying her five-step process. She is not obliged, as BA suggests breakdown her overall assessment of the relevant penalty to distinguish between the level of fine which reflects the

[148] BA's First Representations, para 5.2(a).
[149] BA's First Representations, para 5.2(c).

'infringement' and the level which reflects the controller's turnover (or 'success').[150]

7.76. Ultimately, the Commissioner must – before imposing a penalty – consider all relevant factors, and ensure that the penalty is effective, proportionate and dissuasive. Taking into account an undertaking's financial position as an element of that consideration is necessary and does not result in arbitrary outcomes.

(4) The Appropriate Tier

7.77. In response to the NOI, BA stated that the Commissioner had applied the wrong fining tier by incorrectly categorising the breaches as a "Tier 2 infringement", allowing for a maximum fine of 4% of turnover.[151] Further representations to this effect were made in BA's Second Representations.[152] BA's position was based, in summary, on the following points:

a. There is a clear conflict in the GDPR regarding the maximum administrative fines for breaches of Articles 5(1)(f) and 32 as these impose the same core obligations but attract different maximum fines. The NOI does not distinguish between the obligations imposed by these Articles.

b. Article 83(3) is of no assistance to the Commissioner because it only explains how the Commissioner may proceed where the same or linked processing operations infringe several "*distinct provisions*", i.e. where there is no overlap between the obligations imposed by the relevant GDPR provisions.[153]

c. The maximum fine should be 2% because:

i. the wording of Article 83(4) makes clear that the intention was to impose this lower maximum for breaches of Article 32. It is said that Article 83(2) makes a more explicit reference to Article 32, by referring to *"Articles… 25 to 39"*, than Article 83(5)(a) does in referring to the *"basic principles of processing… pursuant to Articles 5…"* Article

[150] Contrary to BA's Second Representations, para 5.14.
[151] BA's First Representations, paras 5.8-5.13.
[152] BA's Second Representations, paras 5.16-5.21.
[153] BA's Second Representations, para 5.17.

5(1)(f) is not referred to explicitly, or as part of a continuum of sub-provisions;

ii. Article 32 GDPR amounts to the *lex specialis* of Article 5(1)(f); and

iii. as Article 5(1)(f) applies only to controllers, whereas Article 32 also applies to processors, the Commissioner's approach leads to different fining regimes in respect of an identical obligation.

7.78. The Commissioner does not accept these submissions, for the following reasons.

7.79. The principle of *lex specialis* means that "*where a legal issue falls within the ambit of a provision framed in general terms, but is also specifically addressed by another provision, the specific provision overrides the more general one.*"[154] The Commissioner does not accept that the application of the *lex specialis* principle precludes the Commissioner from treating this case as a Tier 2 infringement.

7.80. Article 5(1)(f) and Article 32 are evidently distinct provisions of the GDPR, *notwithstanding* the degree of overlap. Article 32 applies to processors, whilst Article 5 does not. Contrary to BA's submission, there is no conflict between these provisions. They can be applied to controllers at the same time: Article 32 does not override the basic requirements laid down in Article 5(1)(f), read with Article 5(2), which establish the responsibility of the controller for demonstrating compliance with the security obligation and any breach of that principle.

7.81. Further, and in any event, the provisions in Article 83(4) and Article 83(5) are distinct provisions which make explicit provision for different fining tiers to apply to breaches of Articles 5 and 32 GDPR. It is clear that any infringement of Article 32 falls within the scope of Article 83(4) whilst an infringement of Article 5(1)(f) falls within the scope of Article 83(5). Article 83(4) is not more specific than Article 83(5). It is incapable of overriding it. Rather, any issue as to which maximum penalty applies is resolved by the application of

[154] *R (Hallam) v Secretary of State for Justice* [2019] UKSC 2 at [144]. See also Case T-60/06 RENV II *Italy v Commission* (2016), at [81].

Article 83(3) which states in terms that in these circumstances "*the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.*" The legislation itself provides the mechanism for addressing circumstances in which processing engages more than one obligation.

7.82. The Commissioner notes that her interpretation of Articles 83(4)-(5) is supported by the Article 29 Working Party's Guidelines on the application and setting of administrative fines for the purposes of the GDPR, which states:

> *Specific infringements are not given a specific price tag in the Regulation, only a cap (maximum amount). This can be indicative of a relative lower degree of gravity for a breach of obligations listed in article 83(4), compared with those set out in article 83(5). The effective, proportionate and dissuasive reaction to a breach of article 83(5) will however depend on the circumstances of the case…*
>
> *The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement. Therefore, if an infringement of article 8 and article 12 has been discovered, then the supervisory authority may be able to apply the corrective measures as set out in article 83(5) which correspond to the category of the gravest infringement, namely article 12….*[155]

7.83. In any event, BA's core objection to the use of the 4% maximum penalty appears to be its impact on the turnover-bands applied under the Draft Internal Procedure in calculating the proposed fine included in the NOI. As this approach has not been adopted in determining the final level of penalty to be imposed, the same concerns do not arise. It is noted that the final penalty imposed is well below the 2% cap, and so the application of that cap in reaching the final decision, as opposed to a 4% cap, would not have made a difference. BA is wrong to contend otherwise.[156] The Commissioner has considered what level of penalty is proportionate on the facts of

[155] Pages 9-10.
[156] BA's Second Representations, paras 5.20- 5.21.

this case. The fact that this penalty is below both penalty caps merely shows that a dispute over which cap should apply would be academic.

(5) Application of the RAP

7.84. In response to the NOI, BA submitted that the Commissioner had acted contrary to the RAP in: (a) deciding to impose a penalty at all in this case; and (b) in setting the proposed level of fine. BA relied in this regard on the public law obligation on an authority to comply with its published policies unless there is a good reason for any departure.[157]

7.85. The Commissioner has complied with her published policies in preparing the NOI and making her final decision in this case.

7.86. First, the Commissioner has not acted contrary to the RAP by deciding to impose a penalty on BA. At paras 6.5-6.6 of its First Representations and para 5.24(a) of its Second Representations, BA misunderstands and/or misapplies the guidance at page 25 of the RAP:

a. A breach does not need to qualify as a *"most severe breach…"* for the Commissioner to issue a penalty notice. The guidance quoted by BA explains only that in the majority of cases the Commissioner will reserve her powers for the most serious cases. The RAP does not introduce a new criterion that a case must qualify as a "most severe" breach before the Commissioner will apply a penalty in accordance with Article 83 GDPR and the RAP (and the latter must be read and understood in the context of the EU law regime).

b. In any event, the types of the "most severe" breaches which the RAP explains are likely to result in a penalty notice being issued include cases of "*negligent acts*". The Commissioner has found that BA acted negligently (within the meaning of the GDPR) in this case.[158]

[157] BA's First Representations, paras 6.1-6.12; and BA's Second Representations, paras 5.22-5.24.
[158] BA's First Representations fail to accurately reflect the totality of the Guidance provided in the RAP. While page 25 refers to the fact a penalty is more likely to be imposed where it involves *"wilful action",* the RAP also makes clear that the extent of negligence involved in a breach is relevant to deciding whether to impose a penalty and, if so, the amount;

c. The RAP does not list the *"criteria"* which make a penalty more likely to be imposed. Page 25 of the RAP provides examples of circumstances where it is more likely for a penalty to be imposed. These are expressly described as *"examples"* and there is no suggestion that either the list is exhaustive, or that all or many of the circumstances have to be present before the Commissioner can consider the imposition of a penalty to be appropriate. Any such approach would unduly fetter the Commissioner's regulatory discretion.

d. In any event, the facts of this case: (i) satisfy a number of the "criteria" or, more accurately, fall within the examples given at para 25 of the RAP and/or (ii) fall within the relevant considerations at page 24 of the RAP. Contrary to para 6.6 of BA's Representations, the infringements in this case:

i. affected a significant number of data subjects, and the fact that other breaches have also involved millions of data subjects does not detract from this point[159];

ii. are likely to have caused a degree of damage or harm; and

iii. involve *"a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it)"*. BA's Representations state that this example is *"not applicable".* For the detailed reasons given above, BA's position is not correct.

7.87. Second, the Commissioner has not erred by failing to apply the *"criteria"* set out at page 27 of the RAP for applying a higher penalty.[160] This submission is based on a misreading and misapplication of the RAP.

7.88. The types of cases included at page 27 of the RAP are not a list of *"six criteria identified by the ICO as meriting a "higher" penalty"*.[161] As page 27 states, it is a list of examples of the type of situation where, generally, the amount of penalty will be higher. This passage relists a selection of the aggravating factors referred to at page 11 of the RAP and explains – perhaps self-evidently – that where those

[160] BA's First Representations, paras 6.10-6.12.
[161] BA's First Representations, para 6.12.

factors exist, a data controller can, generally speaking, expect the penalty to be higher than where they do not exist, in the case of otherwise similar breaches.

7.89. The examples provided are not to be applied as a list of criteria which must be met in any case before a penalty exceeding £1 million can be imposed, as BA appears to imply in its submissions. This section of the RAP does not refer to the concept of "*very significant*" penalties at all. This language is used only to describe the types of situations in which the Commissioner may convene an advisory panel.[162] While the RAP describes "*very significant*" penalties as "*expected to be those over the threshold of 1M*", this was not intended to be - and in any event cannot objectively be read as - giving an indication to controllers of the likely penalty they may face in the event of a data breach, particularly in light of the provisions of the GDPR.

7.90. The GDPR was enacted in 2016 and came into force two years later. Data controllers, especially global undertakings of the size of BA, would have been fully aware of the maximum penalties permitted by GDPR. The reference to the sum of £1 million in the RAP does no more than describe the circumstances in which the Commissioner may decide to convene an advisory panel. The decision as to whether a penalty should be imposed and at what level, in order to provide an effective, proportionate, and dissuasive result has to be reached through the application of Article 83(2) GDPR and section 155 DPA. It is clear from the RAP that the Commissioner will adopt a case-specific approach, taking into account all relevant considerations. That is the approach taken in this case.

7.91. Third, the Commissioner has taken into account, insofar as necessary, BA's own approach to applying the RAP to this case.

7.92. Paras 6.13-6.28 of BA's First Representations consist of BA's own application of the five-step penalty setting process. The Commissioner has considered those representations. She notes that:

[162] Page 26 of the RAP.

a. To the extent that the Representations raise concerns about the application of the Draft Internal Procedure and/or the use of turnover bands, they have been addressed above.[163]

b. The Commissioner has applied correctly each of the limbs of Article 83(2) in this case. For example, the fact that the breach was not intentional is not the only consideration that is relevant under Article 83(2)(b), contrary to para 6.17 of BA's Representations. Article 83 also requires consideration of whether BA's actions were negligent, within the meaning of the GDPR (which the Commissioner has found to be the case).

c. The distinction drawn by BA between imposing a fine for the infringement of the GDPR and not the *"personal data breach"* is not a good one.[164] Clearly, in establishing the nature and gravity of the infringement, including the impact on data subjects, regard must be had to the impact of the personal data breach.

d. The Commissioner has decided on a reduced level of penalty, having taken into account BA's Representations.

e. BA is wrong to rely on cases issued under the previous DPA 1998 regime to calculate the penalty applicable under the new EU regulatory framework.[165]

f. Concerns about the draft of internal records of the ICO's early decision-making,[166] prior to the issuing of both the NOI and this decision, are no longer relevant. As has been made clear in both the NOI, and this decision, the Commissioner has not increased the penalty at Step 3 of the process as she has not found there to be any aggravating factors in this case.

7.93. It is noted that in Chapter 9 of its First Representations BA applies the five-step process again, but on the basis of: (a) the Commissioner being constrained by the fine levels that were imposed under DPA 1998; and (b) the levels of fines imposed by other EU regulators in the relatively few decisions made under the

[163] BA's First Representations, paras 6.13, 6.16, 6.18, 6.23, 6.28.
[164] See para 6.18 of BA's First Representations.
[165] BA's First Representations, paras 6.20, 6.23-6.25.
[166] BA's First Representations, paras 6.21-6.22.

GDPR to date and/or a single guidance document from another authority. For the reasons provided in detail below, the Commissioner does not accept that she is constrained to apply the RAP in this manner, which would be contrary to Article 83 GDPR. Thus, while she has considered BA's calculation of an alternative fine premised, in particular, on comparisons with fines issued under DPA 1998, BA's arguments do not alter the Commissioner's conclusions on the proper application of Article 83 GDPR and the RAP in this case, set out above.

7.94. In BA's Second Representations, BA sets out an alternative application of the Article 83(2) criteria, as part of its claim that the revised penalty proposed in the draft decision is wholly disproportionate. This alternative application reflects the differences in position between the Commissioner and BA on a number of issues relevant to determining whether any penalty should be imposed and, if so, at what level. In particular, BA disagrees with the Commissioner's judgment as to the seriousness of the infringement and its impact on data subjects, the negligent character of the infringement, the degree of responsibility on the part of BA, the categories of personal data affected. The Commissioner has responded to BA's case on these matters above. However most fundamentally BA entirely ignores Article 83(1) and the obligation on the Commissioner to ensure that any penalty it imposes is "*effective, proportionate and dissuasive*". Any attempt to recalculate the overall penalty, and particularly where the claim is that it is "*wholly disproportionate*" must have regard to this obligation.[167]

(6) Legal Certainty and the approach adopted under DPA 1998

7.95. In its Representations in response to the NOI, BA emphasised that:

a. the proposed penalty engages its fundamental property rights; and

b. as a result, the penalty regime applied under DPA must have sufficient certainty to protect against arbitrariness.

7.96. BA's position is that the current regime does not provide that necessary certainty. Consequently, BA states that the Commissioner

[167] BA's Second Representations, paras 4.14-415 and page 30.

should continue to apply penalties in a manner which is consistent with the approach she adopted under the superseded DPA 1998 regime, or with the limited decisions or guidance issued to date by the other supervisory authorities under the GDPR.[168]

The alleged lack of legal certainty

7.97. As set out above, the Commissioner recognises that in imposing a penalty on a controller, she must comply with any relevant fundamental rights that are engaged, including under the ECHR or the EU Charter. The Commissioner does not accept that the penalty regime applicable under, in particular, Article 83 GDPR (and section 155 DPA) lacks sufficient certainty such that it cannot be lawfully applied in conjunction with the RAP.

7.98. First, in para 7.8 of its First Representations, BA attacks the DPA as failing to provide guidance beyond the requirement that it pay due regard to specified matters. However, the DPA reflects the directly applicable EU law framework for assessing penalties. The Commissioner does not agree with BA that Article 83 GDPR or section 155 DPA are so unclear that they are unlawful. Taken together, those provisions specify the circumstances in which a data protection authority has the power to impose an administrative penalty, and the matters that are relevant to that decision and the amount of any penalty.

7.99. BA seeks to compare section 155 DPA and section 55A DPA 1998. That comparison is inapt. The latter provision was enacted in domestic law in a context where the 1995 Data Protection Directive did not specify how national regulators should make decisions about penalties. The field has now been occupied by Article 83 GDPR. The GDPR regime, which is directly applicable law, was specifically designed to strengthen the enforcement of data protection rights across Europe.

7.100. Further, and in any event, section 55A of the DPA 1998, on which BA relies, gave the Commissioner a discretion as to whether to impose a penalty, where a number of factors were satisfied. These included the seriousness of the contravention, its impact on data subjects, and the degree of culpability on the part of the controller.

[168] BA's First Representations, paras 7.1-7.23.

These criteria are comparable, in terms of specificity, with the provisions of the DPA, which require the Commissioner to have regard to Article 83(2). The factors listed in Article 83(2) include, in substance, all of those under section 55A of the DPA 1998, as well as a number of additional factors. The Commissioner was and remains required to exercise her judgment as to, for example, the seriousness and nature of any contravention, in deciding whether to impose a penalty. Thus, even if the comparison were relevant, the Commissioner does not accept BA's attempt to distinguish the current and old regimes.

7.101. Second, BA contends that it is not challenging the legality of the GDPR legislative regime itself. Instead, it says that Articles 83(8)-(9) and 70(1)(k) GDPR *"directly envisage and expect"* that the high-level principles set out in the legislation will be the subject of national or supranational guidance.[169] In fact, Article 83(8)-(9), make no mention of the need for guidance in order for Articles 83(1)-(6) to be applied lawfully (see above). Article 70(1)(k) provides that the European Data Protection Board can on its own initiative or at the request of the Commission issue guidelines about the setting of administrative fines. However, the application of Article 83 is not made contingent upon the Board doing so, and the Board has in fact adopted the guidelines issued previously by the Article 29 Working Party. This decision (and the NOI and draft decision) are consistent with that guidance.

7.102. BA also relies on the fact that pursuant to section 160 DPA the Commissioner is obliged to issue guidance in respect of how she will determine the amount of penalties to be imposed. However, the Commissioner has done so. In accordance with s. 161 DPA, the RAP was laid before Parliament for approval, and was duly approved. Ultimately, BA's challenge is against the RAP, but that guidance has to be read alongside the obligations imposed on the Commissioner by Article 83 GDPR, and section 155 DPA, in respect of the correct approach to imposing fines.

7.103. Third, turning to the guidance issued by the Commissioner, BA criticises the RAP as being too vague to satisfy the requirements of

[169] BA's Second Representations, para 5.46.

legal certainty. More specifically, it is necessary to address the following points BA makes in this regard:

a. First, that the ICO's previous guidance on penalties under the DPA 1998 was longer or more detailed. However, this is a complaint of form, not substance. If the guidance provided by the RAP, taken together with the legislative regime, satisfies any relevant requirement of legal certainty, it is not relevant whether previous guidance was longer and/or provided across more than one document.[170]

b. Second, BA refers to the fact that the old guidance was a separate document, and not provided as part of the RAP in place at that time. Again, this is a complaint of form and not substance.[171]

c. Third, BA claims that it follows from the development of the Draft Internal Procedure that the RAP is deficient[172] and/or that it follows from the abandonment of that Procedure that the Commissioner no longer has a methodology upon which to base its proposed penalty.[173] These points are incorrect:

    i. The Draft Internal Procedure is no longer relied upon and, in any event, it was not developed in order to 'cure' a gap in legal certainty.[174] It was intended to be a helpful supplement to the RAP for internal decision-making purposes. The GDPR is a new regime. More detailed guidance may be developed over time as the UK and EU Member States gain experience in applying it. The ICO may well seek to publish further guidance in the future on penalty-setting. But the potential for further development is not equivalent to the present guidance being so unclear as to be unlawful. The RAP provides sufficient guidance as to the circumstances in which penalties, including large penalties, will be applied. The Commissioner therefore does not accept BA's argument that the RAP is *"clearly insufficient"*.

[170] BA's First Representations, para 7.9.
[171] BA's First Representations, paras 7.9-7.11
[172] BA's First Representations, paras 7.11-7.15.
[173] BA's Second Representations, paras 5.32-5.41.
[174] Contrary to the submissions at paras 7.12-7.13 and 7.15. of BA's First Representations.

ii. The Commissioner has applied the approach set out in her RAP, and considered the factors identified under Article 83 GDP. In paras 7.1-7.55 above, the Commissioner has explained each relevant step of the calculation. The Draft Internal Procedure was consistent with this approach. The Commissioner does not therefore accept that without the Draft Internal Procedure it is impossible for her to lawfully calculate a penalty, she also does not accept that the legislation and Parliamentary-approved RAP leave any "*lacuna*".[175] This argument in respect of legal certainty is addressed in more detail below.

d. Fourth, BA claims that the penalty setting process set out in the RAP is too opaque, and thereby prevents BA's effective scrutiny of the Commissioner's quantification analysis. Specifically, BA claims that only a "*systematic and transparent calculation methodology in the context of the quantification exercise*" will provide sufficient legal certainty to allow the Commissioner to impose a penalty.[176] It is not accepted that the 5-step process set out in the RAP is opaque, or in fact that any guidance could permit a controller to calculate specifically what any fine might be. The guidance has to cover a wide range of potential situations. In any event, to assist BA, the Commissioner has dealt with the mitigating factors arising in this case under Step 5 of the analysis so that it can see the impact of these on the overall level of penalty.

7.104. The GDPR is a new regime. More detailed guidance may well be developed over time as the UK and EU Member States gain experience in applying it. As BA highlights, the Commissioner has committed to updating its guidance in the future. But the potential for further development is not equivalent to the present guidance being so unclear as to be unlawful (contrary to para 5.45 of BA's Second Representations). The RAP provides sufficient guidance as to the circumstances in which penalties, including large penalties, will be applied.

[175] BA's Second Representations, paras 5.33-5.34.
[176] BA's Second Representations, paras 5.36-5.40.

7.105. Fourth, BA's argument appears to be that because it is possible for the RAP to be more detailed, it must follow that the RAP is insufficiently detailed to fulfil the requirements of legal certainty. The Commissioner considers that the RAP, which must be read alongside the DPA and the GDPR, provides sufficient clarity and legal certainty, as required under the ECHR and EU law. The RAP explains that Step 2 intends to "*censure*" the breach, and this requires taking into consideration its scale (including the number of data subjects affected) and the severity of the breach itself, and expressly refers to the factors set out in the DPA. Where these are not already considered by reason of Article 83(2)(a)-(j), examples of aggravating factors are set out in the RAP to assist with the interpretation of Step 3, as well as mitigating factors (Step 5).

7.106. Fifth, BA also criticises the five-step procedure set out in the RAP on the basis that it is confused and internally contradictory. It is claimed that if Step 2 is complied with properly, Steps 3-5 are rendered duplicative and/or redundant.[177] In a holistic assessment of a penalty, in accordance with Article 83(1)-(2), the five-step process could in theory be applied in a way that results in overlap. However, the Commissioner has made it clear above at which step in the process the relevant factors, as defined in Article 83 and the RAP, have been taken into account in assessing whether to impose a penalty, and in determining the amount. There is no unlawful uncertainty in the approach taken by the Commissioner. In any event, as explained above, the Commissioner has altered how she addresses the potential overlap in this final penalty notice to provide additional transparency as to her approach, in the light of BA's submissions in this regard.

7.107. Sixth, having submitted in its First Representations that the Commissioner's reliance upon the Draft Internal Procedure, which had provided such a quantification methodology, contravened the principle of legal certainty, BA's position in its Second Representations is that the Commissioner has erred by not relying upon a clear and certain quantification methodology as that is also a breach of legal certainty.[178] Yet, BA accepts that the principle of legal certainty does not require the Commissioner to publish a RAP

[177] BA's First Representations, para 7.14; and BA's Second Representations, paras 5.42-5.44.
[178] BA's Second Representations, paras 5.32-5.47.

which allows a controller such as BA to predict exactly the sum of any penalty which may be imposed.[179] The penalty calculation process set out in the RAP was approved by Parliament and, to some extent, reproduces the considerations under Article 83 of the GDPR which is a directly effective harmonising measure. Legal certainty does not require BA to know exactly how the different factors are weighted by the Commissioner in this case. It is sufficient that BA knows a) what those factors are, b) at what stage of the penalty calculation process those factors will be taken into account; c) the need for any penalty to be effective, proportionate and dissuasive, and d) that considering turnover is relevant to (c). The Commissioner has taken into account all of the factors referred to above, these factors were looked at in the round, giving careful consideration for the overall requirement under Article 83(1) for a penalty to be proportionate and dissuasive.

7.108. Thus, the Commissioner not accept BA's argument that the RAP is *"clearly insufficient"*. Consequently, the Commissioner does not accept BA's arguments as to the requirements of legal certainty in this context, nor the contention that, taking Article 83 GDPR, the DPA, relevant EDPB guidance[180] and the RAP as a whole, *"it is impossible for controllers (or anyone else) to assess how the ICO will exercise its fining powers…"*[181]

7.109. The Commissioner notes that BA, at paras 7.17-7.20 of its First Representations, relies upon the penalty-setting guidance of the CMA. The Commissioner has considered penalty setting in other regulatory contexts. She recognises that each regulator must take enforcement action within the bounds of its own legal obligations, and in this case the Commissioner is bound to comply with Article 83 of the GDPR.

Application of the DPA 1998

7.110. BA's solution to the alleged lack of legal certainty in the new EU law regime, read together with the RAP, is for the Commissioner to adopt an approach to fines under Article 83 GDPR which is consistent with its previous enforcement decisions under the DPA 1998 (para

[179] BA's Second Representations, para 5.59.
[180] See Article 29 Data Protection Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, which refers to
[181] BA's First Representations, para 7.16. See also BA's Second Representations, paras 5.35-5.45.

7.23 and Chapter 8 of BA's First Representations). What BA seeks, in effect, is for the Commissioner unilaterally to impose the previous domestic cap and approach to fines which applied in the UK prior to the EU issuing the harmonised regime under the GDPR.

7.111. Plainly it is not open to the Commissioner, as a matter of domestic or EU law, to adopt unilaterally an approach that would undermine the object and purpose of the new EU regime. The GDPR, and consequently the DPA, represent a significant departure from the regime under the DPA 1998 and the 1995 Directive. The GDPR was expressly intended to harmonise the rights of, and protections afforded to, data subjects across the EU. It differs markedly from the 1995 Directive, most obviously in that it introduces significantly higher and more effective penalties, with maximum penalties defined expressly by reference to turnover. The GDPR also imposes new obligations on controllers, including new organisational requirements such as the designation of a data protection officer and new provisions on the lawfulness of processing. The GDPR and the DPA have significantly changed the legal landscape in data protection and enforcement.

7.112. BA's First Representations at paras 7.23 and 8.1-8.11 are to the effect that the Commissioner should, in the alleged absence of legal certainty under the current regime, maintain the position under the DPA 1998. Such an approach would be inconsistent with the obligations imposed on the United Kingdom and the Commissioner by the GDPR and EU law.

7.113. The points made above are unaffected by any public statements that may have been made by the Commissioner or her staff. Those statements to which BA refers have been quoted selectively and/or taken out of their proper context by BA. BA disputes this,[182] however the Commissioner maintains her position for the following reasons:

a. BA refers to a blog post published by Elizabeth Denham on 9 August 2017.[183] Whilst it is true that the post states that the Commissioner will not "*simply scale up penalties*" issued under the DPA 1998, it also states that "*Don't get me wrong, the UK fought for increased powers when the GDPR was being drawn*

[182] BA's Second Representations, paras 5.54-5.60.
[183] BA's First Representations, para 8.14(a).

up. Heavy fines for serious breaches reflect just how important personal data is in the 21st century world. We intend to use those powers proportionately and judiciously."

b. BA refers to a speech made by James Dipple-Johnstone at the Data Protection Practitioner's Conference on 9 April 2018,[184] however the quotation which BA selectively cited is preceded by a summary of the approach the Commissioner intended to take, including "*we will look at each case on its own merits. We'll look at the features and context of each case. And, this is important, we will focus on area of greatest risk to people – potential or actual harm… The more serious, high impact, deliberate, wilful or repeated breaches can expect the most robust response."*

7.114. In this decision, and as set out in the penalty calculation above, the Commissioner has not "simply" scaled up penalties, or added zeros to the maximum penalty applicable under the DPA 1998.[185] None of the statements made by the Commissioner or her office can be relied upon as creating a legitimate expectation that the Commissioner will not fully apply the provisions of the legal regime under the DPA and the GDPR. More specifically, the public statements referred to by BA at paras 8.12-8.15 of its First Representations (and contextualised above) were not intended to be – and cannot objectively be read as – assurances to any controller that the Commissioner would not use her full powers on a case by case basis, to impose effective, proportionate and dissuasive penalties in appropriate cases, which includes the possibility of large fines where appropriate.

Other decisions by the Commissioner / decisions by other European authorities

7.115. BA submits[186] that the proposed penalty is: (a) inconsistent with previous action by other EU supervisory authorities, contrary to the stated aim of the GDPR being to create a harmonised regime; and (b) inconsistent with a decision reached by the Commissioner in a different case. In particular, BA's Representations imply that the

[184] BA's First Representations, para 8.14(b).
[185] BA's Second Representations, para 5.55.
[186] BA's First Representations, paras 8.16-8.24. BA's Second Representations, paras 5.25-5.31.

appropriate penalty in this case should be set at a level consistent with those imposed by:

a. the Romanian authority on UniCredit Bank SA. The company was fined of €130,000 for a breach of Article 25 GDPR due to the compromise of payment details, when its worldwide turnover for 2018 was of €18 billion;

b. the Portuguese authority on a hospital. The hospital was fined €400,000 for the incorrect handling of patient records;

c. the Austrian Data Protection Authority against Osterreichische Post AG, which was fined €18 million;

d. a €2.6 million fine issued by the Bulgarian Commission of Personal Data Protection to the Bulgarian Revenue Agency in relation to a cyber attack which affected over 5 million data subjects; and

e. the Commissioner's decision regarding Doorstep Dispensaree Ltd, dated 20 December 2019.

7.116. The purpose of GDPR is to secure a harmonised regime. However, in the first instance, that harmonisation is achieved through the application of harmonised rules and standards to the particular facts of the case at issue. Any cross-border processing decision must then be subject to the Article 60 process.

7.117. The Commissioner, along with other EU supervisory authorities, must comply with her obligations under Article 83 and that means that she is required to impose a penalty which, in her own judgment, having regard to all the matters listed in Article 83, and on the facts of the individual case, is effective, proportionate, and dissuasive. In principle, 'equivalent' breaches should attach 'equivalent' penalties. But in practice, each case must turn on its own particular facts. Whilst the Commissioner has considered the limited information available about the cases to which BA has referred, she maintains that simple comparisons of the penalties imposed in different cases do not show that the Commissioner has erred in applying Article 83 GDPR, DPA and/or the RAP.

7.118. There is a great degree of variation in the penalties imposed by supervisory authorities even in the context of the limited fines imposed to date,[187] which are – in the Commissioner's view – indicative of a decision-making process that is fact-specific. The Commissioner further considers that it would be premature and not necessarily helpful to rely heavily at this juncture on a survey of the action taken by other supervisory authorities, given the relatively few decisions that have been taken under the new regime. This is particularly the case where there is limited public information available about the reasons for the decisions taken by other authorities.

7.119. As to BA's reference to the guidance published by the Netherlands SA, the Commissioner does not consider that the approach can be distinguished in principle from that of the Commissioner or that the level of penalty – had this matter been before the Netherlands SA – would necessarily have been very different. The guidance leaves open the possibility that, having regard to all of the factors set out in Article 83, the Netherlands SA would consider that in BA's case a penalty above 1,000,000 Euros was appropriate.

7.120. Further, as to the comparison drawn by BA between the policy of the Netherlands authority, and the Commissioner's former Draft Internal Procedure,[188] in the light of the points made above, those concerns no longer arise.

7.121. In any event, as the Commissioner is acting as lead authority in this case, the way to ensure that consistency is not by comparing the penalty to a selection of other penalties issued on different facts in the EU. Rather, the consistency mechanism provided for by Articles 60(4) and 63 GDPR will allow for all of the supervisory authorities concerned to cooperate with the Commissioner, make enquiries, and contribute their views in order to ensure the consistency of the ultimate penalty sum with penalties that have been (if there are any) and/or will be applied in similar situations. Contrary to BA's Second Representations, the Commissioner does not "*simply rely*" on the

[187] Notably the decision of the French SA, the CNIL, to fine Google 50 million Euros. See also https://www.enforcementtracker.com/ which suggests there is significant variation in the level of fines that have been imposed to date, ranging from a few thousand to millions of pounds.

[188] BA's First Representations, para 8.22.

consistency mechanism to ensure consistency.[189] However, the Article 60 process is one of the factors which, as noted in Article 63, contributes to the consistent application of the GDPR and the Commissioner is entitled to rely on the process as a contributory factor.

(7) Effectiveness

7.122. The Commissioner does not accept BA's submission that imposing a large penalty will necessarily have a chilling effect on the self-reporting of breaches. On the contrary, given the powers of the ICO to impose a sufficiently dissuasive penalty, and the fact that failing to report a breach or otherwise cooperate with an investigation are aggravating factors when calculating the penalty sum, the Commissioner considers it unlikely that controllers will decide not to report a major breach as a result of the level of the penalty imposed on BA. This is particularly so in circumstances where BA has been given a penalty reduced from the level proposed in the NOI, and that expressly takes into account early notification and cooperation, which is likely to encourage such conduct by other controllers in the future.

7.123. The Commissioner notes that the revised penalty of £20m is considerably lower than the original proposed penalty, having taken into account BA's detailed Representations.

(8) Rights of the Defence

7.124. BA advances two criticisms of the Commissioner's procedure in respect of the NOI, on the basis that she has failed to comply with the rights of the defence.

7.125. First, it is suggested that the NOI does not comply with the public law requirement that it must be properly and fully reasoned, and it is also too brief (as is the Commissioner's record of her internal decision-making process).[190] Second, it contended in the First Representations that the Commissioner's conduct between the issuing of the NOI undermined due process and BA's right to a defence.[191] Third, in its Second Representations it made similar

[189] BA's Second Representations, para 5.28.
[190] BA's First Representations, paras 11.1-11.11.
[191] BA's First Representations, paras 12.1-12.14.

claims in respect of the Commissioner's conduct in preparing the draft decision. In particular, BA builds upon its claims that the Commissioner's initial NOI was inadequately reasoned, and states that the Commissioner's draft decision bore little resemblance to the case put against BA in the NOI and is therefore unfair and contradicts the spirit of the statutory process.[192]

7.126. The Commissioner does not accept any of these points.

7.127. First, the Commissioner is required to provide an adequately reasoned decision, which is intelligible and which conveys the reasons for the decision in such a way that enables the addressee to make representations and identify any errors of reasoning.[193]

7.128. The NOI complied with those requirements. It is notable, in particular, that the NOI was sufficiently detailed to enable BA to submit 76 pages of closely argued representations, and additional annexes. The NOI (at paras 16 to 24) set out the Commissioner's understanding at that time of how the Attack occurred and the failures it disclosed – based on the information provided by BA - which enabled BA to make representations and provide further information. The Commissioner's reasons for the imposition of the penalty were set out at paras 27 to 35 of the NOI and relied and built upon the preceding paras. The fact that the Commissioner could, in BA's view, have produced a lengthier Notice is not a basis for the contention that the NOI was unlawfully or inadequately reasoned. Nor is it the case that a proposed greater penalty necessarily calls for a lengthier NOI.

7.129. BA gives a number of examples of what it purports to be inadequate clarity on the part of the Commissioner in the NOI, including alleged *"vagueness about the commencement and duration of any infringement by BA"*[194] and the reference to the total number of affected data subjects. Where appropriate and necessary, clarifications were provided in the draft decision and in this document.

---

[192] BA's Second Representations, paras 2.9-2.12.
[193] See, for example, *R v London Borough of Croydon, ex p. Graham* (1993) 26 H.L.R 286; *R v Brent London Borough Council, ex p Baruwa* (1997) 29 HLR 915.
[194] BA's First Representations, para 11.17.

7.130. Second, BA's complaints about the Commissioner's internal record of decision-making are also not accepted, and it is unclear precisely what relevance these points are said to have to the matters under consideration. As would be expected, the Commissioner's internal decision-making processes develop and change, depending on the nature of any particular investigation. The reasons for the Commissioner's decision are fully recorded in this document.

7.131. Third, there is no obligation on the Commissioner to issue a penalty notice in precisely the same terms as the NOI. The Commissioner carried out a lengthy and detailed investigation into the Attack. The purpose of requiring the Commissioner to issue notices of intent is to permit consultation. Through issuing the NOI, BA was afforded the opportunity to use the consultation process to make meaningful representations which were capable of affecting the outcome of the investigation. BA was then provided with a second, additional, such opportunity through the Commissioner agreeing to consult again on the draft decision. As a result, BA has provided significant amounts of new information and documents to the Commissioner, and made detailed written representations. The Commissioner rightly took all of the material submitted by BA into account, which necessarily resulted in further clarity being brought to the circumstances of the Attack and a more detailed decision being produced.

7.132. Thus, while the draft decision and this Penalty Notice are more detailed, taking into account the new evidence and submissions received, this does not constitute an abuse of process or a breach of BA's rights of defence. The Commissioner's core concerns remain the same: BA did not have in place appropriate security measures to address the specific deficiencies that were exposed by the Attack. BA understood from the NOI, and the draft decision, the essential elements of the Commissioner's preliminary view that it had breached, in particular, Articles 5(1)(f) and 32 GDPR.

The Commissioner's conduct

7.133. The Commissioner has considered the claims made in chapter 12 of BA's First Representations about her conduct and that of her office.

7.134. First, there is no basis for BA's contention that the Commissioner has a closed mind. The Notice of Intent was expressly provided, in

accordance with the statutory scheme, to enable BA to make representations, which it has on two separate occasions. Those representations, and the further evidence BA has provided, have been taken into account, as is apparent from the content of this decision.

7.135. As to the fact of the draft decision being made public, the Commissioner made it clear in communications with BA's solicitors that a statement would be made by the Commissioner's office in response to BA's own statement to the markets. The press statement was a confirmation of the factual and regulatory position at that time. The Commissioner had carried out an "*extensive investigation*" and based on that investigation had "*issued a notice of its intention to fine British Airways…*". The statement refers to the "*proposed fine*" and states that the Commissioner "*will consider carefully the representations made by the company and the other concerned data protection authorities before it takes its final decision*".

7.136. The Commissioner has noted BA's complaints about the process that was followed and its wider concerns about natural justice. In the light of the express emphasis in the ICO press statement that no final decision had been made, and the process that has in fact been followed, the Commissioner does not consider that those complaints have any merit.

7.137. To the extent that any of these points are relied upon to allege actual or apparent bias on the part of the Commissioner, that allegation is rejected.[195] BA's claim that there has been any infringement of the right to a defence is not correct.

7.138. As to paras 12.12-14 of BA's First Representations, as explained above the Commissioner has not relied on the Draft Internal Procedure, in the light of BA's Representations.

[195] While paras 12.8-12.11 of BA's First Representations refer to such concerns being raised in other cases, and a concern on BA's [art that the ICO is not in a position to guarantee BA's right to natural justice, it was not specifically alleged that the Commissioner was actually biased or acting with apparent bias.

(9) The Panel of Technical Advisers

7.139. During the initial stages of her decision-making process, the Commissioner anticipated convening the Panel and gave an indication of the possible timetable which would apply in this regard in her letter dated 3 October 2019. That letter explained that the Panel "*may be convened before the ICO consults with the other concerned supervisory authorities*."[196] However, the Commissioner subsequently considered the wider process and decided that she would not convene the Panel on the particular facts of this case, in particular as the draft of this Penalty Notice would be subject to the Article 60 GDPR process.

7.140. The Commissioner does not accept BA's argument that, in deciding not to convene the Panel, it has been deprived of an additional safeguard to protect controllers in complex cases through permitting expert input.[197] The correct starting point is that, even in cases concerning "*very significant penalties*", the RAP only provides that the Panel "*may be convened*". It has always been a matter over which the Commissioner has discretion. The Commissioner is not therefore obliged to convene a Panel. It is open to the Commissioner to keep the need for such a Panel to be convened, especially in the context of a new regime, under review. Given that in this case the notice will be submitted to the consistency mechanism enshrined under Article 60 GDPR, the Commissioner decided that further input from an additional expert panel was unnecessary.

(10) The Extension Agreement

7.141. On 23 December 2019, BA agreed to the Commissioner's request for an extension to the statutory timescales. However, BA states in its Second Representations that it was compelled to agree with the extension request because the Commissioner had mishandled the enforcement procedure and thereby subverted the statutory time limit.[198] BA also criticises the Commissioner for refusing to provide a copy of the draft decision without any agreement being in place to permit for consultation upon it.[199]

---

[196] Emphasis added.
[197] BA's Second Representations, paras 2.13-2.16.
[198] BA's Second Representations, paras 2.17-2.30.
[199] BA's Second Representations, paras 2.17-2.30.

7.142. The Commissioner has already addressed the suggestions that the enforcement procedure was mishandled above.

7.143. Further, and in any event, the Commissioner does not accept that BA was compelled to accept the request for the extension.

7.144. First, as the Commissioner explained in her letter of 6 December 2019, she was willing to agree an extension, as permitted by the legislation, in order to allow for a further round of consultation in this case as sought by BA. The legislative scheme does not envisage consultation on a draft decision. But in the circumstances of this case, the Commissioner agreed that such consultation could take place if appropriate arrangements were put in place. There is nothing improper about a decision to permit further consultation if that can be accommodated within the statutory process.

7.145. Second, the Commissioner explained to BA in her letters of 13 and 18 December 2019 that it may be possible to complete the Article 60 process within a short time. However, if not, the provisions of the DPA must be read down and applied in a manner consistent with the GDPR, and in order to give effect to its provisions. That may involve reading down the six-month statutory deadline (or, if necessary, the Commissioner would issue a fresh notice of intent) in order to allow time for the mandatory EU process, which could be of considerable length, depending on the facts of the case.

7.146. Third, BA's submissions proceed on the basis that it has been deprived of an important procedural safeguard as a result of the extension. Yet, Parliament made explicit provision for the Commissioner to agree an extension with controllers. The agreement of such an extension can permit the EU-law mandated process to be accommodated, as Parliament intended. Further, as outlined above, the extension has provided BA with an additional opportunity for consultation on the draft decision. Contrary to BA's submissions,[200] it has not therefore suffered severe prejudice as a result of the consultation and decision-making processes being extended.

[200] BA's Second Representations, para 2.27.

7.147. Fourth, contrary to BA's submissions,[201] there was no obligation on the Commissioner to conduct a further round of consultation irrespective of whether an extension was agreed. The legislation does not envisage or require such further consultation. BA's criticisms of the Commissioner's position that she could not share the draft decision before an extension was agreed are misconceived. Given that the legislative regime does not envisage such consultation, it could not be accommodated without agreeing an extension. It was also not necessary for BA to see the draft decision (and thereby presumably take up the opportunity to make submissions in response to it in any event) before deciding whether it agreed to an extension, accommodating its request for further consultation and the Article 60 process.

7.148. Fifth, as a matter of fact BA did provide significant new information, and adduced detailed written submissions, during the course of the decision-making process. Given the complexity of the case and matters under investigation, it can be no criticism of the Commissioner that she has taken time carefully to consider all material put before her, and she has offered additional opportunities for consultation in this case.

7.149. In short, the statutory deadline is not absolute. Parliament provided expressly for an extension mechanism. The Commissioner does not, therefore, accept that in agreeing to an extension BA was 'forced' to forego important procedural safeguards envisaged by statute.[202] Instead, by agreeing to the extension, BA chose to obtain the benefit of being able to make a second round of representations.

7.150. Finally, BA has no basis to question the integrity of the Article 60 process, the arguments advanced at paragraph 2.28 of BA's Second Representations are speculative and without any reasonable basis.

(11) The Commissioner's compliance with her statutory obligations

7.151. The Commissioner's conduct of this matter has been transparent, accountable, proportionate, and consistent. As to the specific claims made by BA at paragraphs 6.1 and 6.2 of its Second Representations in this regard:

---

[201] BA's Second Representations, paras 2.25-2.27.
[202] BA's Second Representations, para 2.24.

a. The Commissioner, taking into account BA's First Representations, places no reliance upon her Draft Internal Policy. The factors which were taken into account when calculating the proposed penalty sum have been extensively, fully, and entirely transparently set out in this Penalty Notice (and the earlier draft decision, in response to which BA has made full representations).

b. BA, in both of its Representations, has provided detailed representations which comprehensively challenge the Commissioner's decision to impose a penalty and the calculation of the proposed penalty. In these circumstances, and for the additional reasons given above, the Commissioner does not accept that BA cannot effectively challenge the Commissioner's penalty calculation.

c. The penalty is entirely proportionate, and the Commissioner was entitled to take into account BA's turnover in ensuring that the proposed penalty was dissuasive.

d. The Commissioner is obliged to act consistently with her previous enforcement action only where there are comparable cases (both in terms of their facts and the applicable legal regime). The Commissioner has considered the comparators which BA has cited, and – for the aforementioned reasons - she does not accept these reveal an inconsistent approach. For the reasons given above, the Commissioner has not acted inconsistently with any previous public statements. The fact that the Commissioner took into account BA's Representations with respect to the Draft Internal Procedure and changed her approach, is evidence of the effectiveness of the procedural safeguards built into regulatory decision-making, rather than an example of an inconsistent approach. With regards to convening the Panel, this has been addressed above.

7.152. With regards to paras 6.3-6.5 of BA's Second Representations, the Commissioner accepts that pursuant to section 108 of the Deregulation Act 2015, she must have regard to the desirability of promoting economic growth, and thereby exercise her regulatory functions only where needed and where proportionate. The Commissioner notes that the list of factors referred to by BA are only

described by the relevant statutory guidance at para 4.3 as "*indicators*" that the duty under section 108 has been complied with. They are not intended to be or described as a list of exhaustive factors which must – in all circumstances – be taken into account by the Commissioner to demonstrate compliance with the duty under section 108. In this regard, the Commissioner notes that:

a. she is required, by Article 83(1) GDPR, to ensure that any penalty imposed is proportionate and has done so;

b. Article 83(2) GDPR requires the Commissioner to take into account the nature and gravity of the infringement and the degree of responsibility of the controller (in relation to which the Commissioner has taken into account the steps BA took to achieve compliance and the reasons for BA's failures);

c. Article 83(2) GDPR requires the Commissioner to take into account the degree of BA's cooperation with the Commissioner and the steps which BA took to mitigate the damage suffered by data subjects. The Commissioner has thereby considered the steps BA took towards achieving compliance;

d. The likely impact of any penalty on BA, including in terms of the economic cost, was considered when the Commissioner considered any mitigating factors pursuant to Article 83(2) and also when specifically considering financial hardship under Step 5 of the penalty calculation under the RAP;

e. The Commissioner was obliged to ensure that any penalty imposed would be dissuasive, both in respect of BA but also others, pursuant to Article 83(1) of the GDPR and under Step 4 of the penalty calculation in the RAP.

7.153. The Commissioner has, therefore, had regard to the indicative factors listed within the relevant statutory guidance.

7.154. The Commissioner also notes that the obligation under section 108 is not designed "to *legitimise non-compliance and its purpose is not to achieve or promote economic growth at the expense of necessary protections*." Rather, "*the purpose is to ensure that specified regulators give appropriate consideration to the potential impact of their activities and their decisions on economic growth, both for*

individual businesses and more widely for sectors or groups they regulate, alongside their consideration of their other statutory duties" (see para 1.5 of the statutory guidance). The Commissioner has not identified any risks to economic growth in the exercise of her regulatory functions in this matter, nor has BA put forward any cogent case to suggest that there will be any such risk. BA refers to the use of turnover as a "core metric" as being contrary to the promotion of economic growth, however this is entirely misguided. Turnover is an important metric because it ensures that, for similarly serious infringements, larger companies are issued with larger penalties than smaller penalties. This approach is inherently proportionate and cannot pose any risk to economic growth.

8. HOW THE PENALTY IS TO BE PAID

8.1. The penalty must be paid to the Commissioner's office by BACS transfer or cheque.

8.2. The penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

9. ENFORCEMENT POWERS

9.1. The Commissioner will not take action to enforce a penalty unless:

- the period within which a penalty must be paid has expired and all or any of the penalty has not been paid;
- all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and
- the period for appealing against the penalty and any variation of it has expired.

9.2. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Dated the 16th day of October 2020

Signed: ……

Elizabeth Denham
Information Commissioner

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 162(1) of the Data Protection Act 2018 gives any person upon whom a penalty notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   General Regulatory Chamber
   HM Courts & Tribunals Service
   PO Box 9300
   Leicester
   LE1 8DJ

   a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

   b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;

h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).