TalkTalk Handed Record Fine In Data Protection Breach In The UK

Proskauer

Article By
Kelly McMullon
Daniel Ornstein
Proskauer Rose LLP
Privacy Law Blog

- Communications, Media & Internet
- Consumer Protection
- Global
- United Kingdom

Friday, October 7, 2016

TalkTalk, a major UK telecoms company, has been fined £400,000 for a data breach after they were hacked. This is a record fine given by the ICO (the UK’s data protection authority). Significantly the fine was imposed after a change of leadership this summer when Elizabeth Denham (previously the Information Commissioner in the Canadian province of British Columbia) replaced Christopher Graham as the Information Commissioner.

This record fine followed an in-depth investigation by the ICO into an attack by hackers on TalkTalk’s systems in October 2015. The hackers obtained the details of 156,959 customers, including their names, addresses, dates of birth, phone numbers and email addresses. In 15,656 cases, the hackers also gained access to bank account details and sort codes. The maximum fine the ICO can require companies to pay is £500,000.

The attack exploited vulnerabilities in webpages acquired by TalkTalk from Tiscali in 2009 to access a database. In handing out the fine, the ICO held that there had been elementary errors in TalkTalk’s efforts to safeguard personal data including:

- As part of the Tiscali acquisition, TalkTalk was unaware of webpages it had acquired;

- A bug in the database software, for which a fix was available, remained unfixed
(allowing the hackers to bypass the database access restrictions);

- Two previous attacks to the same webpages in July and September 2015 should have alerted TalkTalk to the vulnerabilities in the webpages that were hacked;

- The database was outdated and could have been upgraded to a newer version unaffected by the bug in question; and

- TalkTalk failed to proactively monitor its own activities – had it done so it would have discovered the vulnerabilities.

The new Information Commissioner, stated “TalkTalk’s failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk’s systems with ease,” and that “in spite of its expertise and resources, when it came to the basic principles of cyber-security, TalkTalk was found wanting”. The contravention was of a kind likely to cause substantial damage and substantial distress to its customers and TalkTalk should have identified the risks and taken appropriate action to prevent the data from being hacked.

The Information Commissioner further stated that “...cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this because they have a duty under law, but they must also do this because they have a duty to their customers.” This is a stark statement of the position of the new Information Commissioner and demonstrates why now, more than ever, boards and top-level executives must proactively address and be seen to be addressing cyber-security issues.

© 2020 Proskauer Rose LLP.

Source URL: https://www.natlawreview.com/article/talktalk-handed-record-fine-data-protection-breach-uk