

Data Protection Act 1998

Monetary Penalty Notice

Dated: 21 July 2014

Name: Think W3 Limited

Address: 21 Ganton Street
London
W1F 9BN


Statutory framework

1. Think W3 Limited ("TW3") 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 TW3 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. TW3 is the data controller in respect of the personal data collected from customers of its wholly owned subsidiary and trading brand, Essential Travel Ltd ("ETL"). ETL acts as a booking agent for airport car parking, travel insurance, and other travel-related services that are made available online. .
5. In early 2006 the data controller internally developed a car parking system for ETL to maintain car park rates and availability. The system was for internal purposes only and was installed on the same web server which contained ETL's main e-commerce application used to

store customer personal data. In order to facilitate homeworking this system could be accessed via a login page on a non-customer facing website which was publicly available over the internet.

6. Unfortunately the website login page coding was not secure as it contained a coding error in the authentication scripts of the administrative interface. The data controller conducted functionality tests when the system was implemented but did not carry out security checks and reviews on the system and website coding at the time of implementation, or subsequently. The login page for the website was therefore vulnerable since the system was implemented in early 2006.
7. The data controller did not subject the web server to appropriate penetration tests or internal vulnerability scans and checks which took place on other servers on the basis that the website and web server were not external facing. However the website (and therefore associated system and web server) could still be discovered and accessed over the internet by anyone with sufficient technical knowledge.
8. On 21 December 2012 an attacker targeted the website and associated system. The coding error on the website login page enabled the attacker to bypass the authentication process for logging into the system using Structured Query Language injection, and log in to the website's administrative interface.
9. Having exploited this vulnerability the attacker then proceeded to upload malicious web shells onto the connected web server which gave the attacker administrative access to all of the data held on the web server. These allowed the attacker to access and modify files within ETL's virtual network, including data within the e-commerce application which contained the ETL's customer database and files used to process payment cards.
10. Evidence obtained as a result of the data controller's own internal investigation suggests that the attacker then created a custom file that would query the customer database to extract and decrypt stored cardholder data (both active and expired cards) using the decryption key which was not stored securely on the web server. The attacker targeted credit and debit card primary account numbers, expiry dates, CVV values and account user names and surnames. Fortunately CVV values were not stored on the database. However following successful extraction of the available data the attacker then extracted other customer details relating to each card, specifically: customer name, address, postcode, mobile and home phone numbers, and email address.

11. The attacker extracted a total of 1,163,996 credit and debit card records, of which 430,599 were identified as current and 733,397 as expired. Cardholder data had not been deleted from the server since 2006.
12. The data controller discovered the breach in security on 24 December 2012 during a routine server check which revealed a notification from the antivirus software installed on the server. This resulted in the data controller taking prompt remedial action to lock down the relevant website, systems and web server in order to prevent any further disclosure of data.

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 by failing to:

- Properly understand the extent to which the web server could be accessed via the internet. This led to the data controller deliberately excluding the web server from penetration and vulnerability tests which were carried out on 'external-facing' servers,
- Properly test/ check/ review the security of the coding of the website at the time of, and following, the website's implementation in 2006,
- Implement a suitable intrusion detection system for the website and server,
- Implement suitable file-integrity monitoring software,
- Implement a suitable encryption key-management process,
- Implement a suitable security policy addressing technical security issues,
- Patch software when updates were available,
- Update anti-virus software properly on some desktop systems,
- Fully comply with the requirements of the Payment Card Industry – Data Security Standard.

The contravention is serious because the measures taken by the data controller did not ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing, and the nature and volume of the data to be protected.

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

Active payment card data was obtained. Whilst CVV values were not obtained, and there has been no evidence/ confirmation 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 be used for fraudulent transactions/ 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 if they were to be 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 payment card and cardholder data due to the nature of the data being collected. By 2011 the data controller was aware of a number of issues with its Payment Card Industry – Data Security Standard compliance which caused it to review some of its security practices. However the data controller was slow in implementing improvements to its systems (partly as a result of external factors).

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 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 a monetary penalty up to the maximum 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

- The data controller's systems were subjected to a criminal attack.
- No previous similar security breach that the Commissioner is aware of.

Effect of the contravention

- No evidence or confirmation has been received that the personal data has been used for fraudulent transactions.

Behavioural issues

- Voluntarily reported to Commissioner's office
- The data controller has been co-operative with the Commissioner's office.
- The data controller promptly locked down the website and associated systems when the breach was discovered and escalated the matter quickly despite the timing of the incident.
- On discovering the incident the data controller quickly de-commissioned the website and associated system which had been replaced by a new system on 19 December 2012. The website and system had originally been due to be de-commissioned in January 2013.
- The data controller had been in the process of a tokenisation program to improve data security. In light of this incident the data controller fast-tracked the implementation of the token-based system for the remaining products that had not yet been transferred to the new system.

Impact on the data controller

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

Other considerations

- 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 2 June 2014. The Commissioner has not received any representations from the data controller in response to the notice of intent. 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 **very serious** and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of **£150,000** (One hundred and fifty thousand 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.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 21 August 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

20 August 2014 the Commissioner will reduce the monetary penalty by 20% to **£120,000** (One hundred and twenty thousand pounds). 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 20 August 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 21st day of July 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 20 August 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)).