Final Notice in Tesco Personal Finance Plc- Cyber Attacks and the Need for Dress Rehearsals

NOVEMBER 7, 2018

In a Final Notice dated 1 October 2018, the FCA sanctioned Tesco Personal Finance Plc for failings connected with a cyber attack it suffered in November 2016. The attack originated from Brazil and attackers managed to generate authentic Tesco bank debit card numbers with which they performed thousands of unauthorized debit card transactions. The cyber-attack lasted approximately 48 hours. It commenced at 2 am on Saturday morning. By Monday morning Tesco had managed to stem the remaining fraudulent transactions. Normal banking operations resumed on the Wednesday. Under the Notice Tesco agree to pay a fine of £16.4 million, after a 30% discount for settling during Stage 1. The Notice should be considered by compliance personnel when assessing the adequacy of their cyber-attack response procedures.

Tesco admitted failings in breach of the FCA's Principles of Business, specifically Principle 2, under which a firm is required to conduct its business with due skill, care and diligence. Essentially the failings fell into one of four categories. The first two of those categories related to the design of the debit cards and the configuration of the authentication and fraud detection rules for the firm's systems. For example, despite Tesco not intending the debit cards to be used for contactless payments, its systems weren't adequately configured to ensure that such payments would be declined. Many of these failings were specific to the technical operation of Tesco's system and are unlikely to have wider application.

The third category concerns the foreseeability and preventability of an attack. In both November 2015 and September 2016 Tesco had been forewarned that fraudulent contactless payments were originating from Brazil. Moreover, Tesco had experienced fraudulent contactless payments on its own cards prior to the attack. Given the risk that Tesco's cards could be used fraudulently, the FCA found that it had failed to take appropriate action to prevent the attack.

The fourth category is likely to prove of most interest to businesses in the regulated sector that face the risk of cyber attacks. The FCA found that Tesco had failed to respond to the cyber attack "*with sufficient rigour, skill and urgency*". Many failings identified by the FCA, were simply born of human errors, which the applicable policies and procedures could not necessarily have legislated for. The Notice cites examples of how the response team failed to follow the applicable procedures and

made errors when reacting to the event. For example, the Fraud Strategy Team entered the wrong 'Country Code' when setting the parameters to block the fraudulent payments (instead of entering the code for Brazil they entered the euro currency code). These errors allowed the fraud to continue longer than it otherwise would have.

These discrete human failings can obviously be attributed to Tesco directly for the purposes of proving the firm's regulatory liability. However, the Notice appears to suggest these errors were the product of a more systemic problem- a failure by the business to adequately embed and rehearse its crisis management procedures. As ever in the context of regulatory obligations, well documented policies and procedures are not enough- firms are expected to implement the procedures adequately. However, most policies and procedures which financial institutions are required to implement relate to processes which will not necessarily be conducted in a fast paced and pressurized environment. When under a cyber attack, time is of the essence. To that extent, the need for individuals, called upon to respond to a cyber attack, to understand the procedures and know when they should be invoked is paramount. The Notice mentions the importance of a firm rehearsing its procedures "*in a variety of scenarios*". Firms should therefore consider how they can conduct training which simulates the pressures of a cyber attacks and thereby expose the pressure points of human error.