DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: The Carphone Warehouse Limited

Of: 1 Portal Way, London, W3 6RS

Introduction

1. The Information Commissioner ("the Commissioner") hereby issues The Carphone Warehouse Limited ("Carphone Warehouse") 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 £400,000.

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 Carphone Warehouse provided in response to the Commissioner's Notice of Intent to issue a monetary penalty. This Notice seeks to set out the Commissioner's position in respect of the primary arguments advanced by Carphone Warehouse.

Legal framework

4. The DPA implements 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.

5. Carphone Warehouse 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 to 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.*

10. The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

11. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—
(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
(b) take reasonable steps to ensure compliance with those measures.

12. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless—
(a) the processing is carried out under a contract—
(i) which is made or evidenced in writing, and
(ii) under which the data processor is to act only on instructions from the data controller, and
(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

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. Carphone Warehouse describes itself as the largest independent telecommunications retailer in Europe. Its retail services cover a wide range of major telecommunications operators. Following a merger with Dixons in August 2014, Carphone Warehouse became a subsidiary of Dixons Carphone Plc.

12. This penalty concerns a specific Carphone Warehouse computer system (referred to here as "the System"), which is overseen by a specific division of Dixons Carphone. The System consists of a complex cluster of virtual servers hosting several internal and external websites, including e-commerce sites. The System was separate from the computer systems for Carphone Warehouse's retail outlets.

13. At the relevant time (July-August 2015), the System contained the following personal data:

    (1) Records for approximately 3,348,869 customers of a number of mobile phone service providers. Those records comprised: full name, date of birth, marital status, current and previous address, time at address, phone number and email address.

(2) Records for 389 customers across two other companies. Those records comprised: full name, date of birth, email, password, phone number and current address.

(3) Historic transaction details for the period March 2010-April 2011, spanning 18,231 payment cards. Those details comprised: cardholder name and address, card expiry date and card numbers (PAN, CID, CVC2, CVV2).

(4) Records for approximately 1,000 employees. Those records comprised: name, home postcode, work email address, work username, personal and work contact phone numbers, car registration numbers, department and line manager information.

14. Over the period 21 July-5 August 2015, the System was subject to an external cyberattack originating from an IP address in Vietnam, but subsequently using more than one IP address from more than one location.

15. The attacker made a scan of the System server using Nikto, a relatively commonplace penetration testing tool for testing security issues such as outdated software and other vulnerabilities. One of the vulnerable points was an installation of the content management system WordPress on one of the websites maintained on the System. That WordPress installation was considerably out-of-date, exposed to the internet, and suffered from multiple vulnerabilities. Carphone Warehouse initially indicated that one or more of these vulnerabilities were exploited by the attacker, but has since submitted that valid login credentials were used for the WordPress administrative account. The Commissioner accepts the latter point, but explains below why she does not accept that this absolves Carphone Warehouse in this case.

16. Via the WordPress installation, the attacker entered the system and uploaded "web shells" (described by Carphone Warehouse as "malicious plugins"), which were intended to provide the attacker with, among other things, basic file management and database functionality over the contents of the System.

17. The attacker was able to locate credentials in plaintext (i.e. information that was inadequately protected by encryption), which they used to search the local databases for information. The attacker accessed numerous databases, including those containing some or all of the personal data specified above, with the apparent aim of extracting as much information as possible. For example, the transaction/payment card information referred to above was located and accessed: it cannot be ascertained whether or not some or all of that information was indeed exported, but that is a very realistic possibility. The attacker also prepared and extracted a large file or files out of the network. The content of those files cannot be determined, but Carphone Warehouse worked on a worst-case assumption that they contained personal data exported from the System. The Commissioner agrees that this assumption was prudent and realistic: it is clear that the attacker viewed databases containing large amounts of personal data and then created files (the contents of which cannot be confirmed) which were then sent out of the system. The likely interpretation is that those files did contain personal data. At the very least, the attacker had access to and was able to view large amounts of personal data.

18. The attacker's decrypting activity alerted Carphone Warehouse staff to the breach. They took steps to put an end to the attack, which ceased on 5 August 2015. Carphone Warehouse then took remedial measures, referred to below.

19. The Commissioner has based her synopsis of this cyberattack on the accounts provided by Carphone Warehouse, including forensic investigation reports into the attack carried out on Carphone Warehouse's behalf by two specialist companies, (referred to here as F and I). She has also considered a third report compiled by an expert for the purposes of Carphone Warehouse's response to the Notice of Intent. That expert report comments on the reports from F and I as well as the points made in the Notice of Intent.

20. The report by I concluded that, while there was no single root cause of the attack, the attacker clearly had everything he needed to take hold of the System and extract a large amount of information quickly. The subsequent report by F identified a number of deficiencies in the technical provisions and security measures in place for the System. The expert report assists in understanding those reports and also the extent to which the deficiencies referred to in the Commissioner's Notice of Intent played causal roles in the attack on the System that prompted this supervisory action. Based on all of those reports and her own analysis, the Commissioner remains persuaded that, once the attacker entered the system through the vulnerable WordPress installation (albeit having used valid login credentials), he had everything he needed to take hold of the System and to access and extract large amounts of personal data quickly. She also remains of the view that deficiencies in Carphone Warehouse'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

21. The material submitted by Carphone Warehouse, including the three reports referred to above and Carphone Warehouse's submissions in response to the Notice of Intent, have all informed the Commissioner's assessment of the technical and organisational measures that Carphone Warehouse had in place for the System up to 5 August 2015.

22. Based on the factual matters set out above, the Commissioner's view is that, at the relevant time (i.e. over a significant period up to August 2015), Carphone Warehouse contravened DPP7 in relation to the System in that:

    (1) Important elements of the software in use on the System were many years out of date. The particular web application in use was released in 2010. The WordPress installation in use dated from 2009. More current versions were available, but Carphone Warehouse continued to use a version that was some six years old at the time of the attack. Although the WordPress installation was accessed with valid login credentials, the Commissioner's view remains that these software deficiencies made such an attack more likely, easier to execute and more fruitful for the attacker in terms of how readily he could take control of the System and access large volumes of personal data.

    (2) Carphone Warehouse's approach to software patching was seriously inadequate. Although a "Patch Management Standard" was in place, it was not being followed by the relevant business area. No measures were in place to check

whether software updates and patches were implemented regularly in accordance with Carphone Warehouse's policy.

(3) Carphone Warehouse's submissions have emphasised that the attacker entered WordPress with valid login credentials. There remains uncertainty as to how those credentials were obtained. Importantly, however, given that this WordPress installation was outdated and exposed to the internet – and that it could provide a potential point of access to the System more broadly – Carphone Warehouse needed to have rigorous controls in place over who had WordPress credentials, and it needed to have measures in place for detecting any unauthorised use of those credentials. It did not have such measures in place. This deficiency was likely to create a security risk and to hinder the detection and investigation of any security incident.

(4) Inadequate vulnerability scanning and penetration testing measures were in place at the time. The Commissioner understands that no routine testing procedures were in place. An internal scan was conducted on the first day of the attack (21 July 2015), but it failed to identify any vulnerabilities. This suggests that such scanning measures were insufficiently robust. Moreover, the Commissioner understands that no internal or external penetration testing had been conducted in the 12 months leading up to the attack.

(5) At the time of the attack, Carphone Warehouse had no Web Application Firewall ("WAF") for monitoring and filtering traffic to and from its web applications. The report by F states that having a WAF in place "would have most likely prevented the intrusion from occurring." Carphone Warehouse's subsequent

expert report contains the view that the lack of WAF would not have prevented this attacker's access via WordPress. Nonetheless, the absence of a WAF was a significant deficiency in Carphone Warehouse's technical measures for protecting the System and the personal data within it. The presence of a WAF may have assisted in this case, for example as a protection against Nikto scans or those of other tools commonly used by attackers, depending on configuration and ruleset. Even if that is not so, however, the absence of a WAF was nonetheless a notable departure from widely accepted security standards at the time of the incident, and it exposed the System and its contents to significant risk.

(6) None of the servers that make up the System had antivirus technology installed. This was contrary to Carphone Warehouse's policy to apply antivirus measures. Again, there appear to have been no measures in place to check whether policies were being followed in respect of such important and basic security measures. Again, the Commissioner accepts Carphone Warehouse's submission that antivirus measures would probably not have protected against this particular attack. As with the absence of a WAF, however, the absence of antivirus measures was nonetheless a notable departure from widely accepted security standards, and it exposed the System and its contents to significant risk. Furthermore, the Commissioner remains of the view that Carphone Warehouse had antivirus policies in place for good reasons and that it failed to ensure that antivirus measures were being applied to the System, or alternatively that a proper assessment was undertaken and the reasons for deviating from the policy were documented. This was a significant organisational deficiency.

(7) Although Carphone Warehouse's internal monitoring measures alerted staff to the attack, this only happened 15 days after the system was first compromised. This suggests that inadequate technical measures were in place for detecting attacks on or unauthorised entries into the System. That inadequacy materially exacerbated the data security risks of the system.

(8) The operating system on the servers making up the System all had the same root password which was known and used by some 30-40 members of staff. The password carried administrator rights. Carphone Warehouse's justification for allowing such wide-ranging access was insufficient.

(9) The system contained large volumes of historic transactions data, including full credit card details as outlined above. There was no good reason for the retention of that data. Carphone Warehouse has explained that an external developer had created – and then failed to remove – a temporary mechanism whereby access to that historical data was retained. Taken together, these points suggest that inadequate measures were in place to identify and purge historic data. The Commissioner accepts Carphone Warehouse's submission that credit cards typically expire in 3-4 years, meaning that the credit card data that was put at risk here was likely to have expired in 2014 or 2015. Her view is that this factor reduces the risks relating to this data to some extent, but not altogether.

(10) Carphone Warehouse has said that it was not even aware that this historic transactions and credit card data was held on the

System at the time. This suggests that Carphone Warehouse had an inadequate understanding of its IT systems architecture, at least in terms of the locations of personal data on those systems. Without an adequate understanding of these issues, security arrangements were likely to be inadequate.

(11) The historical transactions data was encrypted, but the encryption keys were stored in plaintext within the application's source code. The Commissioner considers this use of plaintext storage for encryption keys to be inadequate in terms of data security, in particular for data relating to individuals' financial transactions.

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 Carphone Warehouse's technical and organisational measures for ensuring the security of personal data on the System. The Commissioner reiterates that she has carefully considered the evidence and submissions provided by Carphone Warehouse. She has accepted a number of the points Carphone Warehouse has made, but she remains mindful that DPP7 and the statutory conditions under section 55A DPA are concerned with measures and with 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 very serious risks.

24. In the Commissioner's view, each of the itemised inadequacies listed above would have constituted a contravention of DPP7. The

Commissioner has, however, assessed the arrangements in the round: on that cumulative basis, the Commissioner's 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) The number of distinct and significant inadequacies in the security arrangements for the System is striking. As explained above, each of the itemised inadequacies would themselves have constituted a contravention of DPP7. Cumulatively, this multi-faceted contravention was extremely 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 outdated software, inadequate patching measures and the absence of WAF and antivirus measures. Carphone Warehouse 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 (mid-2015). The Commissioner rejects that submission. The deficiencies set out in paragraph 22 above represent appropriate measures

that data controllers such as Carphone Warehouse should have had in place in mid-2015.

(3) These inadequacies appear to have persisted over a relatively long period of time, given how easily and quickly some of these glaring shortcomings should have been identified and remedied.

(4) The System contained a very large amount of personal data, affecting well over 3 million individuals. This increases the seriousness of its data security inadequacies. So too does the fact that significant volumes of credit card data was put at risk, even allowing for the fact that such data typically expires in 3-4 years. Further, a substantial employee database was put at risk.

(5) The attack had been ongoing for 15 days before it was detected.

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 13 above. A contravention involving personal data of those kinds was likely to be useful in terms of identity theft and fraud. If any such outcomes had materialised (though there is no evidence that 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.

(2) The credit card data – which was specifically targeted and exported by the attacker – represented a particular risk in terms of identity theft and fraud. That data was relatively historic at the time of the attack, and the Commissioner has taken this into account in her assessment of the likely consequences of these contraventions of DPP7, as well as in her determination of the appropriate amount for this monetary penalty. It is clear, however, that there remained a substantial risk of the compromised data being misused. Carphone Warehouse seems to have shared that view: after the attack, it used services such as Financial Fraud Action and provided affected customers with access to credit alert systems. Carphone Warehouse acted correctly in taking such remedial action, but the need to do so illustrates the likelihood of substantial damage or distress arising from a contravention of this kind.

(3) The personal data that was put at risk had a significant bearing on individuals' privacy: for example, it contained their contact details, information about where they lived and had lived, about their marital status. Such information can also be used to undertake checks of individuals' credit histories. 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. Cumulatively, the "substantial distress" threshold was clearly met in these circumstances.

(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. Cyberattacks invariably involve

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 the System (a point which cannot be conclusively established), that data remains at large. This factor is likely to exacerbate the risk of substantial distress to affected data subjects. The Commissioner notes Carphone Warehouse's submission that there is no evidence of this data in fact remaining at large, but she maintains that (a) it is likely that the attacker did remove significant amounts of personal data, and (b) that data has not been recovered from the attacker.

28. The Commissioner considers that Carphone Warehouse 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 Carphone Warehouse failed to take reasonable steps to prevent such a contravention, in that:

(1) Carphone Warehouse is a large, well-resourced and experienced data controller. According to its website, it is the largest independent telecommunications retailer in Europe, with over 1,100 stores across the UK and Ireland. It describes itself as the number one independent mobile online retailer in the UK. A company of this size and standing was well placed to assess any weaknesses in its 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 up-to-date software, adequate patching measures, WAF and antivirus software). Had such measures been in place, this attack may well have been averted. In any event, the absence of these measures created serious and avoidable risks to the contents of the System.

(3) Given its size and prominence, as well as the volume of personal data held on its systems, Carphone Warehouse should have realised that its systems were potentially attractive targets for cyberattack.

(4) Carphone Warehouse should have appreciated that misuse of the personal data on the System was likely to cause substantial distress and damage, including (but not limited to) risks of fraud and identity theft.

(5) The processing of credit card data (notwithstanding its general 3-4 year useful life span) should have alerted Carphone Warehouse to the need for security measures that at least achieved compliance with the Payment Card Industry Data Security Standard. It was working to achieve that compliance standard, but a data controller in its position should have done so much earlier.

(6) In the Commissioner's view, Carphone Warehouse's ignorance about the presence of large volumes of credit card data on the System does not help its case. It ought to have understood its

own IT and data architecture better, and then to have matched adequate security measures to that picture.

(7) The importance of adequate vulnerability and penetration testing should also have been obvious. The Commissioner notes for example that this attack involved the use of Nikto, a commonly used tool for scanning and detecting vulnerabilities in web servers. The Commissioner notes Carphone Warehouse'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 Carphone Warehouse's technical and organisational measures in respect of the System, and that those deficiencies should have been obvious to this data controller.

(8) Indeed, Carphone Warehouse does appear to have been aware of the need for penetration testing. Its own Risk Assessment Standard in place at the time of the incident stated that "Network and Application Penetration testing must be completed on all Carphone Warehouse environments by an authorised third party at least annually". This illustrates an awareness of the need for such testing. Carphone Warehouse failed to take reasonable steps to ensure that its own policies were implemented across this division of Carphone Warehouse and applied to the System.

(9) More broadly, the marked discrepancy between data security measures apparently in place for other Carphone Warehouse divisions and systems – as opposed to this particular division and the System – shows its awareness of the importance of such measures. It failed to take reasonable steps to ensure

that the same standards were followed by this division and applied to the System.

(10) Further, Carphone Warehouse does appear to have been aware of potential systemic deficiencies in its information security. Following its merger with Dixons in 2014, it implemented a wide-ranging review and remedial programme for information security. It was thus well aware of the need to take remedial steps of these kinds, but it ought reasonably to have acted with much greater urgency, by prioritising steps to identify and act on the most pressing deficiencies. The Commissioner's view is that Carphone Warehouse could and should have taken steps – both before and after the Dixons merger – to correct these deficiencies.

(11) In June 2015, the relevant division was identified by a risk assessment conducted by external consultants as having weaker controls and higher exposure to risk (particularly as regards payment card data) than other divisions of Carphone Warehouse. Those points ought to have been apparent to Carphone Warehouse much earlier, and urgent action should have been taken.

(12) As identified in the report by F, a number of remedial measures were introduced within a month of the attack described above. This shows that they were readily and quickly achievable. The Commissioner sees no good reason why such measures were not taken much earlier.

29. The Commissioner's view is therefore that the statutory conditions for issuing a monetary penalty have been met in this case. She has

considered all the circumstances and has reached the view that it is appropriate to issue a monetary penalty in this case.

30. That view is based on the multiple, systemic and serious inadequacies identified above, the likely consequences of such a contravention and Carphone Warehouse's culpability for it. The Commissioner has also considered the importance of deterring future contraventions of this kind, both by Carphone Warehouse 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

31. The Commissioner has taken into account the following mitigating features of this case:

(1) Carphone Warehouse did have a programme in place for improving its information security measures within this division of the company (albeit that urgent measures should have been prioritised much sooner).

(2) Carphone Warehouse quickly took a number of remedial actions to fix some of the problems and to assist affected data subjects in the wake of the attack described above.

(3) There is no evidence that the compromised personal data was in fact used for successful identity theft or fraud activities. The credit card data that was put at risk would probably have had a 3-4 year expiry period. The transaction and payment card data

[redacted] was 4-5 years old at the time of the attack.

(4) There remains uncertainty as to how the attacker obtained valid credentials for the WordPress system. The use of valid credentials played an important role in this particular attack.

(5) There remains uncertainty about how much of the data on the System was successfully extracted by the attacker (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).

(6) Carphone Warehouse proactively reported the attack to the Commissioner and co-operated with her investigation.

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

(1) The cumulative impact of the problems (see the Commissioner's discussion of seriousness above) is striking, including by comparison with many other cases the Commissioner has investigated.

(2) Carphone Warehouse's culpability (see paragraph 28 above) is equally striking. At present, the Commissioner can see no justification or excuse for the extent of these systemic inadequacies on the part of such a large and well-established data controller.

(3) Given the nature of Carphone Warehouse's business, its contravention was likely to impact not only upon individuals, but also a range of businesses (in particular, telecommunications networks who entrusted Carphone Warehouse with their customers' personal data).

33. The Commissioner has also taken into account her underlying objective in imposing a monetary penalty notice, namely to promote compliance with the DPA. 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.

34. Further, she has considered Carphone Warehouse's financial position, as evidenced by its published annual accounts.

Conclusion

35. Taking into account all of the above, and noting that this is a strikingly serious contravention of DPP7, the Commissioner has decided that a penalty in the sum of **£400,000 (Four hundred thousand pounds)** is reasonable and proportionate.

36. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **8 February 2018** 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.

37. If the Commissioner receives full payment of the monetary penalty by **7 February 2018** the Commissioner will reduce the monetary penalty by 20% to **£320,000 (Three hundred and twenty thousand**

pounds). However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

38. 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.

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

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

41. 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
    - the period for appealing against the monetary penalty and any variation of it has expired.

42. 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 8th day of January 2018

Signed ……..

Elizabeth Denham
Information Commissioner
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)).