Data Protection Act 1998

Monetary Penalty Notice

Dated: 29 October 2012

Name: The Prudential Assurance Company Limited

Address: Laurence Pountney Hill, London EC4R 0HH

Statutory framework

---

1. The Prudential Assurance Company 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 the Prudential Assurance Company 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 it 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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 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 holds customer records in a centralised database [redacted] which enables staff to view all of the policies belonging to a customer. [redacted] held records in relation to two customers who shared the same first name, surname and date of birth (hereinafter referred to as customer A and customer B). Customer A had two policies numbered [redacted] and [redacted] and customer B had one policy, an endowment, numbered [redacted]. The Commissioner understands that in March 2007, customer A's financial adviser telephoned the data controller on a matter connected with one of his policies. For some unknown reason the financial adviser gave the address of customer B

which meant that customer A's address was updated on [redacted] to be the same as customer B. Subsequently, both customer records were merged as a result of the data matching function [redacted].

5. In May 2007, customer B received pension and policy statements relating to customer A which detailed the amounts then accrued and the projected income on retirement. In August 2007, customer A telephoned the data controller about an unrelated matter but subsequently his address was re-instated. However, this resulted in the address on customer B's record being amended to that of customer A because their records on the [redacted] database had already been merged. The change of address was also applied to customer B's individual endowment policy. The Commissioner understands that any policy statements relating to customer B were then sent to customer A.

6. On 24 June 2008, customer A contacted the data controller to complain that he was receiving policy information in relation to customer B. A note was then put on the [redacted] database to highlight the error but, because the endowment policy showed customer B's correct address, no further action was taken. In March 2009, a mortgage endowment update letter intended for customer B was sent to customer A, whose address was still shown on the merged record. The letter was returned unopened so the data controller initiated its "gone away" process, which involved sending a letter to the customer's bank and asking them to forward it to their customer's current address.

7. In May 2009, customer B sent the data controller a letter of authority for his financial advisers to act on his behalf. As customer A's address was still shown on the [redacted] record, the data controller assumed that customer B was also notifying them of a change of address even though he was just writing from his usual address. The data controller then changed the address on the merged [redacted] record to that of customer B.

8. In July 2009, customer B's financial advisers had considered his financial position based on previous statements and updated information they had received from the data controller under the authority and advised him to transfer funds in the sum of [redacted] on policy number [redacted] to another investment company, which apparently handled his employment pension. On 17 July 2009, the data controller completed the transfer following receipt of customer B's signed agreement.

9. In August 2009, customer A's financial advisers wrote to the data controller advising that their client wanted to take a payment holiday in respect of policy number [redacted]. On 11 August 2009, the data

controller wrote to customer A's financial advisers (copied to customer B, whose details were still shown on the merged record) that the policy had been transferred to another investment company the previous month with a transfer value of [redacted]. On 31 March 2010, customer A's financial advisers asked for a copy of the transfer papers. On 14 April 2010, the data controller sent a copy of the transfer form signed by customer B, to both customer A's financial advisers and customer B. Surprisingly, customer A's financial advisers do not appear to have taken this matter any further.

10. On 20 April 2010, customer B telephoned the data controller to question why he had received these documents, and had not received any statement for his endowment policy. During the telephone conversation, he was assured that his records had been corrected and that this would be confirmed in writing. On 21 April 2010, customer B and his wife wrote a letter of complaint to the data controller about this mix-up, in which it was clearly stated that they had lived at the same address for over 15 years. On 22 April 2010, the data controller sent a yearly statement to customer B in relation to customer A's policy number [redacted]. On 3 May 2010, the data controller's then Head of Operations wrote to customer B and his wife in response to their complaint, to explain that in 2007 their bonus statement had been sent to another customer with the same name. This letter again reassured them that the records had now been corrected.

11. On 15 September 2010, customer A contacted the data controller in relation to his policies which prompted him to reiterate his current address. The data controller then changed the address record on the policy system, which then required a "change of address" letter to be sent to the customer's previously listed address. On 16 September 2010, therefore, the data controller sent a letter to customer B stating that its records showed he had changed his address but they were writing to his former address as a security precaution. As customer B had lived at the same address for over 15 years, he then telephoned the data controller, on 20 September 2010, to find out why the letter had been sent to him. A further letter was then sent on 22 September 2010 assuring customer B that the data controller did have his correct address on its records.

12. Following an investigation at this point, the data controller finally arranged to de-merge the customer records on 24 September 2010 and then began, in October 2010, to try to obtain a refund of the monies transferred in error to the other investment company by customer B which actually belonged to customer A. The Commissioner understands that the data controller has now taken steps to improve

its processes and staff training to minimise the risk of a recurrence.

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

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

"Personal data shall be accurate and, where necessary, kept up to date".

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

  The records of customer A and customer B had been incorrectly merged since March 2007 which resulted in financial information being erroneously sent to each of them at various times. On 17 July 2009, this culminated in funds held on a policy, which actually belonged to customer A, being transferred in error to another investment company by customer B. The data controller failed to correct the inaccuracy despite a number of complaints from both customers during this period and, in particular, following the complaint from customer B and his wife on 21 April 2010. As it was, the data controller did not de-merge the customer records until 24 September 2010 during which time further harm could have been caused to the customers, which is supported by the facts that two further letters were erroneously sent to customer B and that customer A still had another policy which could potentially have been transferred by customer B's authority.

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

  Personal data consisting of financial information was erroneously sent to customer A and customer B at various times and put at risk due to the inaccurate information held on the [redacted] database. This contravention is of a kind likely to cause substantial distress to the data subjects whose financial information has been sent to another customer who had no right to see that information.

  In this particular case, funds from a policy belonging to another customer were transferred in error by one customer on 17 July 2009 and the potential for further substantial damage remained until the customer records were finally de-merged on 24 September 2010 and the data controller recovered the transferred funds from the other investment company, which did not occur until 2011.

Further, the data subjects would be justifiably concerned that after being sent to the wrong person their data may be further disseminated even if those concerns do not actually materialise. If the parties the data was disclosed to had been untrustworthy 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 distress, but failed to take reasonable steps to prevent the contravention.

  The Commissioner has taken this view because the data controller is a large company in the financial services sector with approximately six million customers. The data controller is used to handling financial information on behalf of its customers on a daily basis and was aware that several thousand of its customers share the same names. Therefore, the data controller knew or ought to have known that there was a risk that customer records could become mixed-up.

  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 taking immediate action to investigate properly and de-merge the customer records on receipt of the complaint from customer B and his wife on 21 April 2010, bearing in mind the background to this matter. The data controller's failure to take reasonable steps to prevent the contravention meant that the customers' records were not finally de-merged until 24 September 2010, and customer A's pension funds were not recovered until several months after that.

  Further, it should have been obvious to the data controller that such a contravention would be of a kind likely to cause substantial damage and substantial distress to the data subjects due to the nature of the data involved.

  Finally, the Commissioner's power to impose a monetary penalty did not come into effect until 6 April 2010. However, the Commissioner is satisfied (having taken into account all the circumstances including the actions or inactions of the data controller prior to April 2010) that there was a serious contravention of the Act between April and September 2010 of a kind likely to cause substantial damage and substantial distress to the data subjects and also that the data controller failed to

take reasonable steps during that six month period.

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

---

Nature of the contravention

- Financial information was sent to the wrong customer as a result of the contravention with the potential to cause financial loss and possible identity fraud
- Contravention was serious because the data controller failed to correct the inaccuracy over a long period of time despite many missed opportunities
- The risk of further damage to customer A remained even after customer B's complaint of 21 April 2010, as the data controller failed to conduct a proper investigation and consequently customer A's other pension policy was still at risk of transfer. This risk remained for a further 5 months until the records were de-merged

Effect of the contravention

- A customer was able to transfer funds from a policy which belonged to another customer to another investment company, with a transfer value of £[redacted]
- The data controller received formal complaints from both customers in relation to the damage and distress they had suffered and a complaint was made to the Pensions Advisory Service

Impact on the data controller

- The data controller is a limited company so liability to pay a monetary penalty will not fall on an individual
- 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

- Only two data subjects were affected

- The Commissioner is not aware of any directly similar contraventions despite the large number of customers on the [redacted] database

Effect of the contravention

- To the Commissioner's knowledge the personal data has not been further disseminated by the customers

Behavioural issues

- Compensation has been paid to both customers
- Funds transferred to another investment company have been recovered by data controller
- Remedial action has now been taken
- Co-operative with Commissioner's office

Impact on the data controller

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

Other considerations

- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act. This is an opportunity to reinforce the need for data controllers to take reasonable steps to ensure the accuracy of data held on their database

Notice of Intent

A notice of intent was served on the data controller dated 6 September 2012. The Commissioner received written representations from Solicitors acting for the data controller in letters dated 5 and 18 October 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 £50,000 (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 30 November 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 29 November 2012 the Commissioner will reduce the monetary penalty by 20% to £40,000 (Forty 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 29 November 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 29th day of October 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 29 November 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)).