COLLAS·CRILL

| Financial Services and Regulatory
| Insolvency and Corporate Disputes
| Private Client and Trusts
| Real Estate

Record fine following TalkTalk cyber attack

October 2016

The UK's Information Commissioner's Office (ICO) has issued its largest ever fine of £400,000 on TalkTalk following last year's data breach.

The current data protection legislation entitles the ICO to issue a penalty of up to £500,000.

What happened?

On 21 October 2015, TalkTalk discovered that certain webpages had been subject to a cyber attack (known as an SQL injection).

The webpages were operated by TalkTalk following its acquisition of the UK operations of Tiscali. It was later discovered that the perpetrators were able to access an underlying database (which was also part of the architecture inherited by TalkTalk) containing a large volume of customer information. Over 150,000 customers were affected, some of whom also had their bank account number and sort codes stolen.

This prompted an inquiry by the UK government into the circumstances surrounding the cyber-security breach and the response to cyber crime in general. The ICO and the Metropolitan Police also launched investigations into the matter.

The ICO took into account a range of factors, including the impact and potential distress that the breach would have on affected customers (with the risk that the disclosure of such data could have future ramifications on customers if the personal data was sold on to third parties, including identity fraud) and found that TalkTalk had failed to take appropriate measures against unauthorised or unlawful processing of personal data. This was in direct contravention of one of the fundamental principles of the UK's data protection legislation: principle 7.

This principle requires all organisations to take "*appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*".

Even though the vulnerabilities exposed were due to legacy issues with the Tiscali web pages, as TalkTalk had not taken any action following two previous attacks and had failed to update their software appropriately, the ICO found that an attack of this nature could have been avoided if TalkTalk had taken basic steps to protect its customers' information.

The ICO concluded in its report that: "*For no good reason, TalkTalk appears to have overlooked the need to ensure it had robust measures in place despite having the financial and staffing resources available*".

Lessons to be learnt

With the new General Data Protection Regulation (GDPR) due to come into force on 25 May 2018, and the prospect of a maximum sanction being the greater of EUR 20 million or 4% of annual worldwide turnover, this fine demonstrates the ICO's growing intolerance towards security breaches of any nature.

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it.

Whilst Guernsey's Data Protection Commissioner (DPC) does not have the power to issue monetary penalties under the current data protection framework, it is not yet clear what powers the Guernsey DPC will have in the future. Furthermore, with the introduction of the GDPR, a Guernsey business whose main establishment is based in another EU country, is also likely to be subject to action by the lead supervisory authority of that state, who will supervise all the processing activities of that business that have an impact throughout the EU.

Although at first blush, the TalkTalk case highlights deficiencies from an IT security perspective, this fine clearly demonstrates that data protection is a boardroom issue.

A breach of the data protection legislation may not only result in regulatory action (and possible government intervention) but may also cost businesses their customers, loss of profit and reputational damage.

As the ICO concludes – there is simply no excuse to ignore this issue any more.

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it.

For more information please contact:

Nin Ritchie

Group Partner *† // Guernsey

t:+44 (0) 1481 734273 // e:nin.ritchie@collascrill.com

Wayne Atkinson

Partner // Guernsey

t:+44 (0) 1481 734225 // e:wayne.atkinson@collascrill.com

This note is a summary of the subject and is provided for information only. It does not purport to give specific legal advice, and before acting, further advice should always be sought. Whilst every care has been taken in producing this note neither the author nor Collas Crill shall be liable for any errors, misprint or misinterpretation of any of the matters set out in it.