First-tier Tribunal
General Regulatory Chamber
(Information Rights)

Appeal Reference: EA/2020/0048
NCN: [2023] UKFTT 00983 (GRC)

Before

TRIBUNAL JUDGE MACMILLAN
MS ANNE CHAFER
MS NAOMI MATTHEWS

Between

DSG RETAIL LIMITED

Appellant

and

THE INFORMATION COMMISSIONER

Respondent

Sitting at Field House, London
15 – 23 November 2021

Further written submissions received:
1 & 14 December 2021

Representation:
DSG Retail Limited: Mr Timothy Pitt-Payne QC and Rupert Paines
Information Commissioner: Peter Lockley

DECISION

1. The Monetary Penalty Notice dated 7 January 2020 in the sum of £500,000 was wrong in law and is substituted by this Decision.

2. A Monetary Penalty in the sum of £250,000 is imposed on DSG Retail Limited pursuant to s. 55A of the Data Protection Act 1998

REASONS

A: Introduction

3. This appeal concerns a Monetary Penalty Notice ('MPN') served on DSG Retail Limited ('DSG') by the Information Commissioner on 7 January 2020.

4. The Tribunal held an oral hearing between 15 - 23 November 2021 and reserved its Decision which we now provide. We considered a hearing bundle of 7036 pages, as well as detailed skeleton arguments, written and oral closing submissions, and an authorities bundle. On 1 December 2021 DSG served a further authority and brief additional submissions. The Information Commissioner served further written submissions in reply on 10 December 2021.

5. Promulgation of the Tribunal's Decision has been delayed, initially by my other professional commitments and subsequently due to a period of ill-health. I can only apologise to the Parties for any inconvenience this may have caused.

6. We have been provided with transcripts of the 7-day hearing and are grateful to the parties for their assistance throughout these proceedings and for their detailed submissions. We have considered all submissions, and all of the evidence to which we have been directed, with care.

7. During the hearing, a naming convention was used to prevent sensitive information about DSG's IT security arrangements from entering the public domain. The Tribunal has agreed that the names of 3rd parties and software used by DSG in connection with IT security may be withheld pursuant to rule 14 of the Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009, as amended.

B: Factual Background

8. DSG is a private limited company whose operations include the well-known retail brands Carphone Warehouse, Currys PC World and Dixons Travel. Between 24 July 2017 and 25 April 2018, DSG was the victim of a sophisticated cyber-attack ('the Attack') carried out by persons unknown ('the Attackers'). During this period DSG was in the process of implementing a long-term programme of upgrade and improvement to its IT security systems.

9. The Attack targeted Currys PC World and Dixons Travel stores, deploying malware to approximately 5300 'Point of Sale' ('POS') terminal. These devices are used to process retail sales and consist of a PC with internet access, connected to a PIN entry device card reader. The Attackers were a sophisticated cyber-criminal group who deployed advanced tools, designed to leave minimal forensic evidence of their activity.

They were able to 'scrape' payment card data from the memory of the POS terminals before it entered DSG's encrypted system and to consolidate the 'scraped' data elsewhere within the DSG domain.

10. DSG have established that 5,646,417 payment cards were affected by the Attack, of which 5,592,349 had EMV protection. EMV is a security standard for storing account information on cards which provides enhanced protection over the magnetic stripe traditionally used to store information on the backs of payment cards. A common example of EMV protection is the use of chip and pin. In relation to EMV protected cards, the Attackers obtained only unique primary account numbers ('PAN' - the 16-digit card number) and card expiry dates. No chip and pin data were scraped from the POS terminals.

11. Of the remaining 54,068 cards:

    a. DSG has been unable to determine whether 1280 had EMV protection.
    b. 52,788 cards are known not to have had EMV protection.
    c. Of these, in relation to 44,160 cards the Attackers obtained only PAN and expiry dates, and
    d. in relation to the remaining 8628 cards, the Attackers obtained PAN, expiry dates and cardholder names.

12. DSG's investigation identified five batches of data within the DSG domain that had been compromised by the Attackers. The card data scraped from the POS terminals is referred to in these proceedings as Batch 1 data. It was stored by the Attackers on a 'staging server' within DSG's domain, and it is presumed that the Attackers did so for the purpose of exfiltration.

13. Forensic experts have been unable to identify the exact point of entry exploited by the Attackers. However, it is known that, once they had gained access to the DSG environment, the Attackers were able to compromise a number of internal systems and accounts, including multiple domain administrator accounts which provided the Attackers with significant access privileges.

14. DSG have also identified a substantial quantity of non-financial personal data, which the Attackers were able to access from areas of the DSG domain other than the POS terminals. This comprised[1]:

    a. 1,181,839 records combining employee data, customer data and supplier information, described as having been obtained from different sources within DSG's domain ('Batch 2'). This data included customer email addresses, postcodes, postal addresses, and telephone numbers. Batch 2 was the 2nd to be identified by the DSG investigation. It had been stored on a different staging server to Batch 1.

    b. Approximately 10 million records of personal data extracted from a marketing database ('Batch 3'). This potentially included data such as customer names, postal addresses, phone numbers, email addresses, dates of birth, and data

[1] Figures taken from Elliott Frazer's statement – D184 – D198

related to failed credit check details. DSG state that approximately 11.6 GB of Batch 3 data may have been transferred out of the DSG environment.

c. Approximately 2.9 million records from a database used by DSG for internal fraud investigations. ('Batch 4.1'). This is personal data described by DSG as being broadly similar to that in Batch 3, but also included payment card data in a masked format (i.e., details of the card expiry date, issue date and PAN with the middle eight digits replaced by XXXXXXXX). Batch 4.1 is assessed by DSG as having been likely to have been exfiltrated by the Attackers.

d. Approximately 4.7 million records from a second database related to internal fraud investigations ('Batch 4.2' identified at the same time as Batch 4.1). This data included bank account details and sort codes. Batch 4.2 is assessed by DSG as being unlikely to have been exfiltrated by the Attackers or, if exfiltrated, to have been in the form of corrupted fragments.

15. There is no definitive evidence as to whether any of Batches 1 – 4.2 were successfully exfiltrated. It is not disputed that the Attackers possessed the technological skills to have done so, or that evidence exists that data were prepared for exfiltration.

16. In early April 2018 DSG received three tipoffs that an attack on its IT system had taken place. One of these originated from the National Crime Agency, which had received intelligence about a breach of DSG's computer systems between August 2017 and 2 April 2018. DSG's initial investigation confirmed that the Attack had taken place and the company immediately implemented additional security actions in response.

17. Having established the initial circumstances of the Attack, on 8 June 2018 DSG notified the Information Commissioner that there had been a data breach. Thereafter DSG engaged in protracted correspondence with the Information Commissioner, whilst at the same time continuing the forensic investigation and implementing the programme of improvement to its IT security.

18. The forensic investigation of the Attack continued over several months. Not all forensic material has been provided, but there is a large volume of technical evidence before the Tribunal, discussed further below. The evidence shows that the Attackers deployed tools designed to leave minimal forensic traces of their incursion. On 27 March 2018, the Attackers created a clean-up script designed to delete traces of their activities. However, this script may not have deployed as intended since evidence of the Attack remained on DSG systems and was subsequently identified by the forensic investigation.

19. Having reviewed a large volume of information about the Attack and IT security provided by DSG, on 5 August 2019 the Information Commissioner served DSG with a Notice of Intent ('NOI') to impose a monetary penalty in the sum of £500,000, issued pursuant to section 55 of the Data Protection Act 1998 ('DPA'). The NOI identified nine aspects of DSG's technical and organisational IT measures that the Information Commissioner assessed as being inadequate for the purposes of data security.

20. DSG responded to the NOI by providing the Information Commissioner with further information about the technical and organisational measures in place in relation to the nine measures identified in the NOI.

21. Having considered DSG's further representations, on 7 January 2020 the Information Commissioner issued a Monetary Penalty Notice ('MPN') in the sum of £500,000. That Notice is the subject of this appeal.

C: Law

Personal data

22. The Data Protection Act 1998 ('DPA') implemented European legislation (Directive 95/46/EC), concerning the right of an individual to the protection of personal data. Although the 1998 DPA has been superseded, it applied throughout the period with which the MPN is concerned.

23. The 'personal data' with which the Act is concerned is defined in section 1 as including:

"*data which relate to a living individual who can be identified—*
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller."

24. An expanded definition is found in Article 2(a) and Recital 26 of Directive 95/46/EC (emphasis added):

"For the purposes of this Directive:

"(a) ' personal data ' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly , in particular by reference to an identification number or to one or
more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of
protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;"

25. Most of the primary facts relating to this appeal are agreed. However, one issue between the Parties, which has been the focus of evidence and submissions (arguably

disproportionately so), is whether PAN are personal data for the purposes of the DPA. If it is not, it should not be the subject of the MPN under appeal. In this regard we have been referred to Opinion 4/2007 of the Article 29 Working Party, which analyses four elements of the definition of personal data set out in the Directive[2]. The key elements identified by the Opinion are (1) 'any information'; (2) 'relating to'; (3) 'an identified or identifiable'; and (4) 'natural person'.

26. In the context of the third element the Working Party concluded that a telephone number, car registration number, Social Security number, and a passport number are all identifiers that meet the definition of personal data. It noted that "*this category typically relates to the phenomenon of "unique combinations", whether small or large in size. In cases where prima facie the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from other individuals."*

27. The Working Party noted that identification of an individual through a name may not be necessary in all cases, because it may be possible to achieve this through the use of other "identifiers ":

    "Indeed, computerised files registering personal data usually assign a unique identifier to the persons registered, in order to avoid confusion between two persons in the file. Also on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user. Thus, the individual's personality is pieced together in order to attribute certain decisions to him or her. Without even enquiring about the name and address of the individual it is possible to categorise this person on the basis of socio-economic, psychological, philosophical or other criteria and attribute certain decisions to him or her since the individual's contact point (a computer) no longer necessarily requires the disclosure of his or her identity in the narrow sense. In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name. The definition of personal data reflects this fact."

28. We were referred to a number of authorities on the issue of when an individual may become "identifiable" from information. Subsequent to the hearing, the Parties drew our attention to a further authority: the Upper Tribunal's decision in *NHS Business Authority v Information Commissioner & Spivack [2021] UKUT 192 (AAC)* ('*NHS BA*'). This reviewed a number of the authorities we had already been referred to. Both Parties were allowed an opportunity to amend their submissions in writing, in light of this newly identified authority.

29. In *NHS BA*, Upper Tribunal Judge Jacobs considered identifiability in the context of data that might be disclosed under the Freedom of Information Act 2000. We note that this decision is concerned with the definitions found in the Data Protection Act 2018 and the General Data Protection Regulation ((EU) 2016/679 - 'GDPR'[3]) rather than under the DPA 1998. However, the definitions considered and the principles identified are broadly similar to those set out in the legislation with which this appeal is

[2] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
[3] Which is now retained EU law with minimal modification as the UK GDPR.

concerned, particularly when the DPA 1998 definition of personal data is read with Recital 26 of Directive 95/46/EC.

30. The relevant principles identified in *NHS BA* are as follows:

    a. The test of whether an individual is identifiable from data is a binary question: can a living individual be identified, directly or indirectly? [paragraph 12].

    b. A test of 'reasonable likelihood' applies to the information likely to be used to facilitate identification, including that information which is reasonably likely to be sought out by a motivated intruder [paragraph 13].

    c. The means reasonably likely to be used must lead to an outcome whereby a data subject is individually identifiable, relying solely on the data available and without speculation as to the individual's identity [paragraphs 20 -22].

31. We note that the question of whether an individual can be identified should be determined on the balance of probabilities. This is a higher threshold than that of whether identification is 'reasonably likely,' which was the test originally proposed by DSG in closing submissions.

MPNs

32. Where data being processed is personal data, sections 4(4) and 27(1) of the DPA require a data controller to comply with eight Data Protection Principles ('DPPs'), set out in Schedule 1. In this case the Information Commissioner imposed a MPN because he decided that, at the time of the Attack, DSG had failed to comply with the requirements of DPP7. The relevant parts of DPP7 provides as follows:

"*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*
…

"Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
(b) the nature of the data to be protected."

33. Section 55A of the DPA provides the Information Commissioner with a discretion to impose an MPN on a data controller where there has been a serious contravention of section 4(4), and where two other conditions are met:

(1) The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that—

(a) there has been a serious contravention of section 4(4) by the data controller, (b) the contravention was of a kind likely to cause substantial damage or substantial distress, and
(c) subsection (2) or (3) applies.

...
(3) This subsection applies if the data controller—
(a) knew or ought to have known—
(i) that there was a risk that the contravention would occur, and
(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but
(b) failed to take reasonable steps to prevent the contravention.

...
(4) A monetary penalty notice is a notice requiring the data controller to pay to the Commissioner a monetary penalty of an amount determined by the Commissioner and specified in the notice.

(5) The amount determined by the Commissioner must not exceed the prescribed amount.

34. The prescribed amount, set out in regulation 2 of the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010, is £500,000.

35. Section 48 of the DPA provides a person who has been served with an MPN the right of appeal to the First-tier Tribunal. The Tribunal's powers are set out in section 49:

49.— Determination of appeals.

(1) If on an appeal under section 48(1) 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 he ought to have exercised his discretion differently,
the Tribunal shall allow the appeal or substitute such other notice or decision as could have been served or made by the Commissioner; and in any other case the Tribunal shall dismiss the appeal.
(2) On such an appeal, the Tribunal may review any determination of fact on which the notice in question was based.

36. The Tribunal determined the appeal by way of a full merits review. When carrying out such a review, the Tribunal follows the principle identified by the Court of Appeal in *R (Hope and Glory Public House) v City of Westminster Magistrates Court [2011] PTSR 868,* and confirmed by the Supreme Court in *Hesham Ali v SSHD [2016] 1 WLR 4799* [paragraph 45]:

"…Where an appellate court or tribunal has to reach its own decision, after hearing evidence, it does not, in general, simply start afresh and disregard the decision under appeal. That was made clear in Sagnata Investments Ltd v Norwich Corpn [1971] 2 QB 614, concerned with an appeal to quarter sessions against a licensing decision taken by a local authority. In a more recent licensing case, R (Hope and Glory Public

House Ltd) v City of Westminster Magistrates' Court [2011] PTSR 868, para 45, Toulson LJ put the matter in this way:

> *'It is right in all cases that the magistrates court should pay careful attention to the reasons given by the licensing authority for arriving at the decision under appeal, bearing in mind that Parliament has chosen to place responsibility for making such decisions on local authorities. The weight which magistrates should ultimately attach to those reasons must be a matter for their judgment in all the circumstances, taking into account the fullness and clarity of the reasons, the nature of the issues and the evidence given on the appeal.' "*

D: The MPN

37. The MPN relies largely on two expert reports provided by DSG during the Information Commissioner's investigation. The names of both are anonymised in these proceedings under the Rule 14 Order previously mentioned above and are referred to in these proceedings as follows:

    a. The 'A Report'. This was commissioned by DSG after it became aware of the Attack. It is dated 28 January 2019 and sets out the results of the post-incident investigation.

    b. The 'B Report'. This sets out the results of a penetration test of two POS terminals and a user laptop, carried out by external IT security experts between 9 – 11 May 2017. It is dated 13 May 2017.

38. The MPN notes that approximately 10 million records of non-financial personal data had been unlawfully processed and exfiltrated from DSG's servers. It further notes that 5,646,417 payment cards were affected by the Attack and proceeds on the basis that the PAN of each card constitutes personal data by itself, providing a relatively limited explanation of this position.

39. The Information Commissioner's decision to issue the MPN was based on both the 'A' and 'B' reports and on his own internal analysis of DSG's IT security arrangements. He concluded that deficiencies in DSG's technical and organisational measures had created a real risk of data breaches such as the Attack occurring, and that this amounted to a failure to comply with DPP7 obligations.

40. The inadequate security measures ('contraventions') identified in the MPN are as follows:

    a. Inadequate network segregation between the POS environment and the wider DSG corporate network. The Information Commissioner cited guidance published by Microsoft in 2014 which recommended that POS devices should be joined to a domain in a separate 'forest'.

    b. The lack of a local firewall configured on the POS terminals. The Information Commissioner relied on the 'B' Report's findings that there was no local firewall configured at the date of testing and that this would have prevented unauthorised access to the POS system and unauthorised movement of data. He

further concluded that DSG should also have had measures in place to detect unauthorised changes to a firewall.

c. Inadequate software patching of DSG's domain controllers and the systems used to administer them. The Information Commissioner noted that the 'B' Report identified numerous instances of missing patches in the POS terminals and concluded that between May 2017 – November 2017 the POS terminals were not compliant with DSG's own patching policy. He further noted that it was suspected the Attacker had exploited an unpatched vulnerability in Group Policy that allowed retrieval of a domain administrator username and password. Storage of passwords in Group Policy was described in the MPN as a known vulnerability, in relation to which a patch had been released by Microsoft in 2014 which required 2 actions to be taken. The second, remedial action – removing existing Group Policies after the patch was applied - was not taken by DSG until after the Attack had been discovered.

d. A failure to perform vulnerability scanning of the compromised environment on a regular basis, which allowed the unpatched vulnerability likely to have been exploited by the Attackers to remain undetected.

e. Failure to consistently manage application whitelisting across the full fleet of POS terminals, with only one of the 2 POS terminals tested for the purposes of the 'B' Report being correctly configured with application control. The Information Commissioner relied on the 'B' Report's recommendation that application whitelisting policies available natively in the system should be enabled, in addition to the 3rd party whitelisting product used by DSG.

f. The lack of an effective system for logging and monitoring IT incidents in a timely manner, which resulted in inadequate oversight of access to DSG's network.

g. Running java software on the POS terminals that was outdated by several years and no longer maintained by the provider.

h. As a further consequence of (issue 7), running an outdated system on the POS terminals that did not support Point to Point Encryption ('P2PE'). In the Information Commissioner's view, it would have been a proportionate measure for DSG to have ensured that P2PE was operating on its systems by the time of the Attack.

i. Failing to manage effectively the security of domain administrator accounts, by failing to risk assess the addition of user accounts and to adhere to its own policies in respect of access permissions and passwords. The Information Commissioner noted that DSG recognised the need to reduce the number of domain administrator accounts in 2016 but had not implemented this by the date of the Attack.

j. Failing to implement standard builds for all system components based on industry standard hardening guidance.

41. The Information Commissioner accepted that remedying the identified shortfalls would not necessarily have prevented the Attack but reminded himself that both DPP7 and the statutory conditions set out in s. 55A are concerned with measures being taken to reduce the exposure of personal data to serious risks. He concluded that each of the 10 deficiencies he had identified were a breach of DPP7 and that, cumulatively, they met the s. 55A conditions for the imposition of an MPN.

42. The Information Commissioner then assessed the seriousness of the contraventions. He concluded that all of the deficiencies identified had persisted over a relatively long period of time. He further concluded that the amount of personal data held on DSG's systems was significant, and that the volume of financial personal data and other personal data affected by Attack increased the seriousness of DSG's contraventions of DPP7.

43. The Information Commissioner noted that the ICO had received 158 complaints from DSG customers about the data breach, and that DSG had also been contacted by 3303 of the customers it had notified of the potential data breach. He further noted that approximately 85 of the payment cards affected by the Attack had been used in a potentially fraudulent transaction in a UK supermarket which allowed payments to be made using only the PAN and expiry date. The Information Commissioner concluded that the contraventions he had identified were of a kind likely to cause substantial damage and distress, particularly as the resulting risk exposed the personal data to a potential cyberattack with resulting criminal use.

44. The Information Commissioner decided that DSG knew or ought to have known of the risks arising from the inadequacies of its technical and organisational measures. Having considered the mitigation put forward by DSG and reconsidered the aggravating features he had identified, he concluded that it was reasonable and proportionate to impose the maximum penalty permitted under the legislation, which is £500,000.

E: Grounds of Appeal

45. DSG challenges the MPN on a number of grounds, summarised as follows:

    a. The technical and organisational measures DSG had in place were adequate and to the standard required by DPP7.

    b. The Information Commissioner's decision to issue the MPN was flawed because:

        i. He failed to adequately consider any of new information, provided by DSG in response to the NOI, relating to the identified contraventions;

        ii. He failed to consider, on a collective basis, the technical and organisational measures DSG had in place, and failed thereafter to assess whether DSG could have rationally considered these to be appropriate measures for the purposes of DPP7. The Information Commissioner concentrating instead on isolated weaknesses in DSG's systems.

iii. He also 'second-guessed' DSG's decisions in relation to the appropriateness of the technical and organisational measures it had in place, substituting his own judgement on appropriateness for that of DSG. He also did so to a large measure through the application of hindsight, informed by the post-Attack investigation (the 'A' report).

c. The Information Commissioner was also in error when concluding that the PAN and expiry date of payment cards constitute personal data in their own right, and when concluding as a consequence that the risks arising from the unlawful processing of this category of personal data aggravates the seriousness of the contraventions of DPP7 identified in the MPN. In DSG's view, only the 8,628 non-EMV payment cards accessed by the Attackers could conceivably meet the definition of personal data.

d. In the alternative, even if the technical and organisational measures in place contravened the requirements of DPP7, the Information Commissioner was wrong to conclude that the statutory conditions in s. 55A were met for the imposition of an MPN. This is because:

i. Any contravention of DPP7 by DSG did not meet the threshold of being a 'serious contravention';

ii. And/or any contravention of DPP7 that took place was not of a nature likely to cause substantial damage (interpreted in this context as constituting financial loss as per *Information Commissioner v Neibel [2014] UKUT 0255 (AAC)*) or substantial distress (interpreted, by virtue of same authority, as being more than mere annoyance, inconvenience, or irritation);

iii. And/or the Information Commissioner failed to apply the appropriate legal test when deciding whether DSG had knowledge of each contravention and/or failed to take reasonable steps to address them. DSG's systems, if assessed overall, were compliant with DPP7 and it was moreover engaged in a significant programme of security improvement at the time of the attack.

e. Again, in the alternative, if the statutory conditions in s. 55A have been met in this case, the approach taken by the Information Commissioner to determine the quantum of the financial penalty was unlawful, with regard to the approach he took to the statutory maximum and his failure to comply with his own published policy.

F: The Information Commissioner's amended position

46. At an early stage in these proceedings DSG applied to the Tribunal for a disclosure order in support of a Request for Further Information. This had broadly been made in relation to ground of appeal b(ii). This application was largely granted following a preliminary hearing.

47. Following a further exchange of correspondence and expert evidence, the Information Commissioner has amended keys aspects of his case in relation to some of the contraventions identified in the MPN. In particular:

    a. He accepts that the reasons given in relation to contravention 1 were flawed. His amended position is that network segregation would have made the Attack more difficult and would have been a quick measure for DSG to adopt.

    b. He accepts that his explanation in relation to contravention 2 is also flawed, in that it is no longer his case that no local firewall was installed on the POS terminals, or that host level firewalls are a requirement of PCI-DSS compliance.

    c. He no longer no longer relies on contravention 10.

48. At the conclusion of oral evidence, the Information Commissioner further narrowed the scope of his case from that set out in the MPN:

    a. In relation to contravention 6, he now accepts that responsibility for logging and monitoring within DSG's server and data centre environment was carried out by a contractor on DSG's behalf. He still maintains that there was a deficit of logging and monitoring in the POS environment for which DSG was responsible.

    b. In relation to contravention 2, he no longer maintains that a second firewall provided by native software was required in the POS terminals. However, on the basis of the 'B' report he questions whether the firewall installed was running consistently.

    c. Similarly, in relation contravention 5, the Information Commissioner's case is now limited to whether the whitelisting software installed on the POS terminals was running consistently.

49. The issue of whether the Information Commissioner should be permitted to further amend his case in relation to contraventions of DPP7 was raised at the hearing. Mr Pitt-Payne directed us to the Court of Appeal's guidance in *Birkett v IC and DEFRA [2011] EWCA Civ 1606, [2012] PTSR 1299,* in particular at ¶*28.* Although concerned with a different regulatory framework, the Court decided that further modification of a regulator's case after service of the Response was permitted but required the permission of the Tribunal who would need to use case management powers to amend the requirements of the Tribunal's Procedure Rules. We adopted the same approach and, having considered and applied the overriding objective, decided that the Information Commissioner should not be permitted to amend his response further at such a late stage.

G: Evidence

50. Both Parties have provided a large volume of documentary evidence supplemented by oral evidence. We have had regard to those parts of the bundle to which we have been

directed and have paid careful attention to the evidence and opinions of expert witnesses. For reasons of brevity, we have only referred in detail to those parts of the evidence we consider to be particularly relevant.

51. We heard oral evidence from 3 non-expert witnesses. The first was Mr Naveed Islam, who was Head of Security Strategy for the Dixons Carphone plc group between 31 January 2017 and 31 December 2020. Prior to that he had advised the group on a consultancy basis.

52. Mr Islam explained that PCI-DSS is the main standard for organisations who process, transmit or store payment card data, and comprises 12 requirements which Mr Islam described as 'prescriptive'. He described PCI-DSS audits as being binary in nature, in that any organisations that fails to meet all 12 requirements will be assessed as being non-compliant. Mr Islam took issue with the approach taken by the Information Commissioner in the MPN to PCI-DSS compliance, and to whether it should be used as an indicator of whether appropriate technical and organisational measures were in place for the purposes of DPP7. He explained how, in his experience, it was possible for retail businesses to operate with an appropriate level of security whilst not meeting all PCI-DSS requirements.

53. Mr Islam also explained in detail the security upgrade programme being undertaken by DSG at the time of the Attack, which was known internally as the Flint Programme. He described the extensive resources that DSG were directing to the programme, and its objective of becoming a market leader for IT security. He further described the systems of internal governance adopted for the Flint Programme which were perceived as being key to success. These included a senior governance committee that met for monthly Information Data Security Protection ('ISDP') meetings. Mr Islam only attended this meeting when specifically required. He did so in November 2017.

54. Mr Islam also described the remedial actions taken by DSG after it has been notified of the Attack, and then in response to the 'A' Report. He explained that the vulnerabilities that were identified after the event as having been exploited by the Attackers addressed as a priority. However, he did not accept that all of these security actions could and should have been carried out as a priority in any event, irrespective of whether the Attack had taken place. He stated that these remedial steps were taken post-Attack because at that stage 'the platform was on fire.'

55. The second witness was Mr Elliott Frazer, who is the Head of Business Standards and Data Protection Officer at Dixons Carphone Plc. He set out the steps taken by DSG when it learned of the Attack and gave evidence about the various batches of data that were accessed by the Attackers.

56. Mr Frazer explained how the ICO was notified of the Attack and how DSG responded to the Information Commissioner's investigation, responding to over 200 queries. He explained how DSG communicated with customers about the data loss and decided in due course to alert all of its 25 million customers, even though a much lower number were known to have been affected. He stated that this decision was taken out of an abundance of caution.

57. Finally, Mr Frazer explained that at the date of the MPN DSG had received 3,003 responses from customers in relation to the Attack, not all of which were either negative or could be classed as complaints.

58. We heard from Mr Romeen Partovnia who is a member of the Information Commissioner's Cyber Investigations and Incident Response Team. From previous employment he has 18 years' experience of managing, maintaining, and securing IT networks. From March 2019 Mr Partovnia was given responsibility for much of the technical aspects of the Information Commissioner's investigation of the Attack. He produced an Enforcement Report upon which the MPN was based, which recorded 158 complaints made to the ICO in relation to DSG's data breach. He explained that this was one of the highest numbers of complaints in relation to a breach of which he was aware.

59. Mr Partovnia's view of the seriousness of the Attack was based in part on his understanding that the PAN accessed by the Attackers were personal data. However, he also took into account the fact that 10 million other personal data records had been affected. He concluded that DSG had contravened DPP7 in the manner set out in the MPN, relying to a large extent on the B Report. Some of Mr Partovnia's conclusions in relation to the technical and organisational measures adopted by DSG were based on an understanding that the status of the devices tested for the purposes of the B Report reflected the status of devices across DSG's IT estate.

60. Mr Partovnia further concluded that DSG should have adopted additional measures, as set out in the MPN. He accepts that non-compliance with PCI-DSS standards does not necessarily equate to a breach of DPP7 obligations, but he considers this to be a helpful tool when assessing the security of payment card data.

61. From his reading of the evidence Mr Partovnia concluded that the Attack had been initiated shortly after DSG had been alerted to the existence of critical risks by the B Report. In his view, some of these critical risks would have been relatively simple for DSG to rectify.

62. We also heard evidence from three expert witnesses. Professor Paul Dorey is an expert in cyber and information security. He was instructed by DSG in relation to the findings in the MPN. His report notes a significant difference between the Parties in terms of what constitutes appropriate security levels. He described a 4-stage model of information security maturity and assessed DSG's security standards in 2017 as having met the second of these stages, starting on the third.

63. His opinion of DSG's information security is based on a range of factors, including internal governance structures, the recruitment of suitably expert staff, and the use of external security service providers.

64. Professor Dorey comments favourably on DSG's long term security transformation programme and of the decision taken to prioritise the transformation of e-commerce systems over POS terminals. In his view this was a reasonable approach to take in light of the wide adoption of EMV protection for payment cards in the UK.

65. He describes the challenges of transforming a large and diverse IT estate of the nature of DSG's and notes that implementing several of the measures described as shortfalls in the MPN would be complex task. He observes that managing a robust privilege management programme in an IT estate of this size would be complex and was, in this case, largely in the hands of a 3rd party security service provider.

66. Professor Dorey reviews and disagrees with many of the contraventions outlined in the MPN. In particular:

    a. Contravention 1: he notes that there is generally low take up of the network segregation arrangements advocated by Microsoft due to complexity and expense.
    b. Contravention 6: he assesses the standard of DSG's logging and monitoring programme as meeting or being better than the standards he would have expected for the retail sector in 2017.

67. Professor Dorey disagrees with Mr Partovnia's assessment of the sophistication of the Attack. In his view, the Attackers demonstrated a high level of sophistication, including in relation to the measures they took to cover their steps. He notes that, according to the 'A' report and contrary to the chronology assumed by the Information Commissioner, the Attack had already begun by the date of the 'B' Report's penetration test. In his view, "*once they had access, the attackers discovered and took advantage of a mistake following a specific security patch remediation. The post remediation action was not fully completed which left readable password data in a user accessible 'Group Policy' store. This enabled the attacker to discover the password for a privileged account which then gave them widespread access to the DSG IT environment, including the ability to bypass technical security controls."*

68. At paragraph 8.102 of his report Professor Dorey endorses the Information Commissioner's focus on the issue of patch security, particularly in light of his conclusions about the use to which the related failure to delete administrator passwords from the Group Account appears to have been put by the Attackers.

69. We also heard from Professor Steven Murdoch, who is an academic expert in the security of payment card data. He was instructed by the Information Commissioner to address issues relating to whether payment card data comprises personal data. In essence, his evidence explains the way in which payment cards function and the different types of data used by the payment card system.

70. In Professor Murdoch's view, a malicious actor would sometimes be able to use a PAN and expiry date to purchase goods and services and could link it with other available information to extract information about the customer to whom the card belongs. Further, in his opinion a PAN and expiry date are not anonymised data. He also explained how a dataset obtained from DSG containing only PAN and expiry dates could be used to refresh an older dataset containing PAN and other personal data.

71. Finally, we heard from Mr Benn Morris, an expert on cyber security. The focus of his evidence is mainly on the use that could be made of PAN and expiry dates by an attacker with access to other data sets. Mr Morris also provides an expert view on various types of payment cards and the security aspects of each.

72. In Mr Morris's view, a PAN and expiry date cannot be linked back to an individual by themselves. He also describes the difficulties that would be encountered when attempting to link a PAN with another data set. In his view the risk of fraud arising from DSG's loss of PAN data is minimal.

73. The experts further assisted the Tribunal with the production of a joint experts' report. This focuses on the data present on EMV-capable cards, the risk of counterfeiting; information that can be obtained and purchases that can be made using a PAN and expiry date; and the extent to which a PAN can be matched with other information. The joint report also considers an academic paper which deals with some of the above issues. The witnesses agree that, because the PAN is a unique identifier, it can be used as a common reference point between two datasets if both contain it.

74. Although we were greatly assisted by these witnesses, given our findings below on the basis upon which PAN should be considered personal data for the purposes of this appeal, we do not consider it necessary to review this expert testimony in any further detail

F: Submissions

75. Mr Lockley submits that the standard of technical and organisational measures DSG is required to have in place is an objective matter. His position is that the Tribunal's jurisdiction is to determine the question of DSG's compliance with DPP7 afresh. He accepts that DSG has a degree of latitude in deciding how the standard is to be met but contends that the appropriateness of measures must be determined objectively by considering firstly any harm that might arise from unauthorised processing of the personal data and secondly the nature of the data being processed. The more sensitive the data, the more significant the security measures required in relation to which the issue of cost is only one factor. He submits that DSG's aim of introducing P2Pe in 2018 was a laudable aim., but that DPP7 required further measures to be put in place in 2017, to ensure security in the interim. The fact that additional measures were put in place quickly after the Attack demonstrates the fact that they were steps capable of being taken quickly.

76. In Mr Lockley's view, in the modern world financial activities are a fundamental part of an individual's identity. He submits that a PAN is personal data where it identifies an account which is a unique identifier of an individual whose identity is singled out by virtue of their financial activities and the money available to them Alternatively, he submits the PAN, whether with or without the expiry date, can be combined as part of a 'mosaic' when considered with other information reasonably likely to be available that will enable to indirect identification of an individual. He focuses on such additional information that might be available to a motivated 3rd party intruder, citing caches of personal data available on the dark web against which the exfiltrated PAN and expiry dates could be matched, and addressed us in detail on five methods that could be used by a 3rd party to achieve a match

77. If the Tribunal accepts that the PAN are personal data, then in Mr Lockley's submission the PCI-DSS standard provides a helpful benchmark of the appropriate standard of security appropriate for data of that nature, one which DSG had failed to

reach. Mr Lockley further relies on the National Cyber Security Centre's Cyber Essential Guidance as representing a minimum standard of acceptable IT in internet-facing areas, and on the admission by Mr Islam that these were also not fully met by DSG's measures.

78. In relation to the B Report, Mr Lockley's case is that this still provides an informative snapshot of DSG's IT systems at the relevant time. It was commissioned to as closely as possible replicate store conditions, and with the aim of providing information to support business decisions. Therefore, to the extent that the B Report identified anything as not performing consistently, this is an indication of inconsistent performance cross the IT estate. Further, the B Report put DSG on notice of critical vulnerabilities such as software patching issues, and these were highlighted again in a further report the next year.

79. Mr Pitt-Payne's submissions largely follow the grounds of appeal. He submits that the issue of DSG's compliance with DPP7 should be approached from the perspective that a wide margin of discretion is afforded to the data controller and the Tribunal's role being confined to an assessment of rationality.

80. Mr Pitt-Payne's case is that the approach taken by the MPN is fatally flawed since it assumes a PAN and expiry date is personal date. In his view a PAN is not personal data because it identifies a bank account, which is not data from which an individual is directly identifiable. He likens a PAN to a cloakroom ticket which, if found, will identify a coat but not the owner. He accepts that the risk of a 'mosaic' identification was not part of the MPN and was put forward by the Information Commissioner only in outline in the course of these proceedings. Mr Pitt-Payne describes the suggested possibility of matching PAN to other datasets as highly speculative ad without evidential support in these proceedings. He challenges the extent to which any of the necessary datasets would be available from a cost-effective source to even a motivated criminal.

81. He maintains that the contraventions of DPP7 identified by the Information Commissioner have been arrived at by way of a substitution of judgement, and by way of hindsight following knowledge of the Attack. He challenges the reliance on both the B Report and on DSG's failure to meet PCI_DSS standards at the time of the Attack. In Mr Pitt-Payne's view, none of the absence of measures still relied upon by the Information Commissioner are contraventions of DPP7 and/or and any finding by the Tribunal of a failure to take appropriate measures amounts to an isolated and specific error.

82. In relation to the requirements of s.55A, Mr Pitt-Payne submits that the absence of evidence of successful fraud as a consequence of the Attack should be taken as an indication that there was no risk of substantial damage. Similarly, the relatively small number of the 25 million people who made a complaint following notification of the Attack should be taken as an indication that there was no risk of substantial distress.

83. Finally, rt Pitt-Payne relies on the extensive IT security measures being undertaken by DSG, including vulnerability scanning, as an indication that it was taking appropriate steps in relation to any risks about which it knew or ought to have known. He further contends that the Information Commissioner's approach to deciding when to impose

the maximum penalty was flawed, failed to consider DSG's mitigation and incorrectly took into account a previous penalty imposed against Carphone Warehouse.

I: Findings of fact and reasons

84. In accordance with the principle identified in *Hope and Glory*, we have considered what weight to attach to the reasons given by the Information Commissioner when issuing the MPN. We note that key aspects of the contraventions of DPP7 are no longer supported because, quite properly, he has reviewed his position as further evidence has been presented to him. However, the extent to which the Information Commissioner's case has been refined is unusual and significant. One contravention has been abandoned and the scope of others has been narrowed to the extent that the Tribunal is now asked to decide simply whether certain applications on the DSG IT estate were switched on and functioned consistently.

85. In respect of his amended case, we have had regard to the fact that the Information Commissioner is the regulator entrusted by Parliament with the protection and enforcement of important public interests relating to personal data. As such the Tribunal should be slow to interfere with the exercise of his regulatory judgement, including in relation to his assessment of the appropriateness of a penalty issued in accordance with the published Regulatory Action Policy. We further note the Information Commissioner's finding in the MPN, which remains the subject of this appeal, that *'[t]here were a number of distinct and fundamental inadequacies in the security arrangements for DSG's system. As explained above, each of the itemised inadequacies would themselves have constituted a contravention of DPP7. Cumulatively, this multi-faceted contravention was particularly serious. The problems were wide-ranging and systemic, rather than single isolated gaps in an otherwise robust package of technical and organisational measures*."

86. We note that this was the basis upon which the quantum of the MPN was determined. We further note the decision maker's comment in the context of the penalty setting meeting that the contraventions identified in the MPN were such that the imposition of a higher penalty would have been appropriate, had this been permitted by under the legislation. This view was necessarily based on the Information Commissioner's case at that time.

87. Having considered the evidence to which we have been directed, and the extent to which the alleged contraventions in the MPN have been modified, we are satisfied that not all of the security shortfalls itemised in the MPN can be described as '*distinct and fundamental inadequacies in security arrangements'* or indeed as contraventions of DPP7. We therefore find that the MPN under appeal is not in accordance with the law and that the Tribunal's decision should serve as a substitute notice.

Relevant personal data

88. We find that approximately 18.5 million records of largely non-financial personal data records were accessed by the Attackers when they took steps in relation to Batches 2, 3, 4.1 and 4.2. These comprised names, addresses, postcodes, email addresses, dates of birth, telephone numbers, details of failed credit checks (Batch 3), partially concealed

PAN in a context where the PAN was linked with other personal data (Batch 4.1) and bank account details (Batch 4.2).

89. We have arrived at the figure of approximately 18.5 million in reliance on DSG's written submissions, which we have taken to represent the most current assessment of the Attackers' activities. We note that the MPN mentions only briefly the loss of non-financial personal data, at paragraph 16(3). This refers to 10 million records, plus an additional 2.9 million records that were likely to have been exfiltrated, along with 73% of a database containing 4.7 million records (which presumably means approximately 3.4 million additional records). It seems likely that paragraph 16(3) reflects the Information Commissioner's understanding of Batches 3, 4.1 ad 4.2 at the date of decision. The total number of personal data records reflected in paragraph 16(3) is approximately 16.3 million.

90. We therefore conclude that approximately 2 million more personal data records were accessed by the Attackers than were known of at the date of the MPN. We have had regard to the fact that all of the figures before us are approximate and may well involve some duplication of personal data records as between the various Batches. Nevertheless, we are satisfied that a very substantial volume of non-financial personal data was unlawfully accessed as a consequence of the Attack.

PAN

91. We have been asked to consider whether the PAN scraped from the POS terminals (i.e., Batch 1 records) are also personal data.

92. We conclude that, in the context of these proceedings, any PAN that identifies the bank account held solely by a living individual are personal data for the purposes of DPP7. This is because we are satisfied, on the balance of probabilities, that a living individual can be identified indirectly from the PAN held by DSG when combined with additional information which is also in the possession of, or reasonably likely to come into the possession of, DSG.

93. The reasons for these conclusions are as follows:

    a. The primary definition of personal data, set out in s. 1 of the DPA, read with Recital 26 of Directive 95/46/EC, is data from which a living individual can be identified either directly, or from those data and other information, which is on the possession of, or likely [reasonably] to come into the possession of, the data controller or a third party. Thus, distilled from the relevant legislation and Upper Tribunal Judge Jacob's approach in *NHS BA,* there are 3 limbs to the definition of personal data:
        i. Data which identifies a living individual directly;
        ii. Data which identifies a living individual indirectly when combined with other information in the possession of (or likely reasonably to be in the possession of) the data controller; and
        iii. As (ii) but where the additional information is or is likely reasonably to be in the possession of a 3rd party.

b. The Parties' submissions concerning the PAN have focussed mainly on limbs (i) and (iii). They disagree as to whether the PAN directly identifies a living individual (the 'cloakroom ticket' argument in relation to identification of an account); or, in the alternative, whether a living individual could be identified indirectly from the PAN when combined with other information that is [reasonably] likely to come into the possession of a third party such as the Attackers. Less attention has been paid to limb (ii).

c. One of the purposes of the DPA is to create legal rights and obligations relating to personal data that are enforceable against the data controller. Unless exempt by virtue of s. 27(1), s. 4(4) requires a data controller to comply with all data protection principles in relation to all of the personal data in respect of which they are the data controller. In short, a data controller has obligations in relation to the personal data they are processing. None of the authorities to which we have been directed suggest that these obligations do not apply to data which is personal data when in the hands of the data controller, but which ceases to be personal data when in the possession of a 3rd party.

d. The fact personal data may be anonymised to the extent that it becomes 'vanilla data' if or when it is published to the world at large, for example following an information request made pursuant s. 1 FOIA, does not preclude the data meeting the definition of personal data whilst it remains in possession of the data controller, provided the data controller is reasonably likely to have other information with which the data could be 'de-anonymised'. Whilst FOIA understandably points towards the DPA and related authorities for its definition of personal data, the DPA's definition of personal data is not limited by the contextual considerations of whether data remains personal data following publication as a result of a FOIA request.

e. It appears to be uncontroversial that the Batch 1 data was scraped from the POS terminals. Mr Islam's evidence is that the PAN processed by the POS terminals was separated from other transaction data, including presumably the name on the payment card, and was transmitted outside DSG's IT domain for processing. He described this as a security measure introduced in part due to concerns about the risks inherent in the POS terminals' internet gateway.

f. However, it has not been suggested that DSG could not thereafter combine the PAN with other data from the transaction should the need arise. In our view and as a matter of common sense, there must be a range of business needs that might require the PAN of a card used in a transaction to be linked to other data in DSG's IT estate, for example when processing a refund to the payment card. Therefore, whilst we accept that there may be some PAN stored on some parts of DSG's IT estate that may have been incapable of being linked to other data records, we are satisfied that a significant proportion of the PAN being processed must have been capable for being linked to other data, if only to the other data from the payment card (which would necessarily include the cardholder's name) or with partial PAN. We note in this regard that Batch 4.1 data comprised 2.9 million records that included masked PAN stored in combination with records that are unarguably personal data and that Batch 1

also included data from 8,628 payment cards in relation to which the records comprised PAN, expiry date and card holder name.

94. We are therefore satisfied that at least some of the PAN processed by DSG was capable of leading to the identification indirectly of a living individual, when combined with other data reasonably likely to be processed by DSG. However, we cannot say definitively on the evidence before us how many of the PAN processed by DSG, or by the Attackers, could be combined with other information in such a manner. We therefore find only that some were so capable and make no findings as to quantity.

95. To clarify, our findings in this regard are not limited to a conclusion that the data in Batch 1 could have been combined with information from other Batches in order to achieve indirect identification. Mr Pitt-Payne objected in closing submissions to Mr Lockley putting such a case in cross examination, which he described as being a significant amendment to the Information Commissioner's case. We note that the Information Commissioner has previously raised as an issue in these proceedings the extent to which PAN could be matched to data from other Batches, primarily to data that contain partial PAN. More recently, , both Parties have focussed on the nature of a PAN once it has passed into the possession of 3rd parties, and on any consequent risks of harm. In our view this overlooks the fundamental purpose of the DPA and the Data Protection Principles, which imposes obligations on data controllers in relation to personal data when it is held by the data controller.

96. Put another way, the approach taken by the Parties in this case would, if taken to its logical conclusion, support a view whereby a data controller need only comply with DPP7 in relation to personal data that will continue to be personal data if and when it is unlawfully processed in isolation by a 3rd party. The fact that a record comprising personal data in the hands of a data controller will become purely 'data' in such circumstances must be relevant to any assessment of the risk of consequent damage and distress. However, this does not remove the requirement for appropriate technical and organisational measures to be in place in relation to the record while it remains personal data in the hands of the data controller.

97. Having concluded that at least some of the PAN processed by DSG were personal data pursuant to limb (ii), we have not gone on to consider whether, as a matter of principle, the PAN also meet the limb (i) definition of personal data. We note that this is the approach relied upon by the Information Commissioner in paragraph 16 of the MPN. Our preliminary view is that data comprising a unique identifier of a financial account is capable of meeting the limb (i) definition but that, in the context of this case, the limb (ii) definition is much more obviously appropriate and applicable. Similarly, we have not gone on to determine whether the limb (iii) definition also applies. Although we appreciate the submissions made with considerable force by both Parties and have considered with care the evidence of the expert witnesses, we are satisfied that no further findings are required. The central question we were asked to determine was whether DSG had obligations under DPP7 in relation to the PAN it processed. We have concluded that it did, for the reasons given.

98. The jurisdiction of the Tribunal, set out in s. 49 DPA, includes the review of any determination of fact upon which a notice has been based and the power to substitute such other notice or decision as could have been served or made by the Commissioner.

We have concluded that the approach we have taken to the identification of PAN as personal data should be substituted for that of the Information Commissioner in paragraph 16 of the MPN.

DPP7

99. We have considered whether the security measures in place at the time of the Attack were appropriate technical and organisational measures against the unlawful or unauthorised processing of personal data, having regard to the state of technological development at the time, the cost of implementing security measures and issues of proportionality.

100. We agree with and adopt DSG's position that the appropriateness of any security measures must be assessed globally, without the benefit of hindsight obtained once the Attack, and the vulnerabilities exploited by the Attackers, had been identified. We have instead considered what technical and organisational measures might rationally be considered by DSG to be appropriate in mid-2017.

101. We note Langstaff J's observations on DPP7 in *Various Claimants v Wm Morrisons Supermarkets plc [2018] EWCA Civ 2339* ¶*68:*

"…The mere fact of disclosure or loss of data is not sufficient for there to be a breach. Rather, "appropriate" sets a minimum standard as to the security which is to be achieved… the fact that a degree of security may technologically be achievable, which has not been implemented, does not of itself amount to failure to reach an appropriate standard: … a balance has to be struck between the significance of the cost of preventative measures and the significance of the harm that might arise if they are not taken"

102. We are satisfied that the issue of whether DSG's security measures met the PCI-DSS standard must be a relevant consideration in the context of DPP7 obligations but not to the extent suggested by the MPN. We note the binary nature of PCI-DSS compliance, and the variety of ways in which it may be achieved. We further note that the focus of PCI-DSS is the protection of financial data, rather than personal data in general. Given the holistic approach that should be taken to DPP7 compliance, allowing a degree of permissiveness in the exercise of judgement, we conclude that it must be entirely possible for an organisation to have in place appropriate technical and organisational measures for the purposes of DPP7 whilst simultaneously failing to meet the PCI-DSS standard, and vice versa.

103. We find that, at the time of the Attack, DSG had embarked on a long-term programme of updating and reinforcing IT security arrangements, one aim of which was to introduce P2PE across its domain. We accept Professor Dorey's opinion that the decisions made by DSG to prioritise certain areas of this work, including the decision to update e-commerce environment areas before the retail environment, was reasonable for the reasons set out in his report. Notwithstanding any residual risks relating to payment card data arising in the UK retail industry following the roll out of EMV protection, we conclude on the basis of Professor Dorey's evidence that DSG's prioritisation involved an exercise of judgement of the kind anticipated by the Court of Appeal in the *Morrisons* case. We are satisfied from the evidence before us that DSG

did so within a framework of appropriate internal governance and in reliance on appropriate expert IT security advice and support.

104. As already mentioned, and in accordance with the principle identified in *Birkett v IC and DEFRA,* we have only considered those contraventions of DPP7 identified by Information Commissioner in the MPN, as amended by his response and at the close of oral evidence.

105. We have in general preferred the evidence of expert witnesses on technical matters to that of Mr Partovnia, where these views have differed. As previously stated, there is little factual dispute between the Parties. At heart, the issues in this case concern technical matters of law and judgement relating to the appropriateness of various IT security measures. We have necessarily afforded greater weight to those witnesses with enhanced expertise in the latter.

106. We agree with Mr Pitt-Payne that, to some extent, the Information Commissioner's approach in the MPN was to substitute his own judgement as to the appropriateness of certain measures for that of DSG. The pitfall of such an approach is that requires the decision maker to have in their possession all of the contextual and technical information that was available to the data controller. It is apparent from the extent to which the Information Commissioner's case has been refined since the MPN was issued, and from Mr Islam's and Professor Dorey's evidence concerning the security upgrade programme, that this was not the case. In particular he has failed to give weight to the considerable resources being directed by DSG to upgrading IT security, to the challenge of introducing the additional measures the absence of which were identified as contraventions of DPP7 and to extent to which this was a matter of judgement to be exercised by DSG in accordance with the decision in *Morrisons*. Although this Tribunal has no role in the supervision of any regulator, in our view it may have assisted the Information Commissioner and his staff to have sought external expert views given the technical complexity of the information provided by DSG, particularly in response to the NOI.

107. We note that, at least on paper, Mr Partovnia appears to have approached the issue of DPP7 compliance from the perspective that the Attack itself was a contravention. We accept from his oral evidence that this does not reflect the approach he followed in practice.

108. We are satisfied that the remedial actions taken by DSG after the Attacker's activities had been investigated should not be viewed as indications that the failure to perform these actions prior to this was a contravention of DPP7. We accept Mr Islam's evidence that, by and large, the remedial actions were taken to protect a 'burning platform' in that it was now known that isolated vulnerabilities had been exploited. These actions mainly demonstrate the operation of common sense.

109. Having considered Mr Partovnia's written and oral evidence, we find that the Information Commissioner placed undue reliance on the content of the 'B' Report as providing an accurate picture of the security of DSG's IT systems. In fact, the authors of the 'B' Report specifically state the opposite, and we therefore conclude that the approach taken by the Information Commissioner aspects of the 'B' report was flawed. In particular, we are satisfied on the basis of Professor Dorey's evidence that key

functions of the POS terminals and laptops tested for the purposes of the 'B' Report were unlikely to represent those operating in DSG's wider domain.

110. We have approached this case on the basis that our jurisdiction is to carry out a full merits review of the Information Commissioner's decision. Although when doing so our task extends to considering globally the measures put in place by DSG, given the extent to which the case against them has changed in the course of these proceedings, for reasons of fairness we have made findings only in relation to the MPN contraventions upon which the Information Commissioner still relies.

a. Contravention 1: We note that this point was not raised with DSG in the NOI and find that the Information Commissioner's assessment of this potential contravention was based on incomplete information. We accept Professor Dorney's evidence that, for reasons of complexity and expense, there is generally low take up of the network segregation arrangements advocated by Microsoft by industry. We conclude as a consequence that neither the decision by DSG not to adopt this measure before the Attack, nor the decision to take remedial action afterwards, should be viewed as a contravention of DPP7 obligations.

b. Contraventions 2 & 5: we find on the balance of probabilities that the POS terminals operating within DSG's live IT domain had adequate, installed, and consistently run firewalls and whitelisting functions. We note from Mr Partovnia's evidence that the MPN assumed otherwise based solely on the 'B' Report. We find that the Information Commissioner failed to appropriately contextualise this evidence and that it is more likely than not that applications such as firewalls and whitelisting would be turned off for the purpose described by the experts as 'sandboxing' the devices whilst the penetration test was carried out.

c. Contravention 4: DSG accepts that, although work was underway with a 3rd party security company to manage and resolve issues with internal vulnerability scanning, no such scanning was performed in relation to the POS terminals. Mr Islam explained that this was due to priority being given to the data centre, an approach which Professor Dorey considers reasonable. We are satisfied that the approach taken by DSG was rational for the reasons set out in the expert report and did not amount to a contravention of DPP7.

d. Contravention 6: We note that Professor Dorey assesses the standard of DSG's logging and monitoring programme as meeting or being better than the standards he would have expected for the retail sector in 2017. We accept his opinion and conclude that the approach taken by DSG in this regard was not a contravention of DPP7.

e. Contravention 7: We note from Mr Islam's evidence that the decision to run outdated java software on the POS terminals was carefully considered by DSG and mitigations against the inherent security risks were put in place. These risks were highlighted by the 'B' Report. However, Mr Islam's oral evidence was that the decision to continue to run the software had been taken in consultation with DSG's external IT security contractor. As such we conclude that this was

an exercise of judgement by DSG of the nature anticipated in *Morrisons*. Given the consultation with an IT security expert and the reliance on mitigations, we find that the continued reliance on outdated software was not a contravention of DPP7 *per se* but must be a relevant factor when assessing the appropriateness of DSG's technical and organisational measures globally.

f. Contravention 8: We find that the approach taken in the MPN to the absence of P2PE at the time of the Attack was based to a large extent on the Information Commissioner's flawed approach to PCI-DSS compliance. We note that the introduction of P2PE was central to DSG's programme of security upgrade and find, based on Professor Dorey's evidence and for reasons already given, that the overall approach of DSG to the upgrade of security was rational. This applies equally to the approach taken to the introduction of P2PE, the absence of which we find does not by itself amount to a contravention of DPP7.

g. Contraventions 3 & 9: We find that DSG was made aware by the B Report that the DSG domain had not been updated with a number of software security patches, some of which were identified as critical. One such critical Microsoft patch from 2014 required a 2-stage process whereby, after application of the patch, the pre-existing administrator passwords had to be deleted from the Group Policy account. DSG accepts that the second step of the 2014 critical patch had not been carried out in May 2017 at the time of the B Report penetration test, which identified this failure as a recurring issue. Nor had the administrator passwords been deleted in November 2017, when Mr Islam reported to the ISDP.

h. We accept Mr Islam's evidence that responsibility for carrying out this action laid with the domain controllers, who were at the relevant time DSG's reputable external IT security contractor. However, we find, also on the basis of Mr Islam's evidence, that DSG remained accountable for the ongoing security of its IT domain, even though day to day responsibility for carrying out security functions such as patch management lay with the external IT security contractor.

i. We note Professor Dorey's view that "*maintaining up to date security patches is an important security requirement, particularly for the systems facing the external internet as vulnerabilities can bypass security controls."* We give appropriate weight to his opinion, given in oral evidence, that the number of critical patches identified in the B Report as outstanding would have been a source of concern to him, and to his description of this as an indication that an erratic patch solution was being applied within DSG's domain.

j. We further note Professor Dorey's agreement in cross-examination that, although the Attackers' initial method of access to DSG's domain remains unknown, once access had been gained, they took advantage of an error in security patch management and, specifically, of inadequate management of administrator passwords for the Group Policy account. Mr Islam also agreed that '*it was very likely that* [failure to delete the administrator passwords] *became one of the vectors of the Attack*.'

k. We note in addition that poor password practices were a risk identified in the B Report and, further, that Mr Islam confirmed that the password exploited by the Attackers did not comply with DSG's password policy, as amended in 2018.

l. There is no evidence before us of any risk assessment or decision(s) made by the ISDP or by any other internal DSG IT security body relating to the critical risks of security patch management and password practices, once these had been drawn to DSG's attention by the B Report and/or following Mr Islam's November 2017 report to the ISDP. The critical risk arising from the failure to properly execute the 2014 Microsoft patch was flagged to DSG in a second penetration test the following year. We note from his evidence that responsibility for oversight of the work of the external IT security contractors probably sat with a legacy Carphone Warehouse IT team rather than with the ISDP. However, we are nevertheless satisfied that senior managers at DSG were made aware at least twice that there was a critical security vulnerability in DSG's IT system arising from the approach being taken to patch management, and at least once that there was an issue with password policy. We find in addition that DSG was notified in this manner about the critical risk arising from the failure to complete required actions relating to the management of administrator passwords in relation to the 2014 Microsoft patch. We conclude that that, having commissioned the B Report for the purpose of identifying security vulnerabilities of this nature, there is a reasonable expectation that DSG should take positive steps to address as a priority any critical risks or systemic weakness identified.

m. We further conclude that, notwithstanding the complexity of the DSG IT domain and the challenges described of rolling out security patches across the entire estate, the approach within DSG to software patching and to the management of passwords/domain administrator password accounts amounted to a failure to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data. We have reached this conclusion having had regard to technological developments and the cost of implementation of appropriate measures required to address these security vulnerabilities. As a matter of common sense, we find that security patches are generated in response to known vulnerabilities. Further, and in the absence of evidence of any risk assessment, we are satisfied that any decision made by DSG in relation to adopting appropriate technical and organisational measures in this regard ought not to be viewed as an exercise of judgement of the nature anticipated in *Morrisons*, whether or not that decision was taken positively or default. We are satisfied that DSG's failure to take appropriate measures in relation to this risk was a contravention of DPP7 for which it is appropriate to hold DSG to account.

n. When reaching this conclusion, we have approached any evidence of use by the Attackers of the vulnerability created by the contravention as being solely confirmation of the potential risks. We are satisfied from the evidence before us that the Attackers were sophisticated criminals and that their ability to gain access to DSG's domain should not be taken as an indication that DPP7 obligations cannot have been met.

s. 55A DPA

111. We are satisfied that the contravention of DPP7 identified was a serious contravention of s.4(4) DPA, having had regard to:

a. The fact that the personal data of approximately 25 million individuals were stored on DSG's IT system at the relevant time;

b. The nature of this personal data, which comprised names, postal addresses, email addresses, dates of birth, and credit check information, as well as an unknown quantity of PAN capable of being used to indirectly identify a living individual, and

c. The reasonable expectation of individuals and society that a body of personal data of this nature would be adequately protected, given the potential consequences of unauthorised or unlawful processing.

112. We have considered whether this contravention was of a kind likely to cause substantial damage and/or distress. When doing so we have given only limited weight to the evidence and submissions before us relating to the actual number of complaints made by DSG customers, either directly to DSG or to the Information Commissioner. Although this evidence provides useful context, the test we must apply is whether the contravention was of a kind likely to cause substantial distress, not whether the Attack did so. We have concluded that the contravention was of such a nature, having regard to the range and volume of personal data held by DSG and the considerable worry and concerns throughout modern society about the risks of identity fraud.

113. In contrast to the approach taken in the MPN, we are not persuaded that the most significant risk arising from contravention was that of the fraudulent use of payment cards. We note from expert evidence that the use of PAN and expiry date alone provides only limited opportunity for unauthorised use. This appears to be reflected in the limited extent to which such data may have been used by the Attackers in this case. However, we find it more likely than not that individuals, whether customers or employees, who became aware that their names, dates of birth, addresses and email addresses had been accessed by a sophisticated criminal group would be caused substantial distress. As previously stated, we find in addition that, in relation to an unknown number of individuals, these records of personal data could potentially be linked to their payment card PAN, a circumstance we are satisfied is likely to compound feelings of distress. We therefore conclude that the personal data in relation to which this contravention occurred was of a kind likely to cause substantial distress both qualitatively and quantitatively.

114. We further conclude that, for reasons already given, DSG knew or ought to have known about the contravention and failed to take reasonable steps to ensure that the external IT security consultant were prioritising this critical risk. We find in particular that DSG ought to have known about the risks arising from this contravention since, before it became part of the DSG Group, Carphone Warehouse had been the subject to an MPN for similar contraventions including seriously inadequate software patching We are satisfied that DSG allowed the critical risks

relating to patch management and administrator password management to persist between from May 2017, even though this was highlighted as a critical risk in penetration tests carried out several months apart. Indeed, the vulnerability arising from the 2014 Microsoft patch remained largely unaddressed until remedial action was taken following the Attack. In making these findings we have borne in mind that the relationship between DSG and the external IT security consultant was contractual in nature and that the setting of priorities would generally be left to the contractor. Nevertheless, we are satisfied that the decision by DSG to allow a critical risk identified in the B Report to persist over time was a failure to take a reasonable step.

Imposition of an MPN

115. Having considered the applicable guidance produced by the Information Commissioner on the imposition of MPNs, we have concluded that it is appropriate to impose an MPN in this case for the following reasons:

a. We consider this contravention to be particularly serious given the nature personal data with which the contravention is concerned, and the number of individuals actually or potentially affected;

b. We have also considered length of time for which an approach of inconsistent patch management was allowed to continue within the DSG IT estate, notwithstanding the fact that it had been identified in penetration testing as a critical vulnerability; and

c. There was an obvious risk that the large volume of personal data held by DSG was of a kind likely to be targeted by a criminal attack, the consequences of which were more likely than not to cause substantial distress.

116. We have balanced these consideration against the fact that, at the time of the Attack, DSG was directing very substantial resources to the Flint Programme with the aim of upgrading IT security to an unarguably high standard, supported by a clear structure of internal governance. We note that DSG had also employed the external IT security specialist for the purpose of ensuring adequate IT security arrangements in the interim. However, for reasons already given we conclude that this arrangement did not abrogate DSG of responsibility for monitoring the extent to which the external specialist was meeting DPP7 requirements, especially in light of the B Report.

117. We have also taken into consideration the fact that the contravention we have identified represents a relatively small aspect of the absent measures identified and assessed originally as meriting the imposition of an MPN.

118. We have further considered the resources available to DSG and the likely financial impact of an MPN. We are satisfied that the imposition of an MPN will not result in any undue financial hardship or disproportionate reputational damage.

119. Having taken all of these matters into consideration we have decided on balance that the imposition of an MPN remains appropriate.

Aggravating features

120. We note again that the identified contravention is serious for reasons already given relating to the nature and volume of data processed by DSG and the number of individuals whose data was put at risk.

121. We are not persuaded that the number of PAN accessed by the Attackers is an additional, relevant consideration for the purpose of identifying the quantum of any MPN imposed in this context. As previously stated, we have concluded that the exact number of PAN meeting the definition of personal data remains unknown. Rather, we consider the overall volume of personal data, both financial and non-financial, which is known to have been unlawfully processed to be a more relevant consideration.

122. We note that Carphone Warehouse was the subject of a previous MPN in relation to a breach of personal data that took place in its online system. Although we have noted some similarities between that breach and the current contraventions, we accept that the Carphone Warehouse breach occurred before that company was part of the DSG Group., Given the precautionary step taken by DSG to use external IT security consultants to manage the Carphone Warehouse part of the IT estate, , we are satisfied that it would not be appropriate to treat the previous MPN as an aggravating feature in this case.

123. We note that the security vulnerabilities arising from the contravention were allowed to subsist for an extended period of time, after DSG had been made aware of them in subsequent penetration tests.

Mitigating features

124. We have considered the written mitigation put forward by DSG, set out in the bundle.

125. We are satisfied that the contravention occurred in the context of a substantial programme upgrading IT security and note again the decision by DSG to employ external IT security specialists, including for the purpose of penetration testing. We have concluded that DSG's approach to IT security at the relevant time was generally of a high standard, other than the failure to adopt appropriate technical and organisational measures which we have identified as being deficient.

126. We note the early, proactive steps taken by DSG to notify both the Information Commissioner and its customers of the potential data breach, including the decision by DSG to notify its full customer base, even though the personal data of only some of the customers were known to have been accessed by the Attackers.

127. We accept on the basis of Mr Frazer's evidence that DSG spent approximately £9million on its response to the Attack and that this reflects a generally appropriate prioritisation of IT security.

128. We note the extent to which DSG co-operated with the Information Commissioner's investigation, as set out in Mr Frazer's witness statement.

Quantum

129. We have considered the submissions of both Parties in relation to the appropriate quantum of any MPN. We have also considered the MPNs in the authorities bundle, imposed by the Information Commissioner in other cases.

130. We note that the highest penalty is generally reserved for multiple contraventions of DPPs and/or contraventions of DPP7 comprising several inadequacies. Neither consideration applies to our findings in this case.

131. Although the facts of this case have similarities with several of those included in the bundle, we consider the circumstances underpinning the MPN imposed against Yahoo UK Services Limited to be a useful starting point. In that case a penalty of £250,000 was imposed after personal data relating to approximately 500 million individuals were accessed in a criminal attack, exploiting the compromised credentials of employees. This did not involve the loss of any financial data.

132. We note that a significantly smaller number of individuals were affected by DSG's contravention, but that it subsisted for a longer period of time and contributed to the loss of financial personal data.

133. Having taken all relevant maters into account we conclude that the appropriate quantum of an MPN in this case is also £250,000.

Conclusions

134. The MPN imposed by the Information Commissioner on 7 January 2020 was wrong in law and is substituted by this Decision.

135. A Monetary Penalty in the sum of £250,000 is imposed on DSG pursuant to s. 55A of the DPA.

136. The Order under Rule 14 of the Tribunal's Procedure Rules is to remain in place indefinitely in order to preserve the security of DSG's IT estate.

Signed: Moira Macmillan

Upper Tribunal Judge
Sitting as a Judge of the First-tier Tribunal

Date: 5 July 2022

Promulgated: 6 July 2022