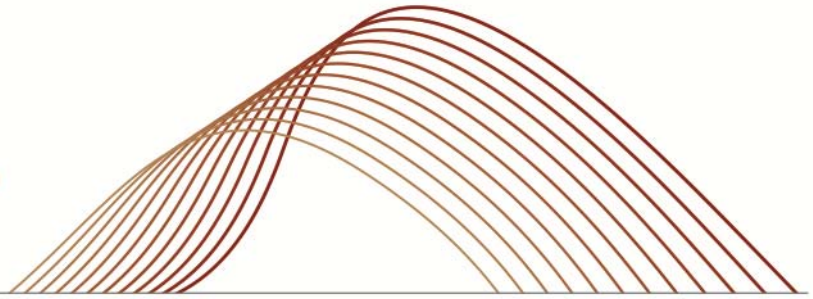
PAUL HASTINGS

STAY CURRENT



October 2018

Follow **@Paul_Hastings**

U.K. Cyber-Security Fine—The FCA Sets a Precedent

By Arun Srivastava, Sarah Pearce & Lara Kaplan

What happened?

The U.K. Financial Conduct Authority ("FCA"), in a landmark cyber-security case, fined Tesco Personal Finance plc (Tesco Bank) £16,400,000 after a foreseeable cyber attack exposed weaknesses in the design of its debit card business and affected 8,261 personal current accounts. It is the first time the FCA has fined a firm for a cyber-security breach. Tesco Bank's fine was discounted by 30% because it cooperated extensively at an early stage with the FCA in its investigation and put in place an effective consumer redress scheme.

The cyber attack took place in the early hours of a Saturday morning in November 2016 before the implementation of the GDPR or PSD2. Hackers generated authentic Tesco Bank customers' debit card numbers to enter into thousands of fraudulent debit card transactions and made contactless MSD transactions by relying on magnetic stripe rules which carry identifying information about the debit card. The hackers had created virtual cards off the back of genuine debit card numbers despite the fact that the debit cards weren't designed for contactless use.

Personal current account holders began receiving automatic text messages asking them to call Tesco Bank about suspicious activity, which is how Tesco Bank were first informed of the cyber attack. As the number of fraudulent transaction attempts increased, Tesco Bank's fraud prevention line and Twitter account were overcome with frustrated customers.

The FCA found that Tesco Bank violated Principle 2 of its principles of business: that firms should exercise due skill, care, and diligence. Four specific areas were highlighted by the FCA where Tesco Bank could have prevented this foreseeable cyber attack:

1. The design and distribution of its debit cards presented vulnerabilities to its customers and Tesco Bank didn't take appropriate cautionary measures when it decided to limit use of contactless transactions with its debit card. Tesco Bank debit cards were not designed for use with contactless transactions—however, Tesco Bank failed to disable this function so that cards could still be used in the case of transactions presented as contactless transactions. While one of the authentication processes that Tesco Bank used was the inputting of a cardholder's PIN number, this was not required in the case of a contactless transaction. The hackers were able to exploit this weakness in the Bank's processes. The cumulative weaknesses in Tesco Bank's systems meant that the hackers could effect transactions on customers' accounts with the card numbers they had generated most likely through an algorithm.

2. Failure to configure specific authentication and fraud detection rules: some debit card transactions bypassed the fraud analysis management system because the system was programmed at an account level rather than card-based.

3. Tesco Bank failed to take appropriate action to prevent the foreseeable risk of fraud. It is a member of and recipient of information from Visa and MasterCard regarding the operation of its card schemes. A year earlier Visa sent Tesco Bank a warning concerning the exact fraudulent transactions that took place. Two months before the cyber attack MasterCard also sent information concerning similar transactions to Tesco Bank and Tesco Bank failed to address either warning.

4. Tesco bank didn't respond to the cyber attack with "sufficient rigour, skill and urgency" as it failed to follow its own written procedures and the correct rules in responding to the attack. There was poor crisis management and significant coding failures, with customers complaining that they were kept on hold for hours and received no communication from the firm.

Every little helps?

It took Tesco Bank 21 hours for its internal fraud strategy team to begin addressing the error in the algorithm causing the fraudulent transactions. The number of affected and frustrated customers was increasing; meanwhile, a series of unfortunate preventable human errors led to the escalating of the cyber attack:

- Tesco Bank's internal fraud strategy team put a rule in place on their system which attempted to block transactions, but it didn't work and they didn't monitor it.

- The cyber attack occurred on a weekend and the relevant business incident manager was un-contactable because the rota for that weekend stated an incorrect telephone number.

- Once the internal fraud strategy team identified that the majority of the suspicious transactions were coming from Brazil they blocked all those transactions and drafted another rule change. Again they didn't monitor this, and the rule was ineffective because they had inputted the wrong currency code—they should have used Brazil's country code, and it took the team close to four hours to realise this.

- When external fraud experts were called in they determined that Tesco Bank's authorisation system was not capable of blocking the remaining fraudulent transactions because Tesco Bank had configured it at customer account level rather than at an individual debit card level.

Tesco Bank's financial crime controls did prevent 80% of the unauthorised transactions, and afterwards they commissioned an independent expert report into the root cause and made improvements to their financial crime systems. A consumer redress scheme was promptly established which refunded fees, charges, and interest to customers, reimbursed customers for the direct losses they had incurred, and paid compensation to some customers for distress and inconvenience and consequential losses on an individual basis.

What does this say about future EU developments? Key Takeaways

Mark Steward, Executive Director of Enforcement and Market Oversight at the FCA, opines that the lesson here is that "the standard is one of resilience, reducing the risk of a successful cyber attack occurring in the first place, not only reacting to an attack". It took the FCA two years to conclude their investigation and in the meantime the PSD2 and the GDPR have been implemented, significantly changing the backdrop and raising some interesting issues highlighted below.

A. Payment Services Directive 2

- PSD2 provides for new Strong Customer Authentication ("SCA") requirements and firms may need to review their authentication and fraud detection processes to ensure that these provide adequate protection to clients. There are many complex issues being debated in relation to SCA. Some trade bodies in the U.K. have suggested that firms might take a less robust approach than might be permitted under the strict letter of the law (PSD2 and the Regulatory Technical Standards).

- The issue of one-leg transactions where the merchant is located outside the EU has been a controversial area with the EU agreeing that a "best efforts" approach to SCA would be sufficient. However, in this case the transactions were targeted from Brazil.

- Under PSD2 firms must establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the payment services they provide.

- Firms have to establish and maintain effective incident management procedures including the detection and classification of major operational and security incidents.

B. General Data Protection Regulation

- It is unclear whether the attackers were able to access genuine card numbers for Tesco Bank customers, though Tesco Bank have stated that the cyber attack did not result in a loss or theft of customer data. GDPR is concerned with personal data, and issues that arose in this case could have GDPR implications, for instance around the appropriateness of the measures that Tesco Bank had previously taken.

- Article 25 of GDPR imposes an obligation of data protection by design and default.

- Data processors are required to implement appropriate technical and organisational measures which are designed to implement data-protection principles to protect the rights of data subjects.

- The fine could have been significantly higher as under the GDPR it could reach up to 2% of annual turnover.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

London

Sarah Pearce
44.020.3023.5168
sarahpearce@paulhastings.com

Arun Srivastava
44.020.3023.5230
arunsrivastava@paulhastings.com

Washington, D.C.

Lara Kaplan
1.202.551.1868
larakaplan@paulhastings.com