Cyber Update:

Byte-Sized Regular Updates on Cyber Liability Issues

Tesco Bank suffers hack

Tesco Bank has reported that some of its customers’ current accounts have been subject to online criminal activity, in some cases resulting in money being withdrawn fraudulently. They have taken the decision to stop temporarily online transactions from current accounts.

Benny Higgins, Tesco Bank’s CEO, said:

"We continue to work with the authorities and regulators to address the fraud . . . We can reassure customers that any financial loss as a result of this activity will be resolved fully by Tesco Bank”.

In accordance with the Financial Conduct Authority’s guidelines, Tesco Bank must refund customers immediately for unauthorised payments, unless it has evidence that there is a reason to refuse a refund e.g. if the customer acted with gross negligence, failed to protect the details of their password in a way that allowed the transaction etc.

James Hutchinson, a Partner specialising in cyber risk at Beale & Company, said:

“2016 has seen an increase in high profile cyber attacks. The nature of the fraud that has hit Tesco Bank is not clear, but they will be working to limit the damage, trace the breach and restore confidence to customers.

The implementation of the General Data Protection Regulation from May 2018 will see a significant increase in fines from a maximum of £500k to up to €20 million. The problems at Tesco Bank are a reminder to all businesses to take practical steps to mitigate the risk of cyber crime.”
UK will opt in to GDPR in May 2018

Despite the ongoing controversy over when the UK will leave the European Union, the Government has now confirmed that the UK will be implementing the General Data Protection Regulation (GDPR) in May 2018.

The Secretary of State, Karen Bradley MP used her appearance before the Culture, Media and Sports Select Committee to say:

"We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."

The Information Commissioner has called for organisations to start preparing for the implementation of the GDPR and has provided a twelve-step guide. The ICO advises organisations to start now to make sure they have the right procedures in place to detect, report and investigate a personal data breach. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

The ICO’s “12 steps to take now” guidance is available here.

ICO issues £400,000 monetary penalty to TalkTalk for data breach

The Information Commissioner’s Office has issued a record £400,000 fine to TalkTalk for security failings that allowed a cyber attacker to access customer data.

The ICO found that between 15 and 21 October 2015, the hacker accessed the personal data of 156,959 customers including their names, addresses, dates of birth, phone numbers and email addresses. In 15,656 cases, the attacker also had access to bank account details and sort codes.

Elizabeth Denham, the Information Commissioner, said:

"TalkTalk’s failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk’s systems with ease."
Yes hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not and we have taken action."

It is worth keeping in mind that had the GDPR being in effect, that fine could have been many times higher (up to €20 million).

**European Commission publishes guidance on cybersecurity for the financial sector**

On 11 October 2016, the European Commission published guidance on the G7 fundamental elements of cyber security in the financial sector.

The guidance recognises that cyber threats are among the top risks to financial stability and there has been an increase in the sophistication, frequency and persistence of such threats.

The following non-binding, high-level fundamental elements are designed to help bolster the overall cybersecurity and resilience of the international financial system:

1. **Cybersecurity strategy and framework** – establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines.

2. **Governance** – define and facilitate performance of roles and responsibilities for personnel implementing, managing, and overseeing the effectiveness of the cybersecurity strategy and framework to ensure accountability.

3. **Risk and control assessment** – identify functions, activities, products, and services—including interconnections, dependencies, and third parties—prioritise their relative importance, and assess their respective cyber risks. Identify and implement controls—including systems, policies, procedures, and training—to protect against and manage those risks within the tolerance set by the governing authority.
4. **Monitoring** – establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.

5. **Response** – Timely (a) assess the nature, scope, and impact of a cyber incident; (b) contain the incident and mitigate its impact; (c) notify internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders, third-party service providers, and customers as appropriate); and (d) coordinate joint response activities as needed.

6. **Recovery** – Resume operations responsibly, while allowing for continued remediation, including by (a) eliminating harmful remnants of the incident; (b) restoring systems and data to normal and confirming normal state; (c) identifying and mitigating all vulnerabilities that were exploited; (d) remediating vulnerabilities to prevent similar incidents; and (e) communicating appropriately internally and externally.

7. **Information sharing** – Engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders on threats, vulnerabilities, incidents, and responses to enhance defences, limit damage, increase situational awareness, and broaden learning.

8. **Continuous learning** – Review the cybersecurity strategy and framework regularly and when events warrant—including its governance, risk and control assessment, monitoring, response, recovery, and information sharing components—to address changes in cyber risks, allocate resources, identify and remediate gaps, and incorporate lessons learned.

The full text of the Guidance is available on HM Treasury’s website [here](#).

**November 2016**

For further information please contact:

James Hutchinson
Partner
T: +44 (0) 20 7469 0408
E: j.hutchinson@beale-law.com

Follow our cyber team on twitter [@cyberclaims](#)