DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Boomerang Video Ltd

Of: Jupiter House, Callerva Park, Aldermarston, Berkshire RG7 8NN

1. The Information Commissioner ("Commissioner") has decided to issue Boomerang Video Ltd ("Boomerang Video") 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 Boomerang Video.

2. This notice explains the Commissioner's decision.

Legal framework

3. Boomerang Video 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. Boomerang Video operates a website that enables its customers to rent video games via a payment web application. The website was developed in 2005 by a third party company ("data processor"). Boomerang Video was unaware that the login page contained a coding

error.

10. On 5 December 2014, an attacker exploited this vulnerability by using SQL injection to gain access to usernames and password hashes for the WordPress section of the site. One password was shown to be a simple dictionary word based on the company's name. The attacker then uploaded a malicious web shell onto the web server to further compromise the system and gain access to the personal data of individuals stored within.

11. 0n 30 December 2014, the attacker was able to query the customer database and download text files containing 26,331 cardholder details (including name, address, primary account number, expiry date and security code). Although part of the primary account numbers were stored unencrypted, the attacker was able to gain access to the decryption key with ease, using information in configuration files on the web server. Industry guidelines prohibit the storage of the security code after payment authorisation.

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

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

The contravention

14. The Commissioner finds that Boomerang Video contravened the following provisions of the DPA:

15. Boomerang Video failed to take appropriate technical 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.

16. The Commissioner finds that the contravention was as follows. Boomerang Video did not have in place appropriate technical measures for ensuring so far as possible that such an incident would not occur, i.e. for ensuring that the personal data stored on the customer database could not be accessed by an attacker performing an SQL injection attack.

17. In particular:

18. (a) Boomerang Video failed to carry out regular penetration testing on its website that should have detected the error.

(b) Boomerang Video failed to ensure that the password for the WordPress account was sufficiently complex to be resistant to a brute-force attack on the stored hash values.

(c) Boomerang Video failed to keep the decryption key secure and prevent it being accessed by the attacker.

19. This was an ongoing contravention from 2005 when the website was developed by the data processor until Boomerang Video took remedial action on 12 January 2015.

20. The Commissioner is satisfied that Boomerang Video was responsible for this contravention.

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

Seriousness of the contravention

22. The Commissioner is satisfied that the contravention identified above was serious due to the number of data subjects, the nature of the personal data that was stored on the database and the potential consequences. In those circumstances, Boomerang Video's failure to take adequate steps to safeguard against unauthorised or unlawful access was serious.

23. 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

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

25. The customer database stored financial information. The attacker accessed 26,331 cardholder details (including name, address, primary account number, expiry date and security code). The personal data that was obtained was clearly of interest to the attacker given the targeted nature of the attack, and some of it was used for fraudulent purposes. The customer database therefore required adequate security measures to protect the personal data.

26. This is all the more so when financial information is concerned – in particular, as regards customers who expected that it would be stored securely. This heightens the need for robust technical measures to

safeguard against unauthorised or unlawful access. For no good reason, Boomerang Video appears to have overlooked the need to ensure that it had robust measures in place despite contracting with a data processor that could have carried out the work.

27. 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 data subjects and the nature of the personal data that was stored on the customer database.

28. Further, the data subjects were distressed by the fact that this information was misused by the person who had access to it, and that the contravention has caused damage to some of the data subjects by exposing them to fraud.

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

Deliberate or foreseeable contravention

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

31. The Commissioner considers that in this case Boomerang Video 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.

32. The Commissioner has gone on to consider whether Boomerang Video 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 Boomerang Video was aware of the data that was stored on the customer database, including financial information.

33. Although common, SQL injection is a well-understood vulnerability and known defences exist.

34. In the circumstances, Boomerang Video ought reasonably to have known that there was a risk that that an attack performed by SQL injection would occur unless it ensured that the personal data stored on the database was appropriately protected.

35. Second, the Commissioner has considered whether Boomerang Video 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.

36. Boomerang Video ought to have known that it would cause substantial damage or substantial distress to the data subjects if the information was accessed by an untrustworthy third party who would expose them to fraud.

37. Therefore, it should have been obvious to Boomerang Video that such a contravention would be of a kind likely to cause substantial damage and substantial distress to the data subjects.

38. Third, the Commissioner has considered whether Boomerang Video 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 carrying out regular penetration testing on its website and correcting the SQL injection vulnerability; ensuring that the password for the WordPress account was sufficiently complex; and keeping the decryption key secure. Boomerang Video did not take those steps. The Commissioner considers there to be no good reason for that failure.

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

40. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of Boomerang Video with respect to the personal data that was stored on the customer database. The contravention was of a kind likely to cause substantial damage and substantial distress. Boomerang Video 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

41. For the above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of Boomerang Video with respect to the personal data that was stored on the customer database. The contravention was of a kind likely to cause substantial damage and substantial distress. Boomerang Video 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.

42. 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.

43. The latter has included the issuing of a Notice of Intent dated 16 December 2016, in which the Commissioner set out her preliminary thinking.

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

45. 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.

46. 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.

47. 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 Boomerang Video's deficiencies and the impact such deficiencies were likely to have on the affected individuals.

48. 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.

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

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

- Boomerang Video's website was subjected to a criminal attack.
- Boomerang Video reported this incident to the Commissioner and was co-operative during her investigation.
- The data processor assured Boomerang Video that the payment security codes were not stored on the customer database.
- Boomerang Video has now taken substantial remedial action.
- A monetary penalty may have a significant impact on Boomerang Video's reputation (and to some extent) its resources.

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

- Boomerang Video was not aware of this security breach until 9 January 2015 when it was notified by its customers.
- Boomerang Video assessed itself to be compliant with the "Payment Card Industry Data Security Standard" despite failing to carry out penetration testing on its website.
- Boomerang Video received approximately 1,100 complaints and enquiries as a result of this security breach.

52. The fifth data protection principle at Part I of Schedule 1 to the DPA was contravened by Boomerang Video in that encrypted cardholder

details and "CVV" numbers were stored on the web server for longer than was necessary for its purposes.

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 remind 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 **£60,000 (Sixty thousand pounds)**.

Conclusion

55. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **12 July 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 **11 July 2017** the Commissioner will reduce the monetary penalty by 20% to **£48,000 (Forty eight 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 9th day of June 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)).