DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: DSG Retail Limited

Of: 1 Portal Way, London, W3 6RS

Introduction

1. The Information Commissioner ("the Commissioner") hereby issues DSG Retail Limited ("DSG") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA") because of a serious contravention of the seventh data protection principle ("DPP7") from Schedule 1 to the DPA.

2. The amount of the monetary penalty is £500,000.

3. This Notice explains the grounds for the Commissioner's decision to issue the monetary penalty. This Notice takes account of the evidence and submissions DSG provided in response to the Commissioner's Notice of Intent to issue a monetary penalty and seeks to set out the Commissioner's position in respect of the primary arguments advanced by DSG.

Legal framework

4. The DPA implemented European legislation (Directive 95/46/EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The DPA must be applied so as to give effect to that Directive. Both the DPA and the Directive have since been repealed, but the contravention at issue in this case took place while they were still in force.

5. DSG is a data controller for the personal data identified below. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which he is the data controller.

6. Schedule 1 of the DPA contains the eight data protection principles. In the present case, the relevant principle is DPP7, which stipulates as follows:

> *7. 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.*

7. As regards DPP7, the interpretative provisions in Part II of Schedule 1 to the DPA provide that:

> *9. 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.

8. Section 55A of the DPA empowers the Commissioner to issue monetary penalties. The relevant provisions are as follows:

(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.

(2) This subsection applies if the contravention was deliberate.

(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.

9. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

10. The Commissioner has issued and published statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties.

Background to the contravention

11. DSG Retail Limited is a private limited company which retails consumer electronic products, and operates under a variety of trading styles, including Currys PC World and Dixons Travel stores.

12. This Notice concerns an extensive compromise to DSG's computer system between 24 July 2017 and 25 April 2018. The compromise was brought to the attention of DSG through external intelligence received on 5 April 2018, which alerted DSG to a potential breach of its computer system.

13. Receipt of the above information prompted DSG to commission a specialist security response team (hereinafter referred to as "A") to provide it with incident response assistance in relation to the intelligence it had received, and in particular to investigate whether there had indeed been a compromise to DSG's computer systems. "A" confirmed that an attacker had compromised the DSG infrastructure and gained control of multiple domain administrator accounts.

14. Information provided by "A" revealed that unauthorised processing of personal data on DSG's systems took place between 24 July 2017 and 25 April 2018. During this period, malware installed by the attacker was running on 5,390 Point Of Sale ("POS") terminals in Currys PC World and Dixon Travel stores. POS terminals are where in-store payment is taken and so the attacker was able to collect payment card details for any transactions that used the POS terminals during that period. "A" was unable to say at that stage exactly how the attacker had infiltrated the system and explained this was because the sophisticated nature and duration of the attack limited evidence collection.

15. In the immediate aftermath of the attack both DSG and "A" were unable to definitively state what data, or how much data, was exfiltrated other than to describe a "significant amount of SQL database reconnaissance and data theft" relating to their investigation.

16. DSG later confirmed in evidence submitted with it's representations to the Commissioner's Notice of Intent (and which the Commissioner accepts), that at the relevant time (24 July 2017 – 25 April 2018) a total of 5,646,417 payment cards were affected.

(1) Of these, 5,529,349 were EMV (the global standard for chip-based card transactions) and chip and pin protected, from which the following information was captured:

- Primary Account Number ("PAN"); and
- Expiry date.

(2) 52,788 cards were non-EMV protected, most likely relating to data subjects outside the United Kingdon and European Union, from which the following information was captured:

- PAN;
- Expiry date; and
- Cardholder name (in respect of up to 8,628 cards).

The PAN identifies which bank the card belongs to and is unique to the card holder. In representations made to the Commissioner DSG opined that in the absence of cardholder name, the PAN did not constitute personal data in the hands of the attacker, on the basis that it did not enable the identification of the individual card or account holder. In effect it was was fully anonymised. DSG submitted that, in relation to PAN data, up to 8,628 unique names only were captured by the attacker,

which originated from the non-EMV protected cards. DSG's position therefore was that the extent of the personal data compromised in this incident was limited to that of the aforementioned 8,628 unique individuals. The Commissioner does not share this view. Following her own guidance[1] and consideration of the opinion of the Article 29 Working Party[2] on the concept of personal data, she maintains that the PAN alone does constitute personal data, and so her position is that the total number of affected cards (5,646,417) contained personal data at risk of being compromised by this incident.

(3) In addition to the financial personal data detailed above, DSG initially determined, on a worst case scenario, that approximately 10 million records relating to non-financial information including name, postal addresses, mobile and home phone numbers, email addresses, date of birth and failed credit check details were also breached from DSG's internal servers and exfiltrated. DSG later determined that a further 2.9 million records were likely to have been exfiltrated, along with 73% of a database containing 4.7 million records. DSG has not been able to confirm with any certaintly confirm how many data subjects these records concerned but estimated that in total they affected approximately 14 million data subjects.

17. The incident was contained once remedial measures were implemented by DSG from June 2018 onwards (see further detail below). It is understood the malware deployed by the attacker remained within

---

1https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/

[2] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf

DGS's network and continued to process personal data in an unauthorised manner until 25 April 2018.

18. DSG first notified the Commissioner that it had suffered a cyber attack on 8 June 2018. DSG subsequently updated the Commissioner on 13 June 2018 with further information about the breach, confirming that it had found evidence of unauthorised access to personal data. In view of the amount of individuals affected, and as the compromised data included payment card data, the Commissioner commenced an investigation.

19. The Commissioner has based her synopsis of this cyberattack on the technical information and accounts provided by DSG, including the investigation carried out on DSG's behalf after the attack by "A" and further evidence provided by DSG in it's representations to the Notice of Intent. The Commissioner has also considered a previous assessment by an information security consultancy (hereinafter referred to as company "B"), conducted between 9 - 11 May 2017. The scope of the assessment was a POS terminal security assessment and laptop build review, but also included commentary on general patch management, perimeter firewalls, Group Policy and server administration. The assessment identified a number of deficiencies in the technical provisions and security measures in place for DSG's systems at that time, and notably when the attacker was present in DSG's systems. The Commissioner remains of the view that based on the reports and her own analysis, the deficiencies in DSG's technical and organisational measures created real risks of such data breaches, and that they played an essential causal role in this particular incident.

The contravention

20. The material submitted by DSG, including details of "A's" investigation and the assessment by "B", together with further evidence provided in

its representations to the Commissioner, has informed the Commissioner's assessment of the technical and organisational measures that DSG had in place for its system up to 25 April 2018.

21. In making her assessment, in addition to consideration of the technical and organisational provisions within DSG's wider IT estate, the Commissioner has also taken account of the secure payment card standard developed by card schemes ("PCI-DSS"). Businesses taking card payments must adhere to relevant security requirements to be deemed "compliant" with PCI DSS, and its members reviewed annually. "B" conducted an assessment between 9 May 2017 and 11 May 2017 on the Dixons and Carphone POS terminals which concluded (in relation to POS terminals) that they were:

"susceptible to critical vulnerabilities that would allow an adversary operating on the internet to compromise the confidentiality integrity and availibility of these devices completely.....The integrity of these devices should not be relied upon... may not be compliant the requirements of the PCI DSS as relating to store networks and POS terminals".

As to the Commissioners reliance upon "B's" assessment, whilst the Commissioner accepts that PCI DSS compliance (or otherwise) is not in itself indicative of compliance (or otherwise) with the DPA, given that its primary purpose is to secure payment card data, she considers it helpful when determining what an "appropriate" measure of security is in relation to personal data processed by the payment card environment. Indeed, the Commissioner's own guidance states:

"Although compliance with the PCI-DSS is not necessarily equivalent to compliance with the GDPR's security principle, if you process card data and suffer a personal data breach, the ICO will consider the extent to which you have put in place measures that PCI-DSS requires particularly

if the breach related to a lack of particular control or process mandated by the standard."

22. Based on the factual matters set out above, the Commissioner's preliminary view is that, at the relevant time (i.e. over a significant period from 24 July 2017 to 25 April 2018), DSG contravened DPP7 in relation to its computer system and organisational measures in that:

(1) DSG's network segregation was insufficient. DSG confirmed that at the time of the incident its POS systems were not segregated from the wider DSG corporate network. Sufficient internal network segmentation could have contained the compromise to a particular section of the network. DSG used Microsoft operating systems for its POS systems. Guidance published by Microsoft in 2014 suggests that an organisation should consider whether POS devices should be part of retailer's production Active Directory forest or joined to a domain in a seperate forest. It says: "*In Active Directory a separate forest provides a security boundary between systems. This would prevent a compromise of AD in one forest from also compromising resources in the other forest*". The Commissioner considers in this case that this would be an appropriate measure;

(2) Furthermore, "B's" assessment confirmed there was no local firewall configured on the POS terminals. A local firewall could have prevented unauthorised access to the POS system, and unauthorised movement of data. Although DSG stated that it had firewalls enabled and running on it's wider system, Microsoft recommends: *"It's important to have Windows Defender Firewall on, even if you already have another firewall on. It helps protect you from unauthorised access."* In representations to the Notice of Intent, DSG contended that the presence of a local firewall

would not have averted this attack because the attacker had domain admin level access, and as such had the ability to log onto a server and reconfigure the rules. The Commissioner considers that the fact an attacker could circumvent the rules does not make the control any less appropriate. An effective firewall can be used collectively with other security controls to prevent an attacker from succeeding. Where an attacker has exploited another vulnerability in order to change the firewall, the attacker would be required to perform reconnaissance, log onto servers, make configuration changes and leave a larger footprint and forensic evidence, which would have increased the likelihood of detection by DSG. The Commissioner considers that DSG should therefore also have had measures in place to enable it to detect any unauthorised changes to a firewall. For these reasons the Commissioner considers a local firewall is an appropriate control that could have supported DSG in preventing a personal data breach, and the absence of a local firewall in this case exposed the system and its contents to significant risk;

(3) DSG's approach to software patching of its domain controllers and the systems used to administrate them was inadequate. Evidence provided by DSG in support of its representations to the Commissioner confirmed that as at May 2017 DSG's POS terminals were not compliant with its own patching policy, and were not fully compliant until November 2017 (following a patching review in August 2017). In this case it is suspected the attacker exploited an unpatched vulnerability in Group Policy (a Microsoft tool that allows centralised management of Microsoft settings) that allowed the retrieval of a domain administrator username and password. Storage of passwords in 'Group Policy' this way was a known vulnerability that Microsoft addressed in 2014 by releasing a patch which

required two actions – firstly to apply the patch, & secondly to remove existing Group Policies configured prior to application of the patch. DSG confirmed that it did not carry out the second action to remove the existing Group Policy until after the attack, in 2018. This meant that the vulnerability remained exploitable for four years, during which time the attacker was able to use extensively the account in order to compromise personal data held on the POS terminals. In addition, the assessment by "B" identified multiple instances of missing patches in some of the POS terminals. The Commissioner considers these are examples of systemic patch management failing which led to it processing personal data without an appropriate level of security measures.

(4) DSG confirmed that vulnerability scanning of the compromised environment was not performed on a regular basis, which prevented DSG from identifying vulnerabilities in its network, such as the unpatched vulnerability that the attacker exploited. That inadequacy materially exacerbated the data security risks of the system and enabled the attacker to exploit vulnerabilities that could have been detected and resolved before compromise.

(5) DSG failed to correctly manage application whitelisting across its full fleet of POS terminals. The assessment by "B" in May 2017 detailed inconsistency in enforcement of application whitelisting, with only one out of two terminals provided for review being configured with application control. Consistency in application whitelisting across all POS terminals would have protected the system from potentially harmful applications. In its representations to the Commissioner, DSG stated that [redacted] was running on it's POS systems, and in any

event the attacker was likely to have used its expertise to surpass DSG's whitelist blocking mechanisms. The assessment by "B" however recommended that application whitelisting policies available natively in the operating system were enabled in addition to the [redacted] product. This was not in place at the time of the attack or at the time of the personal data breach. As per (2) above, the Commissioner's position is that application whitelisting is one of a number of appropriate measures which can be used collectively with other security controls to prevent an attacker from succeeding.

(6) DSG did not have an effective system of logging and monitoring in place to identify and respond to incidents in a timely manner. There remains some uncertainty as to exactly how the attacker compromised the POS system and there were inadequate measures in place for overseeing access to the network. Such uncertainty was likely to create a security risk and to hinder the detection and investigation of any security incident;

(7) DSG did not effectively manage the security of its POS systems in that elements of its POS software were outdated. DSG provided information to the Commissioner that its POS system was a java based client-server application. The assessment by "B" confirmed that the affected hosts were running versions of java many years out of date (eight years in the case of the Dixons POS terminal) which the Commissioner considers would place the POS terminals at increased risk of compromise.

(8) Furthermore, DSG's outdated POS system did not support Point to Point Encryption ("P2Pe"), which is an effective control endorsed by PCI-DSS as a method of preventing the plain-text access of payment card data at the point of swipe (signature) or dip (chip and pin). In its representations to the Notice of Intent

DSG confirmed that P2Pe was in the course of being deployed at the time of the attack at significant cost, but felt its absence was not indicative of ineffective security. As per (2) above, the Commissioner's view is that P2Pe is one of a number of effective measures which when used collectively can prevent attacks succeeding, and whilst she accepts the cost of implementation is high, this should be weighed against the level of harm that might result from unauthorised processing of personal data. Her view is that in this case the cost of implementation of P2Pe was proportionate to the size of the business, the nature and volume of personal data being processed by it and the current standard of security at the relevant time.

(9) DSG failed to effectively manage the security of its domain administrator account in that it did not risk assess the addition of user accounts to the domain administrator group, and failed to adhere to its own policies in respect of access permissions and passwords. During 2016 DSG recognised that the number of domain administrator accounts could be reduced in line with best practises, however DSG has been unable to show that controls available to support the security of the account were implemented.

(10) DSG failed to implement standard builds for all system components based on industry standard hardening guidance. This would have reduced the networks surface vulnerability, thus reducing the likelihood of compromise.

23. Having regard to the state of technological development, the cost of implementing any measures, the nature of the relevant personal data and the harm that might ensue from its misuse, the Commissioner's view is that there were multiple inadequacies in DSG's technical and

organisational measures for ensuring the security of personal data on its system. The Commissioner has carefully considered the evidence and submissions provided by DSG. She has accepted some of the points DSG has made, but she remains mindful that DPP7 and the statutory conditions under section 55A are concerned with measures and the kind of contravention, rather than with any actual data breach. Therefore, even if the remedying of the deficiencies discussed in this Notice would not have precluded this particular attack, they nonetheless exposed the contents of the system to serious risks.

24. In the Commissioner's view, each of the itemised inadequacies listed above would have constituted a contravention of DPP7 in the circumstances of this particular case. The Commissioner has, however, assessed the arrangements in the round: on that cumulative basis, the Commissioner's preliminary view is that there was plainly a multi-faceted contravention of DPP7 in this case.

The issuing of a monetary penalty

25. The Commissioner's view is that the conditions for issuing a monetary penalty under section 55A have been met in this case.

26. The Commissioner considers that this contravention was serious, in that:

    (1) There 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.

(2) It is particularly concerning that a number of the inadequacies related to basic, commonplace measures needed for any such system. See for example the references above to the absence of network segregation, software patching, penetration and vulnerability testing, logging and monitoring, application whitelisting and privileged account management. DSG has submitted that, in taking this view, the Commissioner is imposing unjustifiably high standards of data security, by reference to industry norms at the relevant time, and that DSG's security inadequacies were isolated incidencies in an otherwise robust system. The Commissioner rejects that submission. The deficiencies set out in paragraph 22 represent appropriate measures that data controllers such as DSG should have had in place at the relevant time (mid-2017).

(3) These inadequacies appear to have persisted over a relatively long period of time, given how a foundation level of security standard could have identified and remedied them.

(4) The amount of personal data contained on DSG's systems and the number of affected individuals was significant, which increases the seriousness of DSG's data security inadequacies. DSG confirmed that in relation to financial data, a total 5,646,417 payment cards were affected. Notwithstanding DSG's submissions (which the Commissioner does not accept) on the extent to which these comprise personal data in the hands of the attacker (see para 16 above), the volume and breadth of financial personal data compromised is sufficient to increase the seriousness of its data security inadequacies. So too does the amount of non-financial personal data records (affecting

approximately 14 million data subjects) compromised from DSG's internal servers (paragraph 16(3) above).

(5) The Commissioner received a significant number of complaints in relation to DSG. In the five months between June 2018 and November 2018 the Commissioner received 158 complaints from DSG customers. DSG further reported that as of 14 March 2019 a total of 3,303 customers had contacted it directly in relation to this incident, either to seek further information, to make stand-alone comments and also to raise concerns. DSG submitted that there was lack of evidence to suggest that complaints it received were legitimate or had in fact manifested in actual distress. In relation to complaints made directly to DSG, it said: "*Some customers have contacted us and simply asserted that they have lost money as a result of the incident*". DSG went on to say that it is "*not always able to determine if these types of complaints are legitimate...*". The Commissioner accepts the possibility that some complaints made directly to DSG may not have a legitimate basis, however she maintains the sample complaints reviewed during the course of her investigation evidenced the distress this incident has caused and the worry of increased risk of fraud, and she is entitled to accept those complaints as genuine. The Commissioner further refers to her position as set out in paragraph 27 below.

(6) The attack to DSG's system had been ongoing for 9 months before it was detected. This gave the attacker ample opportunity to view and/or extract data prior to remedial measures being taken.

(7) The seriousness of the incident is heightened by the nature of the personal data involved, which was sufficient to render the

affected individuals susceptible to financial theft and identity fraud (see paragraph 27(1) below).

(8) As a large nationwide retailer, the Commissioner considers the general public would expect that DSG would 'lead by example' and to be sufficiently protected so as to avoid such systemic non-compliance.

27. The Commissioner considers that this contravention was of a kind likely to cause substantial damage or substantial distress, in that:

(1) The personal data that was put at risk as a result of this contravention is described at paragraph 16 above. A contravention involving personal data of those kinds, particularly payment data, was likely to be useful in terms of identity theft and fraud. DSG submitted in its representations to the Commissioner that 99% of affected payment cards were EMV and chip and pin protected and were not therefore susceptible to financial theft. The Commissioner rejects this proposition, on the basis of her understanding that EMV protection is only effective in 'card present' (i.e. in store) transactions, and not in 'card not present' transactions (i.e online or telephone). If any such outcomes had materialised (although there is no confirmed evidence this was the case here) substantial damage was very likely. Exposure to such outcomes (even if they did not materialise) was likely to cause substantial distress. Indeed, examples of complaints made to the Commissioner stated:

- *"I do not wish to take up any offers that Currys PCWorld may propose as they can't be trusted to hold the information thay already hold. I have lost all faith and*

trust in this company and I am distressed and worried about what information is floating around about me and for how long this has been happening";

- *"What I am most concerned about is their carefree attitude in that they have lost my personal data – THAT CAN BE USED TO COMMIT FRAUD IN MY NAME!!!. That is the critical loss of data as well as the fact they cannot quantify it either";*

- *"I'm very disappointed to hear that my private data has been breached.....this is very distressing to me....".*

(2) Information provided to DSG from its acquiring bank indicated that approximately 85 cards had potentially been compromised and subject to fraudulent use in a UK supermarket which accepts payment cards without the CVV code. This analysis identified DSG as the common purchase point. Whilst common point of purchase analysis is a likely indicator rather than a definitive answer to the source of a breach, the Commissioner considers the establishment of a link between the compromised cards and DSG was more probable than not. The Commissioner noted that additional common purchase point analyses identified DSG as the potential source of fraudulent transactions, and other external analysis of published compromised card data available for sale on the 'dark web' also indicated links to DSG.

(3) Moreover, the non-financial personal data put at risk had a significant bearing on individual's privacy: for example, it contained their full name, contact address and telephone numbers, date of birth and detailes of failed credit checks. The

loss of control over such information of a private and personal nature was likely to cause distress to at least some of the affected data subjects. Some individuals may have suffered substantial distress.

(4) This contravention was of a kind that exposed personal data to the risk of cyberattack – as opposed, for example, to the accidental loss of data. Cyberattack invariably involves nefarious and criminal purposes. A contravention that exposed individuals to such consequences was of a kind likely to cause substantial damage and substantial distress.

(5) To whatever extent the attacker successfully removed personal data from DSG's system that data remains at large. This factor is likely to exacerbate the risk of substantial distress to affected data subjects.

(6) The Commissioner's position is that the statutory conditions under section 55A are concerned with whether the contravention was of a kind likely to cause substantial damage or distress. Therefore even if the amount of personal data extracted from payment card data and its associated risks was limited, as submitted by DSG, (but which the Commissioner rejects – see paras 16 and 27(1) above), the deficiencies in DSG's technical and organisational measures highlighted in this Notice nonetheless exposed the contents of the system to serious risks. The Commissioner notes that DSG does not appear to dispute that a significant amount of non-financial personal data records were also compromised which would render those individuals susceptible to identity fraud. The Commissioner considers that even if the damage or distress likely to have been suffered by each affected individual was less

than considerable, the totality can nevertheless be substantial. In this case, given the large number of affected individuals, cumulatively, the "substantial distress" threshold was clearly met in these circumstances.

28. The Commissioner considers that DSG knew or ought reasonably to have known that there was a risk that the contravention would (a) occur, and (b) be of a kind likely to cause substantial damage or substantial distress. She further considers that DSG failed to take reasonable steps to prevent such a contravention, in that:

(1) DSG is a large, well resourced and experienced data controller which handled large quantities of payment card data on a regular basis. It should therefore have been aware of the ramifications of cyber breaches where robust cyber security measures were absent, and was well placed to assess any weaknesses in its own data security arrangements and to take appropriate action.

(2) This is all the more so given that a number of the inadequacies related to basic, commonplace measures, the need for which should have been obvious to any data controller working with such IT systems (such as network segregation, local firewalls, adequate patching, up-to-date software, application whitelisting, regular vulnerability scanning and penetration testing, logging and monitoring). Had such measures been in place, this attack may well have been averted. In any event the absence of such measures created serious and avoidable risks to the contents of the systems.

(3) DSG was aware that its systems were processing payment card data as well as non-financial personal data for a large number

of data subjects. Given its size and prominence it should have appreciated that misuse of the personal data held on its system was likely to cause substantial distress and damage, including risks of fraud and identity theft. It ought to have understood its own IT and data architecture better, and then to have matched adequate security measures to that picture.

(4) DSG is registered as a data controller with the ICO and had access to the ICO Guidance on Information Security (Principle 7). This explains, for example, the need to tailor security measures in light of the context in which the personal data was being used. It is reasonable to consider that DSG knew that failure to address security issues could risk a contravention of the Act.

(5) The storage of passwords in 'Group Policy' (see paragraph 24(2) above) was a known vulnerability addressed by Microsoft in 2014 when it released a patch to resolve this issue. Microsoft announced this as an *"important"* update that should be applied at the *"earliest opportunity"* in order to be fully protected. DSG was clearly aware of the patch given that it took the first of two steps required for the patch to be effective. DSG however conceded that it failed to take the second of the two actions required, rendering this particular vulnerability exploitable for a further four years.

(6) The assessment of DSG's POS systems and user laptops carried out in May 2017 by "B" concluded that its POS systems were untrustworthy and also unlikely to be PCI-DSS compliant. DSG provided no evidence to show that it immediately resolved the risks addressed in "B's" report (which also included that detailed in (5) above), and continued to process personal data through

its POS systems. It was shortly after "B's" warning that the POS systems were compromised by the attacker. DSG submitted that the assessment by "B" was carried out in a limited and specific context in relation to its POS terminals, and was not generally indicative of DSG's overall IT estate. The Commissioners view is that it is likely, in view of the concerted nature of the attack, that the target of the attack was DSG's POS terminals, and so any prior assessment and recommendations made by "B" in relation to it's POS terminals are of direct relevance when considering the appropriateness of the measures DSG had in place at the time of the attack. The Commissioner notes DSG's submission that this particular attack was sophisticated, but this does not detract from the broader point that there were a number of serious deficiencies in DSG's technical and organisational measures, both in relation to its POS system, and its wider IT environment, and that those deficiencies should have been obvious to DSG.

(7) A significant number of measures and controls were implemented by DSG following notification of the attack described above, including account management, retail estate hardening, monitoring, vulnerability discovery and remediation, and deployment of missing patches. DSG has also confirmed that it has undertaken a program to roll out P2Pe, which was already in train prior to the attack. This shows that at least some these measures were readily achievable. At least some of these measures could reasonably have been in place prior to the incident as they are, in some examples, basic security measures. The Commissioner considers that by failing to fully implement basic good practice measures prior the incident DSG failed to take appropriate steps to prevent the contravention.

(8) Following the attack DGS's chief executive issued the following statement to its customers: *"We are extremely disappointed and sorry for any upset this may cause. The protection of our data has to be at the heart of our business, and we've fallen short here".* This statement is demonstrative of DSG's awareness that this contravention was of a kind likely to cause substantial damage or substantial distress.

29. For the reasons explained above the Commissioner is satisfied that the conditions from section 55A(1) DPA have been met in this case. She is also satisfied that section 55A(3) and the procedural rights under section 55B have been complied with.

30. The latter included issuing a Notice of Intent dated 5 August 2019 in which the Commissioner set out her preliminary thinking.

31. The Commissioner received representations and further evidence from DSG in response to the Notice of Intent, dated 17 September and 15 November 2019, and has taken these into account when making her final determination. The Commissioner has considered all the circumstances and has reached the view that it is appropriate to issue a monetary penalty in this case. That view is based on the multiple, systemic and serious inadequacies identified above, the likely consequences of such a contravention and DSG's culpability for it. The Commissioner has also considered the importance of deterring future contraventions of this kind, both by DSG and by others. The Commissioner considers that the latter objective would be furthered by the issuing of a monetary penalty in this case.

The amount of the monetary penalty which the Commissioner intends to issue

32. The Commissioner has considered the following mitigating features of this case:

(1) DSG submitted that it notified 25 million potentially affected data subjects of the contravention by email, and also via advertising. DSG advised it subsequently took further action to assist affected customers, including establishment of a call centre dedicated to attack related questions, procurement of credit monitoring services and working with its acquiring bank to mitigate potential customer exposure to financial fraud. The Commissioner notes however that it was unclear how effectively the offer of credit monitoring was communicated to customers as no communications she viewed contained this information, and on the basis only 25 customers took up credit monitoring. This approach taken by DSG was an industry standard approach to these types of situations and so the Commissioner has given only limited credit to DSG for its actions.

(2) It is not certain whether the compromised personal data was used for successful identity theft or fraud (though the Commissioner is mindful that the focal point for section 55A DPA purposes is the kind of contravention rather than the actual consequences of the contravention).

(3) DSG proactively notified the Commissioner of the attack and fully co-operated with the ICO and other relevant external agencies during the course of the investigation.

(4) Since discovering the attack DSG has made significant investment in its data security processes and systems including

the implementation of P2Pe (which was already in planning at the time of attack).

(5) The attack has adversely DSG's brand and reputation as a leading UK retailer.

(6) Reporting in the press ensured widespread awareness amongst data controllers of the vulnerabilities exploited in the attack and incentivised other data controllers to strengthen their data security.

33. The Commissioner has also taken into account the following aggravating features of this case:

(1) DSG's culpability is striking. At present, the Commissioner can see no justification or excuse for the extent of these systemic inadequacies on the part of a data controller of this size and profile.

(2) DSG did not proactively detect the security breach; it was first alerted to a potential breach 9 months after the system was initially compromised, during which time the attacker was able to operate undetected.

(3) The Commissioner has previously issued a monetary penalty to a subsidiary of Dixon's Carphone (Carphone Warehouse – January 2018) in respect of similar vulnerabilities (including absence of local firewall, inadequate patching, outdated software and inadequate vulnerability scanning, penetration testing and monitoring). Whilst this contravention took place prior to the issuing of the aforementioned penalty, the Commissioners' underlying investigation had already exposed many of the same inadequacies dating back to mid-2015.

34. Furthermore the Commissioner has also taken into account her underlying objective in imposing a monetary penalty notice, namely to promote compliance with data protection legislation. She considers that, given the nature, seriousness and potential consequences of the contravention arising in this case, that objective would not be adequately served by an unduly lenient penalty. Moreover, the Commissioner considers that the amount of £500,000 is not excessive: indeed, but for the statutory limitation on the amount of the monetary penalty, it would have been reasonable and proportionate to impose a higher penalty.

35. Further, she has considered DSG's financial position, as evidenced by its published annual accounts.

Conclusion

36. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£500,000 (Five hundred thousand pounds)** is reasonable and proportionate.

37. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **7 February 2020** at the latest. The monetary 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.

38. If the Commissioner receives full payment of the monetary penalty by **6 February 2020** the Commissioner will reduce the monetary penalty by 20% to **£400,000 (Four hundred thousand pounds).** However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

39. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

a) the imposition of the monetary penalty and/or;

b) the amount of the penalty specified in the monetary penalty notice.

40. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.

41. Information about appeals is set out in Annex 1.

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

- the period specified within the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;

- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and

43. the period for appealing against the monetary penalty and any In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary 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 7th day of January 2020

Signed [redacted]

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation 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:

GRC & GRP Tribunals
PO Box 9300
Arnhem House
31 Waterloo Way
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 monetary 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 (Information Rights) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).