Data Protection Act 1998

Monetary Penalty Notice

Dated: 2 July 2012

Name: Welcome Financial Services Limited

Address: Kingston House, Centre 27 Business Park, Woodhead Road, Birstall, Batley WF17 9TD

Statutory framework

1. Welcome Financial Services 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 Welcome Financial Services 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. Shopacheck and [redacted] are both business divisions of the data controller. As part of its data management and disaster recovery precautions, Shopacheck's IT team maintained back-ups of the Shopacheck Local Area Network ("LAN") for each business day. The storage media were HP LT04 DATA tape format with a capacity of approximately 1.6TB each. The capacity of the back-up tapes (the "tapes") meant that each tape could hold two complete back-ups.

5. After a back-up of the LAN was made the tapes were transported from the Shopacheck offices by a senior administrator and held offsite at the offices of [redacted] in their secure IT Store Room. There were 200 of these tapes in use and each tape was labelled sequentially from 1 to 200. The tapes were then periodically transported back to the offices of Shopacheck in batches of 20. These tapes were then re-used for further back-ups of the Shopacheck LAN. Prior to re-use the tapes were stored in the access-controlled Communications Room at Shopacheck.

6. On 7 November 2011, a Shopacheck IT administrator transported a box of 20 tapes from [redacted] to the Communications Room at Shopacheck. Over the next two weeks, these tapes were used to perform back-ups of the data controller's LAN and transported back to [redacted] on a daily basis. On 23 November 2011, the IT administrator noticed that two of the tapes appeared to be missing from the box in the Shopacheck Communications Room. An analysis of Shopacheck's control records for the tapes confirmed that two of the tapes were unaccounted for and that they contained back-up data of the Shopacheck LAN on 26 and 27 October 2010.

7. The personal data held on the tapes consisted of personal data relating to approximately 20,000 current and former employees of the data controller, Shopacheck and [redacted] during the period 2002 to 2010. There was also personal data relating to approximately 8,000 agents for the same period. Many of these records contained financial information such as bank account details, dates of birth, CV information and National Insurance numbers. There were also customer records relating to approximately 1.94 million customers of the data controller and Shopacheck. This data consisted of customer names, addresses, telephone numbers, dates of birth and customer loan accounts for approximately 510,000 customers. The tapes have not been recovered to date.

8. The Commissioner understands that both tapes were unencrypted which was in breach of the data controller's Information Security Policy. They also held significant quantities of historic personal data although it is accepted that the data on the tapes could only be accessed using specialist IT hardware and software costing several thousand pounds. The data controller has now taken remedial action which included a comprehensive internal review of its IT systems to identify and encrypt any remaining unencrypted data/systems.

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".

- The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act.

  In particular, the data controller failed to take appropriate technical measures against the unauthorised processing of personal data such as encrypting the tapes.

  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 processing and the nature of the data to be protected.

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

  In this particular case the data subjects would suffer from substantial distress knowing that their personal data may be accessed by third parties even though, as far as the Commissioner is aware, those concerns have not so far materialised. This is aggravated by the fact that the tapes have still not been recovered.

  If the data is in fact accessed by untrustworthy third parties then it is

likely that the contravention would cause further distress and also substantial damage to the data subjects such as exposing them to identity fraud and possible financial loss.

- 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 and/or substantial distress, but failed to take reasonable steps to prevent the contravention.

  In the circumstances, the data controller knew or ought to have known that there was a risk that the contravention would occur. The data controller's business divisions were routinely involved in handling large amounts of personal data including financial information. Further, the requirement that the tapes should be encrypted in the Information Security Policy demonstrates that the data controller was fully aware of the possible consequences of the tapes going missing.

  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 encrypting the tapes.

  Further, it should have been obvious to the data controller whose business divisions were routinely involved in handling large amounts of personal data including financial information that such a contravention would be of a kind likely to cause substantial damage and/or substantial distress to the data subjects due to the nature of the data involved. It is possible that an unauthorised third party could still access this data and may already have done so.

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

---

Nature of the contravention

- Contravention was especially serious because of the large number of records involved and the nature of the personal data
- Implementation of appropriate IT security measures would have prevented unauthorised processing of the data

Effect of the contravention

- The tapes have still not been recovered

- 26 formal complaints have been received and a number of calls made to the ICO helpline

Behavioural issues

- Data controller did not follow its own policy on Information Security

Impact on the data controller

- 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

- No previous similar security breach that the Commissioner is aware of

Effect of the contravention

- Personal data can only be accessed using specialist IT hardware and software costing several thousand pounds
- As far as the Commissioner is aware the tapes have not been accessed by unauthorised third parties to date

Behavioural issues

- Voluntarily reported to Commissioner's office
- Full investigation carried out
- Data subjects were informed and those at highest risk of fraud were offered 12 months of complimentary fraud protection
- Fully co-operative with the Commissioner's office
- 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 which was publicised in the national press

Other considerations

- The Third Data Protection Principle at Part I of Schedule 1 to the Act was also contravened by the data controller in that excessive personal data was held on the tapes
- 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 held on portable media

Notice of Intent

A notice of intent was served on the data controller dated 27 April 2012. The Commissioner received written representations from the data controller's Chief Executive in a letter dated 16 May 2012. 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:

- 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 section 4(4) of the Act is 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.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS

transfer or cheque by 1 August 2012 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 31 July 2012 the Commissioner will reduce the monetary penalty by 20% to £120,000 (One hundred and twenty thousand pounds).

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 August 2012 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 2nd day of July 2012

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 August 2012 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)).