Data Protection Act 1998

Monetary Penalty Notice

Dated: 31 October 2014

Name: Worldview Limited

Address: Telephone House, 3rd and 4th floors, Fenton Street, Lancaster, Lancashire LA1 1BA

Statutory framework

1. Worldview Limited is the data controller, as defined in section 1(1) of the Data Protection Act 1998 (the "Act"), in respect of the processing of personal data carried out by Worldview Limited and is referred to in this notice as the "data controller". Section 4(4) of the Act provides that, subject to section 27(1) of the Act, 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.

2. The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act"). By virtue of section 6(1) of the Act, the office of the Data Protection Registrar originally established by section 3(1)(a) of the 1984 Act became known as the Data Protection Commissioner. From 30 January 2001, by virtue of section 18(1) of the Freedom of Information Act 2000 the Data Protection Commissioner became known instead as the Information Commissioner (the "Commissioner").

3. Under sections 55A and 55B of the Act (introduced by the Criminal Justice and Immigration Act 2008 which came into force on 6 April 2010) the Commissioner may, in certain circumstances, where there has there been a serious contravention of section 4(4) of the Act, serve a monetary penalty notice on a data controller requiring the data controller to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice but not exceeding £500,000. The Commissioner has issued Statutory Guidance under section 55C (1) of the Act about the issuing of monetary penalties which is published on the Commissioner's website. It should be read in conjunction with the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

Power of Commissioner to impose a monetary penalty

(1) Under section 55A of the Act 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) of the Act 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.

Background

4. The data controller provides a booking service for serviced apartments and hotels. The coding of the booking terms page for a website (the "web page") was developed in-house and installed in May 2010.

5. There was a vulnerability in the code that retrieved rate information on the web page. This meant that user input was not properly validated so that an attacker was able to inject SQL queries in order to perform a blind SQL injection attack. The content of the web page then differed based on the results of the injected query. By querying the database using equality tests and monitoring the page content, data could be

extracted character by character from the database.

6. The attacker then used a single SQL injection vector multiple times to extract WordPress password hashes from a WordPress blog database. The WordPress software had been recently installed and was the most up to date and stable version available. However, for operational reasons it had been placed on the same server as the booking service website and other websites used by the data controller until the URL could be redirected to a separate isolated server.

7. During the initial set up period, the online marketing team had to install add-ons and customise templates so permissions were granted to WordPress. Passwords for an IT administrator and an online marketing administrator were created. However, the password created for the online marketing administrator was a weak default password in breach of the data controller's policy. The attacker was therefore able to crack the password despite the default WordPress hashing method being appropriate.

8. On 18 June 2013, the attacker used the administrative access to WordPress to log into the blog tool and alter template files to include a malicious code. This acted as a gateway, allowing arbitrary commands to be executed on the server as well as providing convenient methods for browsing the file system, downloading and uploading files and executing database queries.

9. The attacker then made blind SQL injection attempts on the credit card and internal mail account tables of the data controller's database. At the time of the attack the database stored the details of 3,814 clients including encrypted card data and the CVV numbers. The decryption keys for the encrypted card data were stored in a file on the same server. Therefore the attacker could have obtained these keys and decrypted the encrypted card data.

10. This security breach was identified on 28 June 2013 during a regular code update. The files were then locked down by the data controller but the attacker had access to the systems for a period of up to 10 days. The data controller has confirmed that no specific security checks were carried out on the web page prior to launch. There was a lack of relevant training in security matters for developers and insufficient oversight and checking of their work.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

The relevant provision of the Act is the Seventh Data Protection Principle which provides, at Part I of Schedule 1 to the Act, that:

"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".

Paragraph 9 at Part II of Schedule 1 to the Act provides that:

"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".

In deciding to issue this Monetary Penalty Notice, the Commissioner has considered the facts of the case and the deliberations of those within his office who have recommended this course of action. In particular, he has considered whether the criteria for the imposition of a monetary penalty have been met; whether, given the particular circumstances of this case and the underlying objective in imposing a monetary penalty, the imposition of such a penalty is justified; and whether the amount of the proposed penalty is proportionate.

- The Commissioner is satisfied that there has been a serious contravention of the Seventh Data Protection Principle.

  In particular, the data controller failed to take appropriate technical measures against the unauthorised or unlawful processing of personal data such as:

  - Providing relevant training for developers in security matters and providing sufficient oversight and checking of their work,
  - Sufficiently testing the security of a new web page,
  - Ensuring and checking that that the default password was changed for the WordPress administrator account, and
  - Keeping the decryption keys secure and separate from the data itself.

  The contravention is serious because there have been a series of failings by the data controller which in combination have enabled an

attacker to enter the data controller's systems and ultimately access unencrypted card data.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage or substantial distress.

  Active card data was obtained over a 10 day period including the CVV values that could have been decrypted. Although there is no evidence of fraud having taken place as a result of this incident, the personal data that was obtained was clearly of interest to the attacker given the targeted nature of the attack, and could still be used for fraudulent purposes. It is reasonable to assume therefore that it is likely that the attacker would use this information in a manner that would cause substantial damage to the data subjects either in the short or long term.

  The data subjects would also be likely to suffer from substantial distress on being informed that their personal data had been accessed by an unauthorised third party and could have been further disclosed even though, so far as the Commissioner is aware, there has been no evidence of fraudulent transactions being conducted as a result of this incident. The knowledge of this access alone is likely to cause substantial distress.

- The Commissioner is satisfied that section 55A(3) of the Act applies in that the data controller knew or ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

  The data controller should have been aware of the risks associated with any compromise of card data due to the nature of the data being collected. The data controller was also aware of the Payment Card Industry – Data Security Standard covering security related issues, and that there was a risk in storing CVV numbers.

  In the circumstances, the data controller knew or ought to have known that there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention, such as those outlined above.

  Further, it should have been obvious to the data controller who was aware of the nature and amount of the personal data processed stored on the system, that such a contravention would be of a kind likely to

cause substantial damage or substantial distress to the data subjects.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

---

Impact on the data controller

- Data controller is a limited company so liability to pay a monetary penalty will not fall on any individual
- Data controller has access to sufficient financial resources to pay the monetary penalty without causing undue financial hardship

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

---

Nature of the contravention

- Data controller's systems were subjected to a criminal attack
- Online marketing administrator should have used a stronger password
- No previous similar security breach that the Commissioner is aware of

Effect of the contravention

- No evidence that the personal data has been used for fraudulent transactions

Behavioural issues

- Voluntarily reported to the Commissioner's office
- The data controller has been co-operative with the Commissioner's office.
- The data controller promptly locked down the files on discovering the incident and notified the data subjects
- The data controller offered compensation for any inconvenience suffered by individuals
- Substantial remedial action has now been taken

Impact on the data controller

- Significant impact on reputation of data controller as a result of this security breach

Other considerations

- The Fifth Data Protection Principle at Part I of Schedule 1 to the Act was also contravened in that card data was stored on the data controller's systems for longer than was necessary
- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data stored on their information technology systems

Notice of Intent

A notice of intent was served on the data controller dated 8 September 2014. The Commissioner received written representations from the data controller in in a letter from a Solicitor acting on their behalf dated 10 October 2014. The Commissioner has considered the written representations made in relation to the notice of intent when deciding whether to serve a monetary penalty notice. In particular, the Commissioner has taken the following steps:

In the circumstances, the Commissioner has now taken the following steps:

- reconsidered the amount of the monetary penalty generally, and whether it is a reasonable and proportionate means of achieving the objective which the Commissioner seeks to achieve by this imposition;
- ensured that the monetary penalty is within the prescribed limit of £500,000; and
- ensured that the Commissioner is not, by imposing a monetary penalty, acting inconsistently with any of his statutory or public law duties and that a monetary penalty notice will not impose undue financial hardship on an otherwise responsible data controller.

Amount of the monetary penalty

The Commissioner considers that the contravention of the seventh data protection principle is **serious** and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of **£7,500 (Seven thousand five hundred pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

In reaching this decision, the Commissioner considered other cases of a similar nature in which a monetary penalty had been imposed, and the facts and aggravating and mitigating features referred to above.

This case was originally considered to attract a higher penalty of £75,000. However, having given consideration to the financial position of the company as he must do after applying the aggravating and mitigating features, the Commissioner considered that it was necessary to reduce the amount to £7,500 so as not to cause undue financial hardship.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 2 December 2014 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.

Early payment discount

If the Commissioner receives full payment of the monetary penalty by 1 December 2014 the Commissioner will reduce the monetary penalty by 20% to **£6,000 (Six thousand pounds).** However, you should be aware that if you decide to take advantage of the early payment discount you will forfeit your right of appeal.

Right of Appeal

There is a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against:

a. the imposition of the monetary penalty

and/or;

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

Any Notice of Appeal should be served on the Tribunal by 5pm on 1 December 2014 at the latest. If the notice of appeal is served late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

Information about appeals is set out in the attached Annex 1.

Enforcement

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

- the period specified in 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 the data controller to appeal against the monetary penalty and any variation of it has expired.

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 or any sheriffdom in Scotland.

Dated the 31st day of October 2014

Signed: ……..

David Smith
Deputy 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) General Regulatory Chamber (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 he ought to have exercised his 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 served on the Tribunal by 5pm on 1 December 2014 at the latest.

   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;

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

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

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

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 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)).