2 days, 20,000 accounts: Experts shocked at scale of Tesco Bank security hack

November 2016

Tesco Bank's woes continue (and not even Donald Trump can detract from the media attention). The BBC reported yesterday that a number of posts have surfaced on a variety of dark web forums boasting of thefts from Tesco Bank, months before the brand had reported the breach.

This is problematic for a number of reasons:

- If these claims can be substantiated, further reputational damage is inevitable, especially as people ask more questions. Why, for example, weren't customers notified of the risks sooner? Was Tesco Bank aware of the risks and did they do anything to mitigate this?
- This is unlikely to pacify the concerns of regulators

With the implementation of the forthcoming General Data Protection Regulation ("**GDPR**") due in 2018 (watch this space for guidance on this area), it is imperative that companies and firms start to plan their approach to GDPR compliance as soon as possible. Whilst breach reporting is not currently mandatory, organisations will have a duty to report certain breaches under the new regime.

As this story highlights, organisations should be looking at their policies and procedures now to ensure that they know how to manage a data breach: from detection – reporting – to investigation.

Whilst it might be tempting to conceal a breach from the regulator or customers, in the future, a failure to report a breach *when required* could result in a substantial fine, as well as a fine for the breach itself...

What happened?

Over the course of the weekend (5 - 6 November 2016) it was reported that approximately 20,000 customers of Tesco Bank (the banking arm of the supermarket giant) saw their money vanish from their current accounts. A further 20,000 customers reported instances of suspicious activity. The total amount stolen has not yet been revealed but some customers have cited losses of up to £2,400 each. To date, Tesco Bank has confirmed that it has refunded around 9,000 customers up to £2.5 million following the breach.

Why is it so significant?

All banks are vulnerable to cyber security breaches. Financial Fraud Action UK have said that British consumers and financial institutions lost more than £250 million in 2015 – an increase of 26% from 2014. However, a number of senior figures within the banking and cybercrime sectors have commented that a cyber-breach of this scale and concentration is "unprecedented".

How did this happen?

Details are yet to be confirmed, however, according to the Financial Times (FT) on 7 November 2016, the National Crime Agency (NCA) (who have been notified and will be leading the investigation for law enforcement) believe the hack is likely to have originated from an organised crime syndicate rather than state-sponsored actors or hacktivists.

Cyber-attacks vary in terms of sophistication and at this stage, the NCA could not comment as to how they would approach their investigation. However, experts have said that the hackers could have taken any number of routes to obtain the customer data although, given the size and speed of the attack, it is believed that hackers could have targeted a vulnerability in Tesco Bank's central system.

Regulatory impact: what is going to happen?

According to the FT, the UK's Information Commissioner's Office (ICO) has announced that it will be "looking into the details" of the cyber-breach.

Curiously, Tesco Bank was quoted by the BBC in an article on 8 November as stating that personal data "was not compromised" in the attack. This seems a little unlikely. Although financial data will not, on its own, constitute "personal data" for the purposes of data protection law, when linked with other identifiers it is difficult to conceive how a breach, on this scale, could *not* compromise personal data. On this basis it seems inevitable that the ICO will conduct an in-depth investigation into how securely Tesco Bank held its customers' data.

The ICO recently demonstrated its growing intolerance towards security breaches by fining TalkTalk £400,000 for failing to keep its customers' personal data secure. For TalkTalk, the ICO took into account a range of factors including: the impact and potential distress that the breach would have on affected customers. This is something Tesco Bank should be concerned about. The press has already reported numerous stories of customers suffering distress due to the breach, resulting in Tesco Bank's share price falling by 3% on Monday. A spokesperson for the ICO told IT business website, *IT Pro* that if, after assessing the details of the incident, it finds Tesco Bank has failed to have appropriate measures in place to keep customers' personal data secure then it will "enforce as necessary".

An independent expert has stated that given the sheer number of accounts that have been hacked, "the problem was really at Tesco's end". This does not look good for Tesco. Yes, Tesco may have won a few brownie points with the public following "Marmitegate", but this is sure to be yet another reputational blow for the multinational retailer and household name.

Whilst it is far too early to speculate as to the outcome of the investigations, if the ICO applies a similar approach to the Tesco Bank breach as it did with TalkTalk, Tesco Bank could end up receiving a hefty monetary penalty fine. However, there is one small mercy for the brand. As the breach occurred under the existing Data Protection regime, any fine will be limited to a value up to £500,000. The forthcoming General Data Protection Regulation, however, provides supervisory authorities with the power to issue much more gruesome sanctions (being the higher of 4% of annual worldwide turnover or EUR 20 million). It is not yet known what an equivalent fine might look like under this new regime (although clearly a compensation package of £2.5million will pale in comparison to GDPR fine).

Lessons:

It is a fact of modern life: no matter how expensive or sophisticated your security systems are, no organisation is immune from a data breach (especially if it is malicious and/or it is coupled with human error). There are, however, lessons to be learnt here. Irrespective of your size or the depth of your pockets, all organisations have a duty to ensure that:

- They have robust security and monitoring systems in place, which are appropriate for the type of data held
- Staff are kept properly trained as to all relevant security arrangements and protocols
- Well-structured and clear breach management procedures are in place, to answer the door, when the press and the regulators come a 'knockin'

After all, despite what events in the US might lead you to believe, not *all* publicity is necessarily *good* publicity.

For more information please contact:

Wayne Atkinson

Partner // Guernsey

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

Ben Le Page

Senior Associate // Guernsey

t:+44 (0) 1481 734244 // *e:*ben.lepage@collascrill.com