ALERT MEMORANDUM

Key Lessons From the FCA's £16.4 Million Fine of Tesco Bank for Failings Around Cyber-Attack

8 October 2018

The £16.4 million fine imposed by the UK Financial Conduct Authority ("FCA") on Tesco Personal Finance plc ("Tesco Bank") provides a salutary lesson on the regulatory exposure associated with failing adequately to prepare for and respond to a cyber-attack – one of the FCA's stated regulatory priorities.

The episode illustrates how cybersecurity failures can expose a business not only to increasingly draconian penalties under the EU's General Data Protection Regulation ("GDPR") where personal data is involved (effective from 25 May 2018), but also to regulatory enforcement penalties where systems are not in place or are not operated effectively in a crisis.

It highlights the critical importance for businesses of:

— Establishing cybersecurity and data protection compliance firmly on the management and risk agenda. More than just the costs of doing business in the digital economy, these can give rise to serious regulatory and franchise exposure;

— Taking effective action to prevent foreseeable cyber-attacks;

— Establishing appropriate crisis management procedures and providing training to staff on how to invoke them, including through desktop exercises that provide scenario planning training; and

— Engaging constructively and immediately with the relevant authorities and stakeholders to mitigate even greater damage to the business once an attack has occurred.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

LONDON

Jonathan Kelly
+44 20 7614 2266
jkelly@cgsh.com

James Brady
+44 20 7614 2364
jbrady@cgsh.com

Gareth Kristensen
+44 20 7614 2381
gkristensen@cgsh.com

Frances Carpenter
+44 20 7614 2252
fcarpenter@cgsh.com

2 London Wall Place
London EC2Y 5AU, England
T: +44 20 7614 2200
F: +44 20 7600 1698

FCA fine and comment

On 1 October 2018, the FCA imposed a fine of £16.4 million (approx. $21.3 million) on Tesco Bank for failing to exercise due skill, care and diligence by not taking adequate steps to prevent and respond to a cyber-attack that occurred in November 2016 and which caused considerable disruption to Tesco Bank customers, when thousands of fraudulent transactions were attempted.

Mark Steward, Executive Director of Enforcement and Market Oversight at the FCA, commented that the fine *"reflects the fact that the FCA has no tolerance for banks that fail to protect customers from foreseeable risks"* and that Tesco Bank's reaction after the fraud was already under way was *"too little, too late."*

The FCA had identified cyber-attacks in its 2018/19 business plan published on 9 April 2018 as a key risk in the financial services sector, and a risk that is potentially magnified by complex and aging IT systems, outsourcing and data transfers between firms. One of the FCA's cross-sector priorities is to work to ensure increased resilience among firms to cyber-attacks and technology outages.[1]

What happened?

In November 2016, Tesco Bank was the subject of a Brazil-based cyber-attack lasting a total of 48 hours, in which attackers exploited vulnerabilities in Tesco Bank's procedures for issuing debit cards, enabling them to generate "virtual cards" with authentic card numbers, in order to steal £2.26 million.

Importantly, prior to the attack, both Visa and Mastercard had warned their members, including Tesco Bank, of a potential vulnerability to fraudulent transactions and, while Tesco Bank had taken steps to block all relevant transactions for its credit cards, it had not taken any action in regard to its debit cards.

The FCA found that a series of errors led to the prolongation of the attack. Firstly, the correct procedures for cases of fraud were not followed and it took 21 hours for contact to be made with Tesco Bank's Fraud Strategy Team, during which time nothing was done to stop the attack. Secondly, the technical measures put in place to block the fraudulent transactions were coded incorrectly and therefore ineffective. Thirdly, the operation of the technical measures was not monitored and so it took several hours to discover that they was not working and that fraudulent transactions were continuing to be made.

The FCA acknowledged that it was to Tesco Bank's credit that, once the situation had been escalated to senior management, immediate action was taken to block payments and keep customers informed. Following the attack, Tesco Bank reimbursed customers and immediately turned to improvements in security and a comprehensive review of its financial crime controls. An external report confirmed that no customer's personal data was lost.

FCA findings

After completing its review, the FCA found that Tesco's actions breached Principle 2 of the FCA Handbook (the requirement that a firm conduct its business with due skill, care and diligence) for the following reasons:

— The design of Tesco Bank's debit cards was flawed because Tesco Bank's systems were not configured to reject certain types of transactions for which the cards were not intended to be used. The cards had also been distributed in a way that meant that sequential card numbers were in circulation, which simplified the attackers' work;

— Tesco Bank's authorisation system and fraud detection rules were not adequately configured. For example, the authorisation system checked if a card expired in the future but did not verify the month and year of expiry, which made it easier for the attackers to pass the authentication process;

— The risk was both foreseeable and preventable and Tesco Bank had not responded adequately to warnings about the same type of fraud; and

— The response was not sufficiently rigorous, skilful or urgent.

[1] FCA, Business Plan 2018/19, p. 24, available at: https://www.fca.org.uk/publication/business-plans/business-plan-2018-19.pdf.

The FCA imposed a fine of £16.4 million, after categorising the seriousness of the breach as level 4 out of 5 (where 5 is the most serious). The penalty was reduced to give credit for Tesco Bank's cooperation with the FCA, and work it had carried out to strengthen its systems and controls, as well as for initiating a comprehensive customer redress exercise. Tesco Bank also received a further discount of 30% in recognition of the early-stage settlement that was reached. Without mitigation and the early settlement discount, the FCA would have imposed a penalty of almost £33.6 million (approx. $43.7 million).

UK data protection considerations and penalties in similar cyber security cases

This particular attack did not involve the theft of personal data, but cybersecurity incidents often give rise to data protection concerns, which can include unlawful access to data even if data is not stolen or lost.

The UK data protection regulator, the Information Commissioner's Office ("ICO") has extensive investigatory and enforcement powers, and where data protection findings are identified, organisations risk substantial penalties from the ICO, in addition to penalties that may be imposed by other law enforcement agencies.

While the Tesco Bank cyber-attack occurred in 2016 when the principal UK legislation was the UK Data Protection Act 1998 ("DPA 1998"), the new data protection regime under the GDPR and the UK's new Data Protection Act 2018 ("DPA 2018") has significantly increased the levels of penalties that may be imposed for data protection breaches.

The maximum penalty under the old regime of the DPA 1998 was £500,000. In contrast, the maximum penalty under the new regime of the GDPR, as supplemented by the DPA 2018, is the higher of €20 million and 4% of a group's annual worldwide turnover. 4% of the Tesco group's 2017/18 worldwide revenue is £2.3 billion.

The ICO has a track record of imposing penalties at the upper end of the range available to it under the previous regime, including fining Equifax the maximum £500,000 for its failure to protect the personal data of up to 15 million UK citizens and 146 million customers globally during a cyber-attack which took place between 13 May and 30 July 2017. Similarly, the ICO fined TalkTalk £400,000 for a cyber-attack between 15 and 21 October 2015, which affected the personal data of 159,959 customers including their names, addresses and, in some instances, their bank account details.

The FCA's trenchant criticism of Tesco Bank and the level of its fine, coupled with the maximum or near maximum levels of past fines imposed by the ICO in the cybersecurity context are a timely reminder of the importance of investment in ensuring robust data protection, cybersecurity and incident response processes that operate in practice and an effective crisis management plan. In a crisis situation, time is always of the essence and a business needs to react quickly to retain control in order to avoid what could have been a manageable problem mushrooming into a disproportionate risk to the business.

The fine also serves as a reminder of the FCA's role even after the introduction of the GDPR and as an indication that these regulatory threats, together with the emerging risk from the collective action mechanism now introduced in the data protection field, may be bringing the kind of multi-layered risk to businesses previously thought to be reserved to the USA.

…

CLEARY GOTTLIEB