Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: The British and Foreign Bible Society c/o the Bible Society

Of: Stonehill Green, Westlea, Swindon SN5 7DG

1. The Information Commissioner ("the Commissioner") has decided to issue the British and Foreign Bible Society ("the Society") with a monetary penalty under section 55A of the Data Protection Act 1998 ("the DPA"). The penalty is being issued because of a serious contravention of the seventh data protection principle by the Society.

2. This notice explains the Commissioner's decision.

Legal framework

3. The Society is a data controller, as defined in section 1(1) of the DPA in respect of the processing of personal data. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, 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.

4. The relevant provision of the DPA is the seventh data protection principle which provides, at Part I of Schedule 1 to the DPA, 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".

5. Paragraph 9 at Part II of Schedule 1 to the DPA 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".

6. Under section 55A (1) of the DPA 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 DPA 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.

7. The Commissioner has issued statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

8. The DPA implements European legislation (Directive 95/46/EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The Commissioner approaches the data protection principles so as to give effect to the Directive.

Background to the case

9. The Society is committed to translating and distributing the Bible in the UK and around the world. The Society receives card donations from its supporters based in the UK.

10. In 2009, a service account was created in an Organisational Unit (normally separate to the user accounts) of the Active Directory (AD) domain, with rights to logon to the network and access network files

for printing. The password was the same as the account username and therefore weak because the service account was not intended to be externally visible.

11. At a later date, the service account was given the additional user right to log on to the remote desk server (RDS) which enables home working for the AD user accounts. This was possibly due to the scope of the service account being extended. The password had not been changed.

12. Between 16 November and 1 December 2016, one or more attackers exploited this vulnerability by using brute-force until they guessed the weak password and accessed the service account.

13. On 1 December 2016, an attacker deployed ransomware on the RDS in the user profile of the service account.

14. The ransomware encrypted approximately 1 million shared files held on the open network, some of which contained personal data including 1,020 payment card details (card number, start/end date), 27,800 bank details (sort code and account number) and contact details in relation to 417,000 supporters (name, address, telephone number and email address)("the supporter data").

15. Fortunately, the supporter data had been backed-up the day before the attack so the Society could not be held to ransom.

16. However, the dharma variant of crisis ransomware used in the attack was able to transfer files out of the system and back to the attacker. There were also unusual peaks in outbound traffic during the attack. It is therefore considered likely that at least some of the files containing personal data held on the network were copied and extracted by the

attacker.

17. The ransomware was not detected when it was first deployed to the RDS at 16:30 on 30 November 2016 because 'on access scanning' was not enabled. The ransomware was therefore able to operate until it was detected by the daily scan at 05.00 on 1 December 2016.

18. The Commissioner has made the above findings of fact on the balance of probabilities.

19. The Commissioner has considered whether those facts constitute a contravention of the DPA by the Society and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

20. The Commissioner finds that the Society contravened the following provisions of the DPA:

21. The Society failed to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data in contravention of the seventh data protection principle at Part I of Schedule 1 to the DPA.

22. The Commissioner finds that the contravention was as follows. The Society did not have in place appropriate technical and organisational measures for ensuring so far as possible that such an incident would not occur, i.e. for ensuring that the supporter data held in files on the network could not be accessed by an attacker using ransomware.

23. In particular:

(a) The Society's IT team did not have in place sufficient oversight of its network and underlying systems.

(b) The Society did not identify the possible risks to its network when the service account was given an additional user right to logon to the RDS.

(c) The Society did not remove *all* of the shared files from the open network to a secure location with limited access.

(d) The Society did not ensure that 'on access scanning' was enabled.

24. This was an ongoing contravention from when the service account was given an additional right to logon to the RDS until the Society took remedial action on 2 December 2016.

25. The Commissioner is satisfied that the Society was responsible for this contravention.

26. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

27. The Commissioner is satisfied that the contravention identified above was serious due to the number of supporters, the nature of the data that was held on the network and the potential consequences. In those circumstances, the Society's failure to take adequate steps to

safeguard against unauthorised or unlawful access was serious.

28. The Commissioner is therefore satisfied that condition (a) from section 55A (1) DPA is met.

Contravention of a kind likely to cause substantial damage or substantial distress.

29. The relevant features of the kind of contravention are:

30. The attacker accessed the supporter data. It is considered likely that at least some of the files containing personal data held on the network were copied and extracted by the attacker. The attacker who had access to the data could also infer the religious belief of the Society's supporter's. The supporter data was clearly of interest to the attacker given the targeted nature of the attack, and that the information was encrypted in an attempt to hold the Society to ransom. The Society's network therefore required adequate security measures to protect the supporter data.

31. This is all the more so when financial and sensitive information is concerned – in particular, as regards supporters who expected that it would be held securely. This heightens the need for robust technical and organisational measures to safeguard against unauthorised or unlawful access. For no good reason, the Society appears to have overlooked the need to ensure that it had robust measures in place despite having an IT team.

32. The Commissioner therefore considers that, by reference to the features of the contravention, it was of a kind likely to cause distress. The Commissioner also considers that such distress was likely to be

substantial having regard to the number of supporters and the nature of the data that was held on the network.

33. Further, if this information has been misused by the person who had access to it, then the contravention would cause further distress to the supporters and damage such as exposing them to financial or identity fraud.

34. Financial Fraud Action UK states on its website that "Almost every week there's a news report of a data breach happening somewhere around the world. The types of information stolen often varies – from names and email addresses to debit and credit card numbers – but it can all be used by fraudsters to commit their crimes."

35. A major credit reference agency ("the agency") also states on its website that according to research they have conducted that "it takes an average of 292 days for people to discover their information has been used for fraudulent purposes." The agency also highlights that whilst the effects of fraud can be reversed the process "can take an emotional toll on you and the impact can go on for much longer than the actual fraud itself – research by the agency's Victims of Fraud team shows that it can take a staggering 300 hours to set the record straight."

36. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

Deliberate or negligent contravention

37. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that

the Society's actions which constituted the contravention were deliberate actions (even if the Society did not actually intend thereby to contravene the DPA).

38. The Commissioner considers that in this case the Society did not deliberately contravene the DPA in that sense. She considers that the inadequacies outlined above were matters of serious oversight rather than deliberate intent to ignore or bypass the provisions of the DPA.

39. The Commissioner has gone on to consider whether the Society knew or ought reasonably to have known that there was a risk that this contravention would occur. She is satisfied that this condition is met, given that the Society was aware of the supporter data that was held on the network.

40. A ransomware attack is a common and well-understood vulnerability, and known defences exist.

41. In January 2016, the ICO published 'A practical guide to IT security: Ideal for small businesses' on its website. It contains (among other things) guidance in relation to a brute-force password attack and malware.

42. In July 2016 the Society introduced a new password policy, and in September 2016 had identified that the shared files should be removed from the open network to a more secure location with limited access. The Society was also working to achieve PCI DSS compliance at the time of the incident.

43. In the circumstances, the Society ought reasonably to have known that there was a risk that that a ransomware attack would occur unless it ensured that the files containing personal data held on the network were appropriately protected.

44. Second, the Commissioner has considered whether the Society knew or ought reasonably to have known that there was a risk the contravention would be of a kind likely to cause substantial damage or substantial distress.

45. The Society ought to have known that it would cause substantial damage or substantial distress to its supporters if the information was accessed by cyber attackers over a two week period who could expose them to fraud.

46. Therefore, it should have been obvious to the Society that such a contravention would be of a kind likely to cause substantial damage or substantial distress to its supporters.

47. Third, the Commissioner has considered whether the Society failed to take reasonable steps to prevent the contravention. Again, she is satisfied that this condition is met. Reasonable steps in these circumstances would have included a regular review of configuration changes to *all* AD accounts, removing *all* of the shared files from the open network to a secure location with limited access, having 'on access scanning' that was enabled, and immediately acting upon any alert issued by the malware protection. The Society did not take those steps. The Commissioner considers there to be no good reason for that failure.

48. The Commissioner is therefore satisfied that condition (c) from section 55A (1) DPA is met.

49. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of the Society with respect to the supporter data that was held on the network. The contravention was of a kind likely to cause substantial

damage or substantial distress. The Society knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention. The conditions for issuing a monetary penalty are met in this case.

The Commissioner's decision to impose a monetary penalty

50. The Commissioner has concluded that the conditions for issuing a monetary penalty are in place. She has considered whether it is appropriate for her to exercise her discretion in favour of issuing a monetary penalty in this case. Her conclusion is that it is appropriate to do so in all the circumstances. The contravention is serious in terms of both the Society's deficiencies and the impact such deficiencies were likely to (and in this case did) have on the data subjects.

51. The issuing of a monetary penalty in this case would be fair and just. It would accord with the Commissioner's statutory guidance and regulatory objectives. It would act as an encouragement to ensure that such deficiencies are not repeated elsewhere.

52. The Commissioner has taken into account the following **mitigating features** of this case:

- The Society's network was subjected to a criminal attack.
- The Society notified the 1,020 payment card holders and provided advice.
- There is no evidence that the compromised personal data was in fact used for successful fraud activities.
- Some of the compromised personal data was historic.

- The primary account numbers had been redacted from 811 payment cards by a black marker pen.
- The Society was co-operative during the Commissioner's investigation.
- The Society has taken substantial remedial action since September 2016.
- The Society has now achieved compliance with PCI DSS.
- A monetary penalty may have a significant impact on the Society's reputation and (to an extent) its resources.

53. The fifth data protection principle at Part I of Schedule 1 to the DPA was contravened by the Society in that payment card details were held on the network for longer than was necessary for the purpose.

54. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA and this is an opportunity to remind data controllers to ensure that appropriate and effective security measures are applied to personal data.

Conclusion and amount of penalty

55. The Commissioner confirms that she has taken account of the Society's submissions in response to her Notice of Intent.

56. Notwithstanding those submissions, the Commissioner has decided that she can and should issue a monetary penalty in this case, for the reasons explained above.

57. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£100,000 (One hundred thousand pounds)**

is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

58. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **4 July 2018** 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.

59. If the Commissioner receives full payment of the monetary penalty by **3 July 2018** the Commissioner will reduce the monetary penalty by 20% to **£80,000 (Eighty thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

60. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

a) the imposition of the monetary penalty and/or;

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

61. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.

62. Information about appeals is set out in Annex 1.

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

- the period specified within 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 appealing against the monetary penalty and any variation of it has expired.

64. 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 of any sheriffdom in Scotland.

Dated the 31st day of May 2018

Signed [redacted]

Stephen Eckersley
Head of Enforcement
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Information Commissioner's Office

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 (Information Rights) (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 she ought to have exercised her 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 sent so it is received by the Tribunal within 28 days of the date of the notice.

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;

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

h) 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 (Information Rights) 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)).