

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: TalkTalk Telecom Group PLC

Of: 11, Evesham Street, London W11 4AR

1. The Information Commissioner ("Commissioner") has decided to issue TalkTalk Telecom Group PLC ("Group") 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 Group.
2. This notice explains the Commissioner's decision.

Legal framework

3. The Group 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.


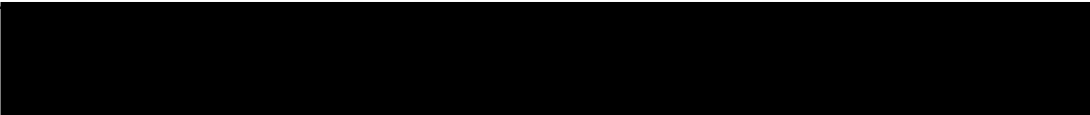
7. The Commissioner has issued statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined 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 Group is a TV, broadband, mobile and phone provider. In 2009, the Group acquired the UK operations of Tiscali. The Group was not aware that Tiscali's infrastructure included webpages ("webpages") that were still available via the internet in 2015, with access to an underlying database known as "Tiscali Master" ("database").

10. Between 15 and 21 October 2015, a cyber-attack exploited vulnerabilities in three of the webpages. The attacker was able to probe for the vulnerabilities and perform an SQL injection attack using an automated tool known as SQLmap, and then exfiltrate data from the database. User input was not validated and the vulnerable pages used outdated software libraries.
11. The database software in use was an outdated version of MySQL. The software was affected by a bug which meant that the attacker could bypass access restrictions that were in place. The bug was first publicised in 2012 when a fix was made available by the software vendor.
12. The database held personal data including the name, address, date of birth, telephone number, email address and financial information of 156,959 customers.
13. The attacker accessed the personal data of those 156,959 customers, including the bank account number and sort code of 15,656 customers.
14. 
15. The Commissioner has made the above findings of fact on the balance of probabilities.
16. The Commissioner has considered whether those facts constitute a contravention of the DPA by the Group and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

17. The Commissioner finds that the Group contravened the following provisions of the DPA:
18. The Group 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.
19. The Commissioner finds that the contravention is as follows. The Group 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 personal data held on the database could not be accessed by an attacker performing an SQL injection attack 
20. In particular:
 - (a) The Group was not aware that Tiscali's infrastructure included webpages that were still available via the internet in 2015, with access to the underlying database.
 - (b) The Group failed to remove the webpages or ensure that they were otherwise made secure.
 - (c) 

- (d) The Group was operating outdated database software that was affected by a bug for which a fix had been made available over three and a half years before the cyber-attack.
 - (e) The Group failed to undertake appropriate proactive monitoring activities to discover vulnerabilities.
21. This was an ongoing contravention until the Group took remedial action following the security breach on 21 October 2015.
 22. The Commissioner is satisfied that the Group was responsible for this contravention.
 23. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

24. 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 held on the database [REDACTED] and the potential consequences. In those circumstances, the Group's failure to take adequate steps to safeguard against unauthorised or unlawful access was serious.
25. 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

26. The relevant features of the kind of contravention are:
27. The database held the personal data of 156,959 customers, including financial information. The attacker accessed the personal data of those 156,959 customers, including the bank account number and sort code of 15,656 customers. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] as a result of this incident, the personal data that was obtained was clearly of interest to the attacker given the targeted nature of the attack, and could still be used for fraudulent purposes. The database therefore required adequate security measures to protect the personal data.
28. This is all the more so when financial information is concerned – in particular, as regards customers 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 Group appears to have overlooked the need to ensure that it had robust measures in place despite having the financial and staffing resources available.
29. 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 held on the database [REDACTED]
[REDACTED]

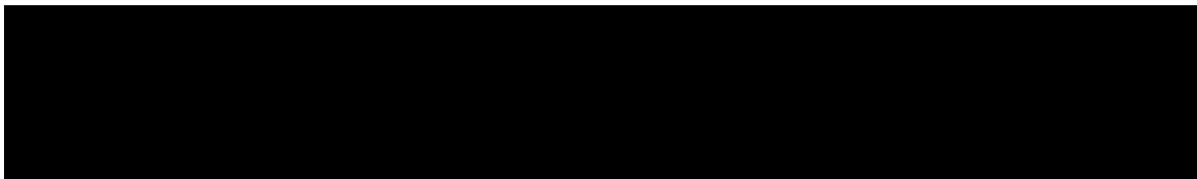
30. Further, the data subjects would be distressed by justifiable concerns that the information has been further disseminated even if those concerns do not actually materialise.
31. If this information has been misused by the person who had access to it, or if it was in fact disclosed to untrustworthy third parties, then the contravention would cause further distress to the data subjects and damage such as exposing them to blagging and possible fraud.
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 the Group's actions which constituted those contraventions were deliberate actions (even if the Group did not actually intend thereby to contravene the DPA).
34. The Commissioner considers that in this case the Group 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 the Group 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 Group should have been aware that Tiscali's infrastructure included webpages that were still available via the

internet in 2015, with access to an underlying database that held the personal data of 156,959 customers, including financial information.

36.



37. Although it is a common security vulnerability, SQL injection is well-understood and known defences exist. On 17 July 2015, there was a successful SQL injection attack that exploited the same vulnerability within the webpages. There was a second attack between 2 and 3 September 2015.

38. In the circumstances, the Group ought reasonably to have known that there was a risk that an attack performed by SQL injection would occur unless it ensured that the personal data held on the database was technically and organisationally protected.

39. Second, the Commissioner has considered whether the Group knew or ought reasonably to have known that the contravention would be of a kind likely to cause substantial damage or substantial distress.

40. She is satisfied that this condition is met, given that the Group ought to have known that it would cause substantial damage or substantial distress to the data subjects if the information was accessed by an attacker who could expose them to blagging and possible fraud.

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

42. Third, the Commissioner has considered whether the Group 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 being aware of the webpages either in 2009 or in the intervening period; removing the webpages or ensuring that they were otherwise secured; [REDACTED] ensuring that adequate testing and monitoring was in place and that appropriate technical measures were applied to its database software, either by applying a bug fix that had been available since 2012 or by upgrading that software to a more recent supported version that was unaffected by the bug in question. The Group did not take those steps. The Commissioner considers there to be no good reason for that failure.
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 above reasons, the Commissioner considers there to have been a serious contravention of the seventh data protection principle on the part of the Group with respect to the personal data that was held on the database [REDACTED]. The contravention was of a kind likely to cause substantial damage and substantial distress. The Group knew or ought to have envisaged those risks and it did not take reasonable steps to prevent the contravention. 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.

45. The latter has included the issuing of a Notice of Intent dated 10 June 2016, in which the Commissioner set out her preliminary thinking.
46. The Commissioner is accordingly entitled to issue a monetary penalty in this case.
47. 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.
48. 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.
49. 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 Group's deficiencies and the impact such deficiencies were likely to have on the data subjects.
50. 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.
51. For these reasons, the Commissioner has decided to issue a monetary penalty in this case.

The amount of the penalty

52. The Commissioner has taken into account the following **mitigating features** of this case:
- The database was subjected to a criminal attack.
 - The Group reported this incident to the Commissioner and was co-operative during her investigation.
 - The Group notified all of its customers and offered 12 months of free credit monitoring.
 - The Group has now taken substantial remedial action.
 - A monetary penalty may have a significant impact on the Group's reputation.
 - This incident has been widely publicised in the media.
53. The fifth data protection principle at Part I of Schedule 1 to the DPA was also contravened by the Group in that data was kept for longer than was necessary for its purposes.
54. The Commissioner has considered the likely impact of a monetary penalty on the Group. She has decided that the Group has access to sufficient financial resources to pay the proposed monetary penalty without causing undue financial hardship.
55. 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.
56. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£400,000 (Four**

hundred thousand pounds).

Conclusion

57. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **2 November 2016** 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.
58. If the Commissioner receives full payment of the monetary penalty by **1 November 2016** the Commissioner will reduce the monetary penalty by 20% to **£320,000 (Three 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.
59. 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.
60. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.
61. Information about appeals is set out in Annex 1.

62. 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.
63. 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 30th day of September 2016

Signed

Elizabeth Denham
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 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;
 - 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)).