October 4, 2018

U.K. financial regulator issues £16.4 million fine for cyber fraud — and it's *not* even GDPR

Attorneys
Rohan Massey

The U.K. Financial Conduct Authority ("FCA") on Monday (1 October 2018) fined Tesco Personal Finance plc ("Tesco Bank") £16.4 million for its failings in relation to a cyber attack in November 2016.

The fine is the first issued by the FCA for cyber fraud. It comes amid a heightened focus on informational security following a series of high-profile data breaches at UK multinationals and the introduction of the General Data Protection Regulation ("GDPR"), under which fines of up to two per cent of an organisation's annual worldwide turnover can be issued for failing to implement security measures to protect personal data.

The FCA penalised Tesco Bank for failing to protect its current account holders against the "largely avoidable" attack, which exploited deficiencies in its debit cards, financial crime controls and financial crime operations team. Having been given a specific warning that fraudulent transactions had been carried out in Brazil and the U.S., the FCA said in its Final Notice that Tesco Bank failed to take appropriate action to prevent the foreseeable risk of fraud. In doing so, it breached Principle 2 of the FCA's Principles for Business, which requires regulated firms to conduct their business with due care, skill and diligence.

The attack occurred over 48 hours in November 2016, during which time the perpetrators stole approximately £2.26 million. According to the FCA, a series of errors meant that it took Tesco Bank's financial crime operations team nearly 24 hours to make contact with its fraud strategy team, which then used an incorrect currency code to block fraudulent transactions originating in Brazil.

The attack affected 8,261 of Tesco Bank's 131,000 personal current accounts and resulted in approximately £9,000 in charges and interest, and 668 unpaid direct debits, on customers' accounts. Tesco Bank subsequently reimbursed all customers for their direct losses, paid compensation to some customers for distress and inconvenience, and assessed payments for consequential losses on a case by case basis. Tesco Bank also cooperated with the FCA and agreed to an early settlement, for which its final penalty was reduced from a proposed fine of £33.6 million.

Whilst this penalty is the first issued by the FCA in relation to a cyber incident, its predecessor, the Financial Services Authority, fined a number of financial services organisations for their data security failings. These included:

- **Zurich Insurance** — Fined £2.275 million in 2010 for failing to prevent the loss of 46,000 customers' details when outsourcing insurance data to its South African division.
- **HSBC** — Fined £3 million in 2009 for a series of failings, including sending unencrypted customer data through the post; losing CDs containing customer details; and failing to store confidential customer information in locked cabinets.
- **Norwich Union Life** — Fined £1.26 million in 2007 for weaknesses in its systems and controls which allowed criminals to use publically available information to impersonate customers and obtain sensitive personal details.
- **Nationwide** — Fined £980,000 in 2007 following the theft of a laptop containing confidential customer information.
- **Capita Financial Administrators** — Fined £300,000 in 2006 after a number of its employees stole the identities of clients to make fraudulent payments worth £328,000.

Given the size and scope of the Tesco Bank penalty, the FCA has put the U.K. financial industry on notice that security failings (and weak cyber defences in particular) may give rise to fines that rival those under the GDPR. Organisations in the U.K. should therefore ensure that cyber security is firmly on the boardroom agenda — and remain alive to bad actors and regulators looking to infiltrate their defences.