Data Protection Act 1998

Monetary Penalty Notice

Dated: 30 July 2013

Name: Bank of Scotland plc

Address: The Mound, Edinburgh, EH1 1YZ

Statutory framework

---

1. Bank of Scotland plc 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 on by Bank of Scotland plc 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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

---

4. Section 55A of the Act provides that:

(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) [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

[redacted]

5. On 27 February 2009, [redacted] reported to the data controller that they had received, by fax, a Further Advance declaration relating to a private individual's mortgage. It had been sent to [redacted] in error.

6. The data controller completed an internal breach report in response to the incident. The report noted that there was a one digit

difference between the internal fax number at the data controller's office, to which the fax should have been sent, and the fax number at [redacted] to which it had actually been sent; the misdialled number had substituted an 8 for a 2.

7. The data controller's correct fax number belonged to a centralised business area within the data controller's organisation ("Nexus") which scanned documentation into its workflow systems.

8. The action plan produced by the data controller stated that the error was to be raised with the individual who had sent the fax, the correct number would be confirmed and a reminder would be sent to the rest of the data controller's team involved, regarding checking of correct fax numbers when sending personal data.

9. On 3 March 2009, a member of the public reported a second breach to the data controller, relating to a fax breach that occurred on 24 February 2009. The individual reporting the breach also reported another occasion on which he had received information faxed from the data controller, but he had shredded the information. The data controller was therefore unable to identify the source of that breach. This incident disclosed personal data relating to a private mortgage and details of working tax benefits received.

10. A breach report was produced by the data controller which noted that the fax number involved in that breach was two digits different to the data controller's correct fax number which was again the Nexus fax number referred to at §7 above. The data controller identified the different employee responsible and provided training to them. A communication was sent to employees alerting them to the issue of misdialling, checking they were aware of the correct fax

number and seeking to ensure that any pre-programmed numbers used in fax machines had been entered correctly.

11. On 28 March 2011, a complaint was received by the Information Commissioner from [redacted]. [redacted] stated that, despite complaining to the data controller directly, they had continued to receive misdirected faxes from the data controller. [redacted] provided copies of those faxes, which contained personal data, to the Commissioner. [redacted] advised the Commissioner that it had received many more faxes in addition to those provided to the Commissioner, but that it had safely shredded them.

12. [redacted] contacted the Commissioner again on 6 May 2011 and 6 July 2011, advising that it had received further faxes from the data controller. It provided copies of those faxes which comprised approximately sixty fax transmissions containing personal data relating to a total of eleven individuals.

13. In summary, the personal data contained in those faxes included:

- Payslips, including salary details and national insurance numbers;
- Bank Statements and bank account details:
- Mortgage application letters including details of an individual's monthly household budget and expenditure, prepared in relation to a mortgage application;
- Customer information summary, including contact history and the data controller's lending risk summary;
- Detailed contact details for a named customer;
- Details of that named customer's pension plan; and
- Photocopies of DVLA counterpart driving license and photo card.

- Photocopies of passports.

14. The faxes had been sent from a number of different branches in the data controller's network.

15. The Commissioner contacted the data controller on 23 August 2011. The data controller responded substantively on 23 September 2011 outlining the remedial measures it had taken.

16. The data controller also advised the Commissioner that there had been a further five or six instances of misaddressed faxes sent to [redacted] which they had advised the data controller of directly. These breaches had occurred in or around October 2009.

17. On 3 April 2012 the data controller was notified that the Commissioner had started his formal investigation, with a view to deciding if enforcement action was appropriate.

18. Despite this, further breaches occurred. These involved faxes containing personal data relating to five individuals being misdirected to [redacted] by the data controller on 26 April 2012, 29 April 2012, 4 May 2012 and 10 May 2012. Copies of this material were provided by [redacted] to the Commissioner.

19. The faxes received by [redacted] were again sent to the fax number referred to at §6 above, whereas all been intended to be sent to the data controller's Nexus fax number, referred to at §7 above.

20. In summary, the personal data contained in those faxes included:

- Pay slips and payroll details, including national insurance numbers and a P60;

- Bank Statements and a Council Tax bill;
- Mortgage account details; and
- A payslip and Deferred Bonus award scheme details, including details relating to mortgage for one of the data controller's employees.

21. Other than the six faxes sent in May 2012, the data controller was not able to ascertain whether its previous errors dating back to 2009 were due to misdialling or the inaccurate pre-programming of their fax machines. However, the data controller concluded that it was probable that the numbers were not pre-programmed incorrectly; of the six incidents in May 2012, five separate fax machines were used. For operational reasons principally relating to the age of the machines, 4 of those machines did not have the Nexus number pre-programmed into them. The data controller further found that there was no evidence that any of its documentation, letters or guidance has been issued quoting an incorrect fax number.

Mr K

22. On 13 February 2012, that data controller was advised by a private individual ("Mr K") that a number of documents had been faxed in error to him. Ten faxes had been received between 7 May 2011 and 11 February 2012. Those faxes included eight requests relating to investment plans, one death certificate and a will, one Lasting Power of Attorney and one confirmation letter in respect of a previously sent fax.
23. On 5 March 2012, Mr K contacted the data controller to advise that he had received a further fax which contained a death certificate and bereavement form.

24. The data controller identified that the eleven faxes received by Mr K had been sent from eight different fax machines at eight different locations within its organisation. It was not possible to identify where a further two faxes had been sent from. Only two of the faxes were sent with a fax header sheet containing a disclaimer.

25. The fax number which these eleven faxes were intended for was the number for the data controller's office in Edinburgh which processes customer requests. The intended fax number was one digit different from Mr K's fax number, a 2 having been substituted for an 8.

26. The data controller took remedial action to prevent further breaches by arranging with Mr K to purchase his fax number from him. This step effectively prevented any further breaches occurring which related to that fax number.

27. During the Commissioner's investigation, the data controller provided the Commissioner with a table summarising the details of occasions since 2009 on which the data controller said it had been made aware of misdirected faxes intended for the Nexus number. That table set out twenty one separate occasions of misdirected faxes. The faxes were sent from twenty separate locations by twenty different employees. All of the instances involved, (in some cases amongst other errors) the same transposition error of misdialling of the numbers 2 and 8.

28. The data controller also provided a further table detailing the occasions of misdirected faxes reported to it by Mr K. That table recorded a further ten instances of faxes being misdirected by the data controller's staff to Mr K's fax number. As noted above, these beaches also involved the transposition of the numbers 2 and 8 when dialling.

29. The data controller confirmed that, in all but one instance, the data controller in relation to the misdirected faxes containing personal data was Bank of Scotland plc trading as Halifax. In that one further instance the data controller was Lloyds TSB.

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

---

30. 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".*

31. Paragraph 9 at Part II of Schedule 1 to the Act further 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".*

32. In deciding to issue this Notice of Intent, 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.

33. The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act in that there has been a breach of the data controller's duty to comply with the Seventh Data Protection Principle.

34. In particular, the data controller has failed to take sufficient appropriate technical and organisational measures against unauthorised processing of personal data so as to effectively prevent such unauthorised processing occurring. Such measures may include providing its employees with appropriate and adequate training, the outcomes of which are suitably monitored, sufficient management training and management checks on the efficacy of the fax protocol in place, taking subsequent steps to ensure that the protocol was sufficiently adhered to, and taking timely steps to introduce the use of a more secure means of transmission such as sending material containing confidential personal data via secure electronic or other means.

35. The Commissioner notes that all of the breaches to which this notice relates arise from a consistent error, repeated across a number of the data controller's staff and offices and over a number of years, which has involved the transposition of numbers, particularly the

numbers 2 and 8, when dialling fax numbers. Given the consistent and widespread nature of this error, it appears reasonable to the Commissioner that the data controller should also have taken steps to alert its staff, not only to the general issue of misdialling, but also the prevalence of this particular error.

36. The Commissioner considers that the contravention is serious because it was persistent and repeated over a number of years.

37. Whilst the Commissioner acknowledges with approval such measures as have been, and continue to be, put in place by the data controller, those measures were not sufficient, during the period of time to which this Notice relates, to ensure a level of security appropriate to the harm that might result from any unauthorised processing and the nature of the data to be protected. The Commissioner does recognise, however, that the steps taken by the data controller have been substantial and are on-going and that collectively they represent a considerable improvement in the data controller's procedures and processes.

38. Nevertheless, the Commissioner is satisfied that the contravention is of a kind likely to cause substantial damage and substantial distress. Confidential personal data was disclosed to unauthorised third parties due to the inappropriate technical and organisational measures taken by the data controller. The failure to take appropriate technical and organisational measures has the potential to cause substantial distress to the data subjects whose confidential personal data has been disclosed to those third parties who had no reason to see it.

39. In this particular case, the data subjects would suffer from substantial distress knowing that their confidential personal data has

been disclosed to third parties and that there is the possibility that their data may have been further disseminated and possibly misused. That is so, even if those concerns do not actually materialise in practice. In this context it is important to bear in mind that the affected individuals had entrusted their detailed financial information to the data controller, on the basis that it would be dealt with in confidence.

40. If the data has been disclosed to 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.

41. The Commissioner is satisfied that section 55A (3) of the Act applies in that the data controller 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 it failed to take reasonable steps to prevent the contravention.

42. The Commissioner has taken this view because staff employed by the data controller were used to handling private individuals' detailed and confidential financial information and the data controller was aware of the confidential (and occasionally, sensitive) nature of the personal data they were sending by fax on a regular basis.

43. In the circumstances, the data controller knew, or ought to have known that there was a risk that these contraventions would occur, and would continue to occur, unless reasonable steps were taken to prevent the contravention such as providing its employees with appropriate and adequate training, the outcomes of which are suitably monitored, sufficient management training and management checks on the efficacy of the fax protocol in place, taking subsequent

steps to ensure that the protocol was sufficiently adhered to, and taking timely steps to introduce the use of a more secure means of transmission such as sending material containing confidential personal data via secure electronic or other means.

44. The risks of using simple fax facilities are self-evident and, in the Commissioner's view, were clearly apparent to the data controller from the time (at the latest) of the first reported breach in February 2009.

45. The fact that the breaches continued over a four year period, and were occurring as recently as February 2013, is clear evidence of the data controller's failure to take appropriate measures to adequately address and remedy the cause of these repeated breaches.

46. 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.

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

---

Effect of the contravention

47. The contravention is of a kind likely to result in identity fraud and financial damage to the data subjects concerned. This is so because

the personal data disclosed was of sufficient character and detail to be of actual and practical use in perpetrating fraudulent activities.

Behavioural issues

48. The data controller did not voluntarily report all of these incidents to the Commissioner and only responded once the Commissioner contacted it.

49. The data controller has been aware of this potential risk since February 2009 when the first breach occurred. Furthermore, it has had the risk highlighted to it on a number of occasions subsequently.

50. [redacted] has advised the Commissioner that there have been many more instances of it receiving misdirected faxes, but it states that it securely shredded any such faxes.

Impact on the data controller

51. The data controller has sufficient financial resources to pay a monetary penalty up to the maximum without it causing undue financial hardship.

52. Liability for this breach does not fall on any named individual.

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

---

Nature of the contravention

53. At the time of the breaches, the data controller advised the Commissioner that the Nexus fax number received 325,000 items of correspondence from various sources in an average week. The misdirected correspondence constitutes only a small percentage of that total.

54. As far as the Commissioner is aware, none of the personal data involved in any of the security breaches has been further disseminated.

Effect of the contravention

55. The personal data compromised in these breaches has been confirmed by the data controller as having been either retrieved or shredded.

Behavioural issues

56. The data controller has taken remedial action in respect of these breaches, with a view to preventing a recurrence. The Commissioner particularly notes the significant measures taken in relation to the breaches involving Mr K, which included purchasing his fax number from him. The Commissioner recognises this as indicative of the

seriousness with which the data controller treated that particular series of breaches.

57. Furthermore, in taking steps to move away from its legacy faxing system toward more secure systems, the Commissioner considers that the data controller has recognised, and seeks to address, the inherent insecurity of such a system for transmitting large volumes of confidential personal data.

58. The data controller has been cooperative with Commissioner's investigation.

Impact on the data controller

59. There is likely to be a significant impact on the reputation of the data controller as a result of these security breaches.

Other considerations

60. 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 review the sending of confidential and sensitive personal data by fax and to ensure either that alternative more secure means are used or that, at a minimum, appropriate and effective security measures are applied to the use of fax.

61. A notice of intent was served on the data controller dated 30 May 2013. The Commissioner received written representations from the data controller's Information and Data Security Manager dated 18 June 2013. 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:

- recorded more fully in this notice the remedial action taken by the data control;

- 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 proposes to impose

62. 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, he considers that a monetary penalty in the sum of £75,000 (Seventy five thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

63. In reaching this decision, the Commissioner considered other cases of a similar nature in which a monetary penalty has been imposed and the facts and aggravating and mitigating features referred to above. Of particular relevance in this case is the nature of the personal data disclosed, the potential for harm and likelihood of distress and the chronic and repeated nature of the contravention.

Payment

64. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **28 August 2013** 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

65. If the Commissioner receives full payment of the monetary penalty by **28 August 2013** the Commissioner will reduce the monetary penalty by 20% to £60,000 (Sixty thousand pounds).

Right of Appeal

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

    a. the imposition of the monetary penalty
    b. and/or;
    c. the amount of the penalty specified in the monetary penalty notice.

67. Any Notice of Appeal should be served on the Tribunal by 5pm on **28 August 2013** 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

68. 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.

69. 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 30th day of July 2013

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

4. The notice of appeal should be served on the Tribunal by 5pm on **28 August 2013** at the latest.

5. 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.

6. 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.

7. 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.

8. 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)).