DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Royal & Sun Alliance Insurance PLC

Of: St Mark's Court, Chart Way, Horsham, West Sussex, RH12 1XL

1. The Information Commissioner ("Commissioner") has decided to issue Royal & Sun Alliance Insurance PLC ("RSA") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The penalty is being issued because of a serious contravention of the seventh data protection principle by RSA.

2. This notice explains the Commissioner's decision.

Legal framework

3. RSA 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. RSA is a multinational general insurance company. It provides (among other things) personal products and services to its customers.

10. At some point between 18 May and 30 July 2015, a portable 'Network Attached Storage' device ("device") was taken offline and stolen by a member of staff or contractor who was permitted to access the data

server room ("DSR") in the RSA's premises at Horsham, West Sussex.

11. An access card and key were required to access the DSR. 40 of RSA's staff and contractors (some of whom were non-essential) were permitted to access the DSR unaccompanied.

12. The device held (among other things) personal data sets containing 59,592 customer names, addresses, bank account and sort code numbers and 20,000 customer names, addresses and credit card 'Primary Account Numbers'. However, it did not hold expiry dates or CVV numbers.

13. The device was password protected but unencrypted. It has not been recovered to date.

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

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

The contravention

16. The Commissioner finds that RSA contravened the following provisions of the DPA:

17. RSA 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.

18. The Commissioner finds that the contravention is as follows. RSA 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 device would not be stolen from the DSR by a member of staff or contractor.

19. In particular:

(a) RSA did not encrypt the datasets prior to loading them on the device.

(b) RSA failed to physically secure the device in the DSR.

(c) RSA failed to routinely monitor whether the device was still online and (if not) raise the alarm.

(d) RSA did not have CCTV installed inside the DSR.

(e) RSA failed to restrict access to the DSR to essential staff and contractors.

(f) RSA permitted its staff and contractors to access the DSR unaccompanied.

(g) RSA failed to monitor access to the DSR.

20. This was an ongoing contravention from April 2013 when RSA acquired the device until RSA took remedial action on 30 July 2015.

21. The Commissioner is satisfied that RSA was responsible for this contravention.

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

Seriousness of the contravention

23. The Commissioner is satisfied that the contravention identified above was serious due to the number of affected individuals, the nature of the personal data that was held on the device and the potential consequences. In those circumstances, RSA's failure to take adequate steps to safeguard against unauthorised or unlawful access was serious.

24. 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

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

26. The device held (among other things) personal data sets containing 59,592 customer names, addresses, bank account and sort code numbers and 20,000 customer names, addresses and credit card 'Primary Account Numbers'. However, it did not hold expiry dates or CVV numbers. Portable devices have a high risk of loss or theft and therefore require adequate security measures to protect the personal data.

27. This is all the more so when financial information is concerned – in particular, as regards RSA's customers who expected that it would be held securely. This heightens the need for robust measures – in technical and organisational terms – to safeguard against unauthorised or unlawful access. For no good reason, RSA appears to have overlooked the need to ensure that it had robust measures in place despite having the financial and staffing resources available.

28. The Commissioner therefore considers that, by reference to the features of the contravention, it was of a kind likely to cause distress to RSA's customers if they knew that their financial information might have been accessed by the member of staff or contractor who stole the device.

29. Further, RSA's customers would be distressed by justifiable concerns that this information would be further disseminated even if those concerns do not actually materialise.

30. If this information has been misused by the member of staff or contractor who stole the device, or if it was in fact disclosed to untrustworthy third parties, then the contravention would cause further distress to RSA's customers and damage, such as exposing them to blagging and possible fraud.

31. The Commissioner considers that such damage or distress is likely to be substantial having regard to the number of affected individuals and the nature of the personal data that was held on the device.

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

Deliberate or foreseeable contravention

33. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that RSA's actions which constituted those contraventions were deliberate actions (even if RSA did not actually intend thereby to contravene the DPA).

34. The Commissioner considers that in this case RSA 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.

35. The Commissioner has gone on to consider whether RSA 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 RSA was aware that the device held personal data, including financial information.

36. In the circumstances, RSA ought reasonably to have known that there was a risk that such an incident would occur unless it ensured that the personal data held on the device was technically protected and/or the device itself was physically protected.

37. Second, the Commissioner has considered whether RSA knew or ought reasonably to have known that the contravention would be of a kind likely to cause substantial damage or substantial distress. She is satisfied that this condition is met, given that RSA was aware of the nature of the information that was held on the device. RSA ought to have known that it would cause substantial distress if the information

was used in ways its customers did not envisage.

38. RSA should also have known that if the data on the device has in fact been accessed by untrustworthy third parties then it would cause further distress and also damage to RSA's customers.

39. Therefore, it should have been obvious to RSA that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the affected individuals.

40. Third, the Commissioner has considered whether RSA 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 using encryption; physically securing the device in the DSR; routinely monitoring whether the device was still online and (if not) raising the alarm; installing CCTV in the DSR; restricting access to the DSR to essential staff and contractors; permitting its staff and contractors to access the DSR only when accompanied; and monitoring access to the DSR by auditing access logs. RSA did not take those steps. The Commissioner considers there to be no good reason for that failure

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

The Commissioner's decision to issue a monetary penalty

42. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of RSA with respect to the device. The contravention was of a kind likely to cause substantial damage or substantial distress. RSA knew or

ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention.

43. The Commissioner is satisfied that the conditions from section 55A(1) DPA have been met in this case. She is also satisfied that section 55A(3A) and the procedural rights under section 55B have been complied with.

44. The latter has included the issuing of a Notice of Intent dated 12 October 2016, in which the Commissioner set out her preliminary thinking.

45. The Commissioner is accordingly entitled to issue a monetary penalty in this case.

46. The Commissioner has considered whether, in the circumstances, she should exercise her discretion so as to issue a monetary penalty. She has taken into account the representations made in response to the Notice of Intent and in other correspondence on this matter.

47. The Commissioner has also considered whether the contravention identified above could be characterised as one-off events or attributable to mere human error. She does not consider that the contravention could be characterised in those ways.

48. The Commissioner has concluded that it is appropriate for her to exercise her discretion in favour of issuing a monetary penalty in the circumstances. The contravention is serious in terms of both the RSA's deficiencies and the impact such deficiencies were likely to have on the affected individuals.

49. 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.

50. For these reasons, the Commissioner has decided to issue a monetary penalty in this case.

The amount of the penalty

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

- The device was password protected.
- The personal data held on the device was not easily accessible.
- So far as the Commissioner is aware, the information has not been further disseminated or accessed by third parties, and has not been used for fraudulent purposes.
- RSA notified its affected customers and offered free CIFAS protection for 2 years.
- RSA has now taken substantial remedial action.
- A monetary penalty may have a significant impact on the RSA's reputation and, to an extent, its resources.
- RSA has sought independent professional advice to assist with the remediation of this incident.
- There is no indication that any RSA customer has suffered a financial loss.

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

- RSA was unable to pinpoint exactly when the device was stolen.
- RSA received 195 complaints about this incident.

53. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the DPA 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.

54. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£150,000 (One hundred and fifty thousand pounds)**.

Conclusion

55. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **8 February 2017** 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.

56. If the Commissioner receives full payment of the monetary penalty by **7 February 2017** the Commissioner will reduce the monetary penalty by 20% to **£120,000 (One hundred and twenty thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

57. 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.

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

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

60. 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.

61. 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 5th day of January 2017

Signed ……..

Stephen Eckersley
Head of Enforcement
Information Commissioner's Office
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 (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)).