DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Instant Cash Loans Ltd trading as the Money Shop

Of: 6, Bevis Marks, London, EC3A 7BA

1. The Information Commissioner ("Commissioner") has decided to issue Instant Cash Loans Ltd trading as the Money Shop ("Money Shop") 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 the Money Shop.

2. This notice explains the Commissioner's decision.

Legal framework

3. The Money Shop 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. On 16 April 2014, a Money Shop store in Lurgan, Northern Ireland was burgled and a server was stolen ('Lurgan incident'). The server had been left on a work station in the manager's office overnight. The work station was next to a locked fire escape door through which the burglar gained entry.

10. The server was only [redacted] and the data could be accessed by a 'motivated expert user'. The store was also alarmed and monitored by CCTV. The police were immediately notified about the burglary but the server has not been recovered to date.

11. The Money Shop had a 'safe haven procedure' whereby local servers had to be locked in a separate room when a shop was closed. However, [redacted] out of the 521 Money Shop stores in the UK (including Lurgan) were too small for such a room.

12. On 27/28 May 2014, the Money Shop lost a second server that was being transported from their Head Office in Nottingham to its Swindon store by a third party courier ('Courier incident'). An encryption process had been initiated on the data but it had not been completed by the Money Shop's technician. The unencrypted data on the server could be accessed by a user with forensic knowledge and the appropriate software.

13. The servers held in total [redacted] full customer records (name, address, date of birth, telephone number, bank account and payment card details); [redacted] partial customer records (name, date of birth, maiden name or password, gender); [redacted] cheque drawer records

(name, address, telephone number, bank sort code and account numbers) and the records of [redacted] Money Shop employees (store location, employee number and password).

14. The local customer records for the Lurgan and Swindon stores were held on each server respectively but the national customer records for the rest of the UK stores were also duplicated on the servers. The customer records were backed up.

15. The Money Shop transported some servers or computer equipment holding unencrypted customer records between its Head Office in Nottingham and local stores on a weekly basis when necessary, mainly to repair and upgrade computer hardware.

16. The Money Shop did not delete customer details from their servers when they were no longer required.

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

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

The contravention

19. The Commissioner finds that the Money Shop contravened the following provisions of the DPA:

20. The Money Shop failed to take appropriate technical and organisational measures against the unauthorised processing and accidental loss of

personal data in contravention of the Seventh Data Protection Principle at Part I of Schedule 1.

21. The Commissioner finds that the contravention was as follows:

22. The Money Shop did not encrypt the personal data held on its servers or computer equipment. This was in the context of there being 521 Money Shops nationwide and transfers of some servers or computer equipment between the shops and Head Office on a weekly basis when necessary. Further, [redacted] out of 521 Money Shops did not have a 'safe haven' in which to lock a server holding personal data overnight or alternative physical security measures. This was an ongoing contravention by the Money Shop until it took remedial action following both the Lurgan and Courier incidents in May 2014.

23. The Commissioner is satisfied that the Money Shop was responsible for this contravention.

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

Seriousness of the contravention

25. The Commissioner is satisfied that the contravention identified above was serious. This is because the servers or computer equipment held [redacted] customer records. The Money Shop also had [redacted] shops nationwide that did not have a 'safe haven' and transferred some servers or computer equipment holding customer records between the shops and Head Office on a weekly basis when necessary.

26. It is accepted that the Lurgan store was locked, alarmed and monitored by CCTV at the time of the burglary and that the customer records held on the server that was lost in the Courier incident were partially encrypted. However, in the circumstances the Commissioner considers that the contravention was serious having regard to the number of affected individuals and the nature of the personal data involved.

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

Contraventions of a kind likely to cause substantial damage or substantial distress

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

29. The lost servers held in total [redacted] full customer records (name, address, date of birth, telephone number, bank account and payment card details); [redacted] partial customer records (name, date of birth, maiden name or password, gender); [redacted] cheque drawer records (name, address, telephone number, bank sort code and account numbers) and the records of [redacted] Money Shop employees (store location, employee number and password). The servers have not been recovered to date although the customer records that were held on the server in the Courier incident were partially encrypted.

30. The Commissioner considers that the contravention identified above had the following potential consequences:

31. The contravention would cause distress to the Money Shop's customers who may suspect that their personal data has been disclosed to a recipient who had no right to see that information. Further, the Money

Shop's customers would be distressed by justifiable concerns that their data could be further disseminated to unauthorised third parties. The lost servers have still not been recovered. In the circumstances, the distress suffered by the Money Shop's customers is considered to extend beyond mere irritation.

32. The Commissioner understands that [redacted] Money Shop customers who had full records on the lost servers were most at risk of fraud, although all of the customers were potentially at risk. If this information had been misused by those who had access to it, or if it was in fact disclosed to untrustworthy third parties, then the contravention would cause further distress and also substantial damage to the Money Shop's customers such as exposing them to fraud and possible financial loss.

33. The Commissioner considers that the damage and/or distress described above was likely to arise as a consequence of the kind of contravention. In other words, the Commissioner's view is that there was a significant and weighty chance that a contravention of the kind described would have such consequences.

34. The Commissioner also considers that such damage and/or distress was likely to be substantial, having regard to the number of affected individuals and the nature of the personal data involved together with the fact that the lost servers have still not been recovered. In the circumstances, the likely damage or distress was certainly more than trivial.

35. The Commissioner has also given weight to the number of affected individuals. The Commissioner considers that even if the damage or distress likely to have been suffered by each affected individual was

less than substantial, the cumulative impact would clearly pass the threshold of "substantial". In addition, given the number of affected individuals, it was inherently likely that at least a small proportion of those individuals would have been likely to suffer substantial damage or substantial distress on account of their particular circumstances. For example, disclosure to a recipient who has no right to know that a customer has borrowed money from a lender has the potential to cause acute embarrassment to the affected individual.

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

Deliberate or negligent contraventions

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

38. The Commissioner considers that in this case the Money Shop did not deliberately contravene the DPA in that sense.

39. The Commissioner has gone on to consider whether the contraventions identified above were negligent. First, he has considered whether the Money Shop knew or ought reasonably to have known that there was a risk that these contraventions would occur. He is satisfied that this condition is met, given that the Money Shop had identified the risk associated with the wholesale lack of encryption in 2013. The Money Shop also had a 'safe haven procedure' whereby local servers had to be locked in a separate room (if available) when a shop was closed. The Money Shop stores were also alarmed and monitored by CCTV.

Therefore, the Money Shop must have been aware that the servers or computer equipment must be kept secure.

40. In the circumstances, the Money Shop ought reasonably to have known that the personal data held on their servers or computer equipment would be vulnerable to a security breach in the absence of appropriate security measures.

41. Second, the Commissioner has considered whether the Money Shop knew or ought reasonably to have known that those contraventions would be of a kind likely to cause substantial damage or substantial distress. He is satisfied that this condition is met, given that the Money Shop was used to holding a large number of customer records including financial information on its servers or computer equipment in order to carry out its business of lending money. Therefore, it should have been obvious to the Money Shop that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the affected individuals.

42. Third, the Commissioner has considered whether the Money Shop failed to take reasonable steps to prevent the contravention. Again, he is satisfied that this condition is met. Reasonable steps in these circumstances would have included ensuring that the servers or computer equipment in the [redacted] shops without a 'safe haven' had Kensington locks/server cages or were encrypted. The customer records held on those servers or computer equipment that had to be transferred between the shops and Head Office on a weekly basis when necessary should have been fully encrypted. The Money Shop failed to take any of those steps.

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

The Commissioner's decision to issue a monetary penalty

44. For the reasons explained above, the Commissioner is satisfied that the conditions from section 55A(1) DPA have been met in this case. He is also satisfied that section 55A(3A) and the procedural rights under section 55B have been complied with.

45. The latter has included the issuing of a Notice of Intent dated 29 June 2015, in which the Commissioner set out his preliminary thinking. In reaching his final view, the Commissioner has taken into account the representations made in response to that Notice of Intent, as well as those made in other correspondence from the data controller.

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

47. The Commissioner has considered whether, in the circumstances, he should exercise his discretion so as to issue a monetary penalty. He has taken into account the data controller's representations made in response to the Notice of Intent and in other correspondence on this matter.

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

49. The Commissioner has decided that it is appropriate to issue a monetary penalty in this case, in light of the nature and seriousness of the contraventions, the data controller's shortcomings in terms of its

DPA duties and the risks posed to a number of individuals. He has also considered the importance of monetary penalties in dissuading future contraventions of the DPA and encouraging compliance, in accordance with his policy.

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:

- Voluntarily reported to the ICO.
- The Money Shop instructed independent consultants to conduct a full investigation into the Lurgan incident.
- The data held on the server in the Courier incident was partially encrypted.
- There is no evidence that the data on the servers has been accessed by an unauthorised third party.
- The Money Shop contacted the customers whose full records were held on the Lurgan server and offered them (and any complainants) financial protection for 12 months.
- The Money Shop has been fully co-operative with the ICO.
- The FCA has also investigated both security breaches.
- The Money Shop has now taken substantial remedial action.
- As far as the Commissioner is aware there have been no other similar security breaches.
- There will be a significant impact on the Money Shop's reputation as a result of these security breaches.

- The Courier incident was publicised in the media.

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

- The Money Shop did not identify the risk associated with the wholesale lack of encryption until 2013 and then failed to address it.
- The Money Shop received 56 complaints about the Lurgan incident.
- The Money Shop is a limited company so liability to pay a monetary penalty will not fall on any individual.

53. The Commissioner has also taken into account the fact that the Money Shop has contravened the fifth data protection principle at Part I of Schedule 1 to the DPA in that the Money Shop did not delete customer details from their servers when they were no longer required.

54. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£180,000 (One hundred and eighty thousand pounds).**

Conclusion

55. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 4 September 2015 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 3 September 2015 the Commissioner will reduce the monetary penalty

by 20% to **£144,000 (One hundred and forty four 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 4th day of August 2015

Signed .....

David Smith
Deputy Information Commissioner
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) 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 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;

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)).