Avoid the Worst, Put Data Security First! Warns the UK ICO

Emma L. Flett

Joanna Balata*

Data protection offences; EU law; Fines; Monetary penalty notices

The UK Information Commissioner has recently issued TalkTalk Telecom Group Plc and Royal & Sun Alliance Plc with record monetary penalties under s.55A of the Data Protection Act 1998 (DPA) for failing to take appropriate security measures with regard to their customers' personal data. Such decisions should be considered a warning shot to all data controllers who could potentially face substantially larger penalties (i.e. 4 per cent of global turnover or €20 million, whichever is higher depending on the nature and severity of the breach) for such breaches when the EU General Data Protection Regulation (GDPR) takes effect in May 2018.

Legislation

Under current legislation in the UK (i.e. the DPA):

> "[A]ppropriate 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."

The DPA further provides that such measures must ensure a level of security appropriate to: (1) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and (2) the nature of the data to be protected.

The Information Commissioner's Office may serve a data controller with a monetary penalty notice (up to a maximum of £500,000) under s.55A(1) for a serious contravention of the DPA where the data controller "knew or ought to have known of the risk" of contravention, and that it is likely to cause "substantial damage or substantial distress", but failed to take reasonable steps to prevent it. However, as set out above, under the GDPR, which comes into force on 25 May 2018, fines for such breaches could potentially increase overnight to 4 per cent of global turnover or €20 million, whichever is higher.

Royal & Sun Alliance Plc

The sun did not appear to be shining on Royal & Sun Alliance Plc (RSA) on 10 January 2017, as the ICO fined the insurance company £150,000 for failing to keep customers' information secure. At some point between 18 May and 30 July 2015, a hard drive device was stolen by a member of staff or contractor who was permitted to access the data server room in RSA's premises in West Sussex.

The device held personal data sets containing 59,592 customer names, addresses, bank account and sort code numbers, and 20,000 customer names, addresses and credit card numbers. The device was password-protected, but unencrypted.

The contravention

The ICO found that RSA had contravened the DPA by failing to take appropriate technical and organisational measures against the unauthorised or unlawful processing of personal data. In particular, RSA: (1) did not encrypt the datasets before loading them on the device; (2) failed to physically secure the device in the data server room; (3) did not have CCTV installed inside the data server room; (4) failed to restrict access to the data server room to essential staff and contractors; and (5) failed to monitor access to the data server room. This was an ongoing contravention from April 2013 when RSA acquired the device until RSA took remedial action on 30 July 2015.

ICO's decision

Given the number of affected individuals, the nature of the personal data that was held on the device and the potential consequences, the ICO confirmed that this was a serious contravention for the purposes of s.55A(1) of the DPA.

The ICO further stated that portable devices have a high risk of loss or theft and therefore require adequate security measures to protect the personal data. This is all the more so when financial information is concerned, and that RSA's customers would have expected that it would be held securely. In the ICO's view this heightened the need for robust measures, to safeguard against unauthorised or unlawful access. For "no good reason", RSA appeared to have overlooked the need to ensure that it had robust security measures in place despite having the financial and staffing resources available.

Deliberate or foreseeable contravention

Although the ICO found that the contravention identified above was not "deliberate", RSA knew or ought reasonably to have known that there was a risk that the contravention would occur. The ICO also found that RSA had failed to take reasonable steps to prevent the contravention, and that there was no good reason for that failure.

* Emma L. Flett is a Partner and Joanna Balata an Associate, Technology & IP Transactions, Kirkland & Ellis International LLP.

Monetary penalty

The ICO decided it was right to issue a monetary penalty in this case, although the ICO took into account the following mitigating factors: (1) the device was password-protected; (2) as far as the Commissioner was aware, the information had not been further disseminated or accessed by third parties, and had not been used for fraudulent purposes; (3) RSA notified its affected customers and offered free CIFAS protection for two years; (4) RSA had taken substantial remedial action; (5) a monetary penalty may have a significant impact on the RSA's reputation and, to an extent, its resources; (6) RSA had sought independent professional advice to assist with the remediation of the incident; and (7) there was no indication that any RSA customer had suffered a financial loss. She decided to issue a penalty of £150,000.

TalkTalk

In a similar scenario, the ICO issued TalkTalk Telecom Group Plc (TalkTalk) with a record monetary penalty of £400,000 under s.55A of the DPA on 5 October 2016, for failiing to keep its customer's personal data secure.

The contravention

The problem was that in 2009, after TalkTalk acquired the UK operations of Tiscali, it failed to secure an underlying customer database that was part of the acquisition. In essence, TalkTalk was unaware that Tiscali's infrastructure included web pages through which the database could be accessed and which were vulnerable to attack.

The database software was an outdated version of MySQL which was affected by a bug that left it vulnerable to an SQL injection attack. Between 15 and 21 October 2015, an SQL injection attack occurred and the attacker bypassed access restrictions to access personal data of 156,959 customers, including the bank account numbers and sort codes of 15,656 customers.

ICO's decision

The ICO found that TalkTalk failed to keep their customer's personal data secure by not having in place appropriate technical and organisational measures for ensuring that the personal data in the database could not be accessed by an attacker performing a SQL injection attack. In particular, TalkTalk was unaware of the webpages, and failed to remove or secure them, was operating outdated database software affected by a bug for which a fix had been available for three and a half years before the attack, and had failed to undertake appropriate proactive monitoring activities to discover vulnerabilities.

Moreover, the contravention was serious given the number of data subjects affected, the nature of the personal data and the potential consequences, particularly given that financial information was compromised. The ICO found that Talk Talk was all talk, and for no good reason, it "appears to have overlooked the need to ensure that it had robust measures in place despite having the financial and staffing resources available".

While the ICO accepted that the inadequacies were not the result of a deliberate intention to ignore or bypass the provisions of the DPA, they were nevertheless matters of serious oversight. TalkTalk should have known that there was a risk since SQL injection is a common security vulnerability, is well understood and known defences exist. Indeed, the company had been warned, in July 2015, when there was a successful SQL injection attack which exploited the same vulnerabilities within the webpages. This was followed by a second attack in September 2015.

Monetary penalty and PR disaster

The ICO considered that a monetary penalty in this case would be fair and just. In arriving at a figure of £400,000, the ICO took into account a number of mitigating factors: (1) this was a criminal attack; (2) TalkTalk reported the incident and was co-operative during the ICO's investigation; (3) it notified all its customers and offered 12 months of free credit monitoring; (4) it had now taken substantial remedial action; (5) the penalty might have a significant impact on TalkTalk's reputation; and (6) the incident had been widely publicised in the media. This has been a PR disaster for TalkTalk, and the fine itself pales in comparison to the commercial damage suffered by the company, including reported costs of £60 million and the loss of 101,000 customers.[1]

The GDPR looms

The ICO's fine is a record amount, but TalkTalk is fortunate that the breach took place before the GDPR comes into force on 25 May 2018. The new Regulation will see potential fines increase overnight to 4 per cent of global turnover or €20 million, whichever is higher, meaning TalkTalk would have faced an even more significant amount—a word of warning to all data controllers. Furthermore, any company that experiences data loss, regardless of whether it's their fault or a third party's fault, will have 72 hours to disclose it to the regulators where such breach is likely to result in a risk to the rights and freedoms of individuals, and to data subjects "without delay" where there is a "high risk". Therefore having breach notification processes in place and the ability to investigate data transfers and monitor cloud use will become essential.

[1] Sean Farrell, "TalkTalk counts costs of cyber-attack", *Guardian*, (2 February 2016), *https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave* [Accessed 27 June 2017].

A crash course in security

It is interesting to compare the RSA decision with the £400,000 fine slapped on TalkTalk. Some may argue that TalkTalk was by comparison hard done by or, alternatively, that the RSA got off lightly. Although the TalkTalk incident involved a cyber-attack, the cases otherwise share a number of similar aggravating and mitigating factors. TalkTalk, however, had failed to heed warnings after vulnerabilities in webpages through which the database was accessed had been exposed by two previous attacks. It will also be interesting to see how the ICO treats the recent data breach suffered by Wonga (the UK payday loan company) in April this year, which may have affected up to 245,000 customers in the UK.

In issuing the monetary penalty against RSA, the ICO stressed that its underlying objective in imposing a monetary penalty was to promote compliance with the DPA and that this was "an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data". The idea is, therefore, that the fine will act as a deterrent to other businesses against taking a lax attitude to protecting personal data.

Should either type of contravention occur under the GDPR, however, particularly if actual fraud perpetrated on customers can be linked to the personal data breach, the monetary penalty is likely to be significantly higher. It is not surprising, therefore, that companies like TalkTalk are not only looking to secure their back office operations and keep personal data locked up, but are also turning to more sophisticated security measures such as voice biometrics[2] to ensure that the interface between the company and customer is not compromised. In other words, when it comes to personal data, avoid the worst and put security first!

[2] Reported on TalkTalk's webpage, *https://www.talktalkgroup.com/articles/talktalkgroup/TalkTalk-Group--moved-articles-/2016/TalkTalk-introduces-voice-biometrics* [Accessed 6 June 2017].