Information Commissioner's Office

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Construction Materials Online Ltd

Of: Airport Business Centre, Thornbury Road, Estover, Plymouth PL6 7PP

1. The Information Commissioner ("the Commissioner") has decided to issue Construction Materials Online Ltd ("CMO") 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 CMO.

2. This notice explains the Commissioner's decision.

Legal framework

3. CMO 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. CMO operated a website environment that enabled its customers to purchase building products online such as roofing, drainage and insulation materials. A customer could enter their card details which were then encrypted and sent directly to an external payment system.

10. The website was developed in September 2009 by a third party company ("data processor"). However, CMO was unaware that the

login pages contained a coding error.

11. An attacker exploited this vulnerability in two domains by using SQL injection to gain access to usernames and password hashes for the WordPress section of the site. Many of the passwords were insecure and so easily derived from the password hash values. The attacker then uploaded a malicious web shell onto the web server to further compromise the system.

12. On 6 May 2014, the attacker was able to modify payment pages and access 669 unencrypted cardholder details at the point of entry to the website (including name, address, primary account number and security code).

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

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

The contravention

15. The Commissioner finds that CMO contravened the following provisions of the DPA:

16. CMO 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.

17. The Commissioner finds that the contravention was as follows. CMO 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 unencrypted cardholder details processed on the website could not be accessed by an attacker.

18. In particular:

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

(b) CMO failed to ensure that the passwords for the WordPress account were sufficiently complex to be resistant to a brute-force attack on the stored hash values.

19. This was an ongoing contravention from September 2009 when the website was developed by the data processor until CMO took remedial action on 16 January 2015.

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

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

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

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 processed on the website and the potential

consequences. In those circumstances, CMO'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 attacker accessed 669 unencrypted cardholder details (including name, address, primary account number and security code). The personal data that was obtained was clearly of interest to the attacker given the targeted nature of the attack, and that some of the information was used for fraudulent purposes. CMO's website 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 processed securely. This heightens the need for robust technical measures to safeguard against unauthorised or unlawful access. For no good reason, CMO 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 processed on the website.

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 could have 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 CMO's actions which constituted those contraventions were deliberate actions (even if CMO did not actually intend thereby to contravene the DPA).

31. The Commissioner considers that in this case CMO 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 CMO 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 CMO was aware of the financial information that was processed on its website.

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

34. In the circumstances, CMO 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 processed on its website was appropriately protected.

35. Second, the Commissioner has considered whether CMO 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. CMO 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 CMO that such a contravention would be of a kind likely to cause substantial damage or substantial distress to the data subjects.

38. Third, the Commissioner has considered whether CMO 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 and ensuring that the passwords for the WordPress account were sufficiently complex. CMO 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.

The Commissioner's decision to impose a monetary penalty

40. For the above reasons, CMO considers there to have been a serious contravention of the seventh data protection principle on the part of CMO with respect to the personal data that was processed on its website. The contravention was of a kind likely to cause substantial damage or substantial distress. CMO 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.

41. 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.

42. The latter has included the issuing of a Notice of Intent dated 16 February 2017, in which the Commissioner set out her preliminary thinking.

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

44. 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.

45. 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.

46. 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 CMO's deficiencies and the impact such deficiencies were likely to have (and in this case did have) on the affected individuals.

47. 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.

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

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

- CMO's website was subjected to a criminal attack.
- CMO notified the data subjects so that fraudulent transactions were intercepted.
- CMO was co-operative during the Commissioner's investigation.
- CMO has now taken substantial remedial action.
- A monetary penalty may have a significant impact on CMO's reputation and (to some extent) its resources.

50. The Commissioner has taken into account the following **aggravating feature** of this case:

- CMO was not aware of this security breach until 16 January 2015 when it was notified by a customer.
- CMO received approximately 50 complaints and enquiries from its customers as a result of this security breach.

51. The seventh data protection principle in paragraphs 11 and 12 at Part II of Schedule 1 to the DPA were also contravened in that CMO did not have a DPA compliant contract with the data processor.

52. 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.

53. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£55,000 (Fifty five thousand pounds)**.

Conclusion

54. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **30 May 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.

55. If the Commissioner receives full payment of the monetary penalty by **26 May 2017** the Commissioner will reduce the monetary penalty by 20% to **£44,000 (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.

56. 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.

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

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

59. 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.

60. 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 26th day of April 2017

Signed [redacted]

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.

Information Commissioner's Office

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)).