FINAL NOTICE

To: **Tesco Personal Finance plc**

Reference Number: **186022**

Address: 2 South Gyle Crescent, Edinburgh, EH12 9FQ

Date: 1 October 2018

1. ACTION

1.1. For the reasons given in this Final Notice, the Authority hereby imposes on Tesco Personal Finance plc ("Tesco Bank") a financial penalty of £16,400,000 pursuant to section 206 of the Act.

1.2. Tesco Bank agreed to settle at an early stage of the Authority's investigation and therefore qualified for a 30% (Stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £23,428,500 on Tesco Bank.

2. SUMMARY OF REASONS

The Cyber Attack

2.1. Tesco Bank was the subject of a Cyber Attack in November 2016. The attackers most likely used an algorithm which generated authentic Tesco Bank debit card numbers and, using those "virtual cards", they engaged in thousands of unauthorised debit card transactions. The attackers exploited deficiencies in Tesco Bank's design of its debit card, its financial crime controls and in its Financial Crime Operations Team to carry out the attack. Those deficiencies left Tesco Bank's personal current account holders vulnerable to a largely avoidable incident that occurred over 48 hours and which netted the attackers £2.26 million. The attack did not involve the loss or theft of customers' personal data.

2.2. The Cyber Attack started at 02:00 on Saturday, 5 November 2016. At 04:00, Tesco Bank's fraud analysis and detection system started sending automatic text messages to Tesco Bank's personal current account holders asking them to call about "suspicious activity" on their accounts. Tesco Bank first became aware of the attack as a result of these calls. As the fraud attempts increased, the calls quickly overwhelmed Tesco Bank's fraud prevention line.

2.3. Through a series of errors, which included Tesco Bank's Financial Crime Operations Team emailing the fraud strategy inbox instead of telephoning the on-call fraud analyst (as Tesco Bank's procedures required), it took Tesco Bank's Financial Crime Operations Team 21 hours from the outset of the attack to make contact with Tesco

Bank's Fraud Strategy Team, a specialist group in the Financial Crime Operations Team. In the meantime, nothing had been done to stop the attack, the fraudulent transactions multiplied, calls from customers mounted and the attack continued.

2.4. Once the Fraud Strategy Team had been alerted, it determined that the majority of fraudulent transactions were coming from Brazil using a payment method known as "PoS 91". PoS 91 is an industry code which indicated that the attackers were making Contactless MSD transactions, transactions which rely on magnetic stripe rules which carry identifying information about the debit card. PoS 91 is used predominately outside of Europe and has no limits in terms of the value or the number of transactions. The fact that some of the transactions were successful suggested that the attackers may have obtained authentic Tesco Bank debit card "PAN" numbers, the long numbers across the front of debit cards, to make the transactions.

2.5. Having identified PoS 91 as the primary channel and Brazil as the source of most of the attempted fraudulent transactions, Tesco Bank's Fraud Strategy Team put a rule in place to block those transactions at 01:48 on Sunday, 6 November 2016.

2.6. Tesco Bank's Fraud Strategy Team did not, however, monitor the rule's operation and discovered a few hours later, that not only was the rule ineffective, but the attempted fraudulent Brazilian transactions were increasing, reaching a peak of 80,000 by Monday, 7 November 2016 (with Tesco Bank's systems blocking approximately 90%). The rule was ineffective because the Fraud Strategy Team erroneously used the Euro currency code instead of Brazil's country code when it coded the rule designed to block PoS 91 transactions originating in Brazil.

2.7. Having discovered their mistake, Tesco Bank's Fraud Strategy Team redrafted the rule, but a residual number of PoS 91 transactions continued to go through Tesco Bank's authorisation and fraud detection systems. Unable to solve the problem, the Fraud Strategy Team called external experts to help them. It took Tesco Bank until 00:59 on Monday, 7 November 2016 for the external experts to uncover the problem. The residual PoS 91 transactions were attributable to a coding error which Tesco Bank's Financial Crime Operations Team had made when it originally programmed the fraud detection system.

2.8. Once it was alerted to the incident on Sunday, 6 November 2016 at 15:00, Tesco Bank's senior management analysed the situation and took immediate action. At 23:30 on Sunday, 6 November 2016, it decided to block all online transactions and contactless transactions for debit cards, excluding Chip & PIN, ATM and online banking. The block was implemented at 03:35 on Monday, 7 November 2016. Tesco Bank removed it on Monday, 7 November 2016 at 17:10 and by Wednesday, 9 November 2018 at 08:00, it was able to remove the remaining blocks that prevented some customers from using Chip & PIN and ATM machines and normal banking operations resumed. Senior managements' actions stopped the fraudulent transactions. They updated customers regularly and deployed significant resources to return customers to their previous financial position.

Effect on customers

2.9. Although Tesco Bank's controls stopped almost 80% of the unauthorised transactions, the Cyber Attack affected 8,261 out of 131,000 Tesco Bank personal current accounts. Personal current account holders received text messages which were likely to cause customers distress in the early hours of the morning. Some customers suffered embarrassment and inconvenience when they were unable to make payments using their debit cards. Some experienced long call queues and did not always receive the help they needed from Tesco Bank's call centre. Tesco

Bank applied around £9,000 in charges and interest to customers' accounts and account balance reductions led to 668 unpaid direct debits on customers' accounts.

Consumer redress programme

2.10. Following the Cyber Attack, Tesco Bank immediately initiated a consumer redress programme and tried to limit the effect of the attack on customers. It removed pending debits from being posted to customer accounts which meant that the total amount debited from customers' accounts was £1,830. It also promptly 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. It paid compensation for consequential losses on a case by case basis.

Co-operation

2.11. Tesco Bank co-operated fully with the Authority. It independently commissioned expert reports on the root cause of the incident and its financial crime controls. It provided the reports to the Authority and took prompt steps to examine and revise its processes and procedures consistent with the recommendations in the reports. Tesco Bank made three technical presentations to the Authority on an open basis, accepted responsibility for the events, fully supported the improvements the external experts recommended and worked closely with the Authority to ensure that the Authority was apprised of the improvements. Tesco Bank also agreed to participate in a symposium to discuss the lessons it learned from the attack with banks, other regulators and law enforcement agencies.

Principle breaches

2.12. Principle 2 requires a firm to conduct its business with due skill, care and diligence. Tesco Bank is in the business of banking and fundamental to that business is protecting its customers from financial crime. On the basis of the facts and matters described in more detail below, Tesco Bank breached Principle 2 because it failed to exercise due skill, care and diligence to:

(1) Design and distribute its debit card:

(a) Tesco Bank never intended for its debit cards to be used for contactless MSD transactions, but card users could still use that payment method or "channel".

(b) Tesco Bank inadvertently issued debit cards with sequential PAN numbers. This increased the likelihood that the attackers would find the next PAN number in the sequence.

(2) Configure specific authentication and fraud detection rules:

(a) Tesco Bank configured its authorisation system to check whether the debit card expired on a date in the future instead of an exact date and month.

(b) Tesco Bank programmed its fraud analysis management system at account level instead of card level. This meant that debit card transactions for cards that had been replaced did not go through the fraud analysis management system.

(3) Take appropriate action to prevent the foreseeable risk of PoS 91 fraud:

(a) Visa warned its members, including Tesco Bank, about fraudulent PoS 91 transactions occurring in Brazil and the US. Tesco Bank immediately implemented a rule to block these transactions on its credit cards, but failed to make parallel changes to its debit cards.

(4) Respond to the Cyber Attack with sufficient rigour, skill and urgency:

(a) Tesco Bank's Financial Crime Operations team failed to follow written procedures to alert the on-call Fraud Strategy Analyst resulting in a significant delay in addressing the attack and mitigating the risks to its customers.

(b) Once the Fraud Strategy Team was alerted to the attack, it tried to draft a rule to block the fraudulent Brazilian transactions, but coded the rule incorrectly.

(c) Having drafted the incorrect rule, the Fraud Strategy Team failed to monitor the rule's operation and did not discover until several hours later, that the rule was not working and the Brazilian transactions were multiplying.

(d) Tesco Bank's crisis management procedures, including the criteria for assessing the seriousness and scale of the incident were documented, however the training materials explaining the stage at which crisis management should be invoked should have been clearer and the responsible managers should have invoked crisis management procedures earlier.

2.13. As a result, the Authority hereby imposes a financial penalty on Tesco Bank in the amount of £16,400,000 pursuant to section 206 of the Act.

2.14. The Authority makes no criticism of any third party referred to in this Notice.

3. DEFINITIONS

3.1. The definitions below are used in this Notice:

(1) "Act" means the Financial Services and Markets Act 2000.

(2) "Algorithm" means a sequence of instructions described so precisely that a computer can follow them to solve a task.

(3) "Authority" means the body corporate known as the Financial Conduct Authority.

(4) "Card Not Present Transaction" means a transaction involving the purchase of goods or services made when the physical debit card is not used to make a purchase.

(5) "Card Present Transaction" means a transaction involving the purchase of goods or services made when an actual debit card is physically used to make a purchase.

(6) "Check Digit" means the final digit at the end of the PAN.

(7) "Contactless MSD Transaction" means a transaction made when a customer presents a debit card to a PoS Terminal and the terminal interacts with the

chip associated with the debit card or where a customer makes a payment with a mobile device.

(8) "Cyber Attack" means the mass algorithmic fraud attack which affected Tesco Bank's personal current account and debit card customers from 5 to 8 November 2016.

(9) "dCVV" means Dynamic Card Verification Value.

(10) "LUHN Check" is an algorithm banks use to calculate the Check Digit and to check that the PAN number is correct.

(11) "PAN" means primary account number, the long number on the front of a debit card comprised of 15 digits plus the Check Digit.

(12) "PCA" means a Tesco Bank personal current account.

(13) "PoS" means point of sale.

(14) "PoS Entry Mode" indicates the method a customer uses to make a debit card payment.

(15) "PoS Terminal" means the device a merchant uses to accept a customer's payment and to transmit it to the bank. Typical PoS Terminals include electronic terminals and web-portals.

(16) "Principles" means the Principles for Businesses set out in the Authority's Handbook.

(17) "Relevant Period" means 1 June 2014 to 9 November 2016.

(18) "Tesco Bank" means Tesco Personal Finance plc.

4. FACTS AND MATTERS

Background

4.1. Tesco Bank is a wholly owned subsidiary of Tesco plc. Tesco Bank was originally a joint venture between The Royal Bank of Scotland plc ("RBS") and Tesco plc. Tesco plc purchased RBS' share in the joint venture on 19 December 2008. Tesco Bank offers customers a number of financial products including savings accounts, personal current accounts, credit cards, mortgages, loans, insurance products and debit cards.

4.2. Before the establishment of Tesco Bank, Tesco plc and NatWest offered customers a savings card known as the Tesco Clubcard Plus. The Tesco Clubcard Plus was linked to customers' savings accounts and allowed customers to make in-store purchases and ATM withdrawals and eventually became a Tesco Bank product. Tesco Bank also offers customers an instant access savings account, a card linked to those accounts and it started offering credit cards in July 1997.

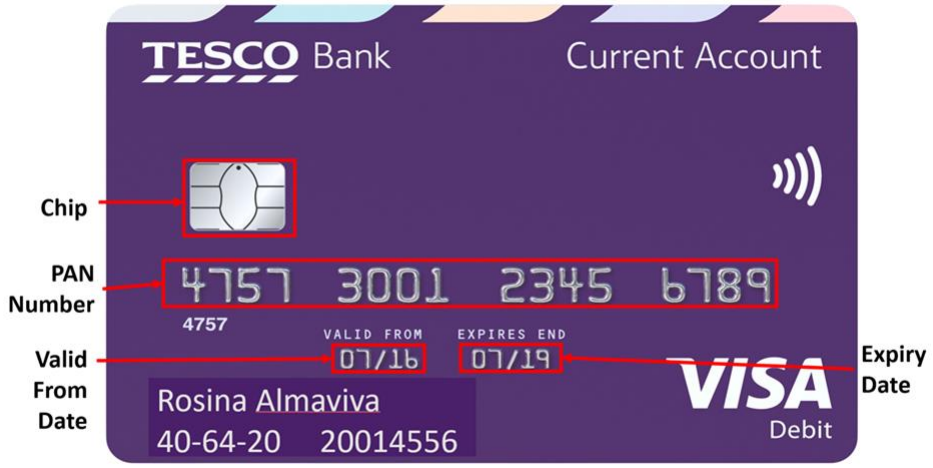
4.3. In 2010, Tesco Bank decided to offer personal current accounts to its customers and, as a feature of those accounts, debit cards. It used Tesco plc's existing base of customers as a foundation for the offering by linking the debit cards to its loyalty reward schemes including the Tesco Clubcard. Tesco Bank introduced the debit card when it started offering personal current accounts in June 2014. Tesco Bank used an authorisations system to provide basic authentication, routing, switching

and authorisation services and a separate system to provide fraud analysis and fraud detection services.

4.4. The Tesco Bank debit card is linked to a customer's personal current account. As at November 2016, at the time of the Cyber Attack, Tesco Bank had approximately 7.6 million customer accounts, including approximately 133,101 personal current accounts.

The anatomy of a Tesco Bank debit card

4.5. Tesco Bank's debit card, like all debit cards, contains a variety of information which is set out on the face of the card and encoded electronically within the card.



The PAN

4.6. The PAN is the long number on the front of the card. It comprises 15 digits plus the Check Digit. The first six digits are the BIN, the number which identifies Tesco

Bank as the issuer of the card. The next nine digits are unique to the customer's account. The remaining single digit at the end of the PAN is the Check Digit calculated by a LUHN Check. Its purpose is to ensure that the customer or merchant has not inadvertently transposed the digits in the PAN.

4.7. Before 13 December 2016, Tesco Bank issued debit cards with random PANs within a batch of 50,000 numbers. Successive batches of 50,000 numbers would not be used until all 50,000 numbers in the previous batch had been issued. The result was that thousands of Tesco Bank debit cards with valid sequential PANs were in circulation, even though Tesco Bank had neither issued them sequentially nor intended to issue them sequentially. The result was that debit cards with sequential PAN numbers made it easier for the attackers to identify authentic debit card numbers. Following the Cyber Attack, Tesco Bank revised the system it uses to issue PANs.

Issue date and expiry date

4.8. The issue date is the date from which the debit card is valid and takes the form of both a month and a year. The expiry date is the last date the debit card is valid and takes the form of both a month and a year. Tesco Bank did not programme its authorisation system to check for an exact month and year when authenticating the expiry date field on its debit cards. It was only necessary to check that the expiry date was a date in the future. Following the attack, Tesco Bank revised its expiry date checks.

Chip and PIN

4.9. The chip is embedded in the physical debit card and contains track data, the basic information required to process the card. The PIN is the customer's personal identification number. The PIN is validated differently depending upon whether the transaction is online or offline.

Three digit CVV code

4.10. The card verification value, CVV, is a three-digit code printed on or embedded in the debit card. The CVV used depends upon the type of transaction. The Tesco Bank debit card uses three types of CVV:

(1) CVV: embedded in the magnetic stripe.

(2) CVV2: printed on the signature panel on the back of the card.

(3) iCVV: embedded in the Chip.

4.11. Track data is encoded in the debit card's magnetic stripe or chip. It contains basic information required to process debit card transactions including the PAN number, the expiration year, and the CVV/iCVV. Some cards use dCVV, but Tesco Bank did not design its debit card to have the dCVV feature. Consequently, it did not expect to receive dCVV data or design its authentication system to check for dCVVs.

4.12. The signature stripe is the white stripe on the back of the physical debit card which a customer must sign before using his or her card. Depending upon the type of transaction, the card scheme rules may require the merchant to check the purchaser's signature to confirm that it matches the signature on the card.

PoS Entry Mode - methods of making debit card payments

4.13. The PoS Entry Mode refers to the data that is produced that identifies the method the merchant used to take a customer's payment. The kinds of payment methods that can be used to make debit card payments are defined by the card scheme (Visa in this case) used by the card issuer. The PoS Entry Mode should not be confused with the actual Point of Sale Terminal a merchant uses to accept a payment from a customer.

4.14. There are a variety of PoS Entry Modes, but those used by the attackers were:

(1) PoS 01/10 which indicates that the merchant is submitting the card details on behalf of a customer. PoS 01/10 is used where the customer provides his card details to the merchant via telephone or e-commerce or where the merchant has accepted payment via a carbon copy machine.

(2) PoS 91 which indicates that the transaction is a Contactless MSD transaction. PoS 91 is used for two types of Contactless MSD transactions, namely where (1) the customer makes the payment by placing the card on or near the PoS Terminal (Card Present Transaction); and (2) the customer makes a payment by placing a mobile device (which contains the card details) near the PoS Terminal (Card Not Present Transaction).

Debit card transactions

4.15. A debit card transaction is initiated when a cardholder uses a debit card to purchase goods or services from a merchant and concludes with the financial settlement of the transaction. The key stages and entities involved in a Tesco Bank debit card transaction, from the cardholder's initiation of the process to the financial settlement are outlined below.

4.16. Debit cardholders initiate transactions by providing debit card information to the merchant via a PoS Terminal. Cardholders can do this at the merchant's premises (by presenting a physical debit card to a merchant) or remotely (by entering debit card details into an online retailer's website. Tesco Bank has no influence over the way the controls operate in the merchant's domain. The merchant's responsibilities are determined by the card scheme rules and depend on the type of transaction.

4.17. Transactions made when the card is physically used to make the payment are known as Card Present transactions. Typical PoS Terminals allow the cardholder to insert the card into a chip-reading device, to position the card on or near a contactless reader, or to swipe the card through a magnetic-swipe card reader.

4.18. Transactions made when the card is not physically present at the merchant's premises are known as Card Not Present Transactions. The cardholder initiates a Card Not Present Transaction by providing debit card information to the merchant via a telephone, website or an electronic device like a mobile phone.

4.19. The merchant (via the PoS Terminal) transmits the debit card details and purchase information to the acquirer. The acquirer is a financial institution which processes the debit card transaction on behalf of the merchant. The acquirer transmits the debit card information to the card scheme.

4.20. The card scheme transmits the information to Tesco Bank, the issuer. The card scheme's rules codify the responsibilities of each party in the transaction chain.

4.21. The checks which occur during the authorisation stage determine whether the debit card is valid. Tesco Bank operates a three-stage authorisation process.

Stage 1 -- Transaction Authorisation

4.22. Tesco Bank uses an authorisation system which, at the time of the Cyber Attack, required it to perform the authorisation checks described below:

(1) **PAN**. Determine whether the PAN matches a valid PAN.

(2) **Card status**. Determine whether the debit card is active or inactive.

(3) **Expiry date**. Determine whether the debit card's expiry date is a date in the future. If the expiry date was a date in the past, it would be declined. If it was a date in the future, the transaction would not be declined.

(4) **PIN attempts**. Determine whether more than a specified number of attempts to enter the PIN have been made. Tesco Bank debit cards could not "interact" with merchant terminals to generate contactless MSD transactions because the chip does not contain the dCVV so such transactions cannot be verified. PINs did not apply to PoS 91 transactions, so this authorisation check did not apply.

(5) **Account number validation**. Determine whether the debit card corresponds to a Tesco Bank personal current account.

(6) **Account status**. Determine whether the personal current account's status is valid.

(7) **Usage limit**. Determine whether the number of times the debit card has been used exceeds a pre-determined limit.

(8) **CVV**. Determine whether the CVV/CVV2/iCCV matches Tesco Bank's records. The type of CVV supplied depends on the PoS Entry Mode which transmits the information. The CVV2 check is only performed if the CVV2 data has been provided.

(9) **Address Verification System**. Determine whether the address provided matches the address in Tesco Bank's records.

4.23. If the authorisation system validation fails, the transaction will be declined. If the transaction passes the validation checks, it passes to the second stage of the authorisation process.

Stage 2 -- Funds Availability Check

4.24. After Tesco Bank's authorisation system validates the debit card, it sends a message to an internal messaging routing system which, in turn, sends information to a funds availability checking system. The system determines whether there are sufficient funds in the customer's account to cover the transaction. If there are insufficient funds, it declines the transaction.

Stage 3 -- Fraud Screening Check

4.25. Following the first stage authorisation checks and second stage fund availability checks, the transaction is then routed to Tesco Bank's fraud analysis system for

fraud checks. The system assesses the authenticity of the purchase based on a behavioural score.

4.26. Depending upon which fraud rules are triggered, the system will either automatically send a message to the customer (typically by text message or email) or it will decline the transaction.

4.27. As a result of the authorisation process, Tesco Bank can either approve or decline the transaction. If no decision is made to decline the transaction at any of the stages outlined above, a message approving the transaction is sent back through the card scheme and the acquirer to the merchant. If the transaction is approved, the available balance on the customer's account will be reduced, but funds will not be debited from the customer's account.

4.28. The merchant then sends a message back to Tesco Bank confirming that the transaction is going ahead at which point the transaction is posted to the customer's personal current account and the monies are then debited.

The Cyber Attack

Saturday, 5 November 2016

4.29. The Cyber Attack started at 02:00 on Saturday, 5 November 2016 when the attackers transmitted 579 fraudulent transactions to Tesco Bank using authentic Tesco Bank debit card PAN numbers. Attempting a small volume of fraudulent transactions to test the strength of a bank's financial crime controls is a common technique criminals use when initiating an attack.

4.30. At 04:00, Tesco Bank's fraud detection system, started sending automatic text messages to personal current account holders. The messages said, "*This is a message from Tesco Bank Fraud Department. It's important we speak with you regarding your account. Please call us on 0345 366 1281*".

4.31. Customers started telephoning Tesco Bank's fraud prevention line following receipt of the messages. It was from these customer telephone calls that Tesco Bank originally learned about the suspicious activity that would later be known as the Cyber Attack.

4.32. At 08:00, Tesco Bank's out of hours team noted that a higher than normal number of customers were telephoning the fraud prevention line. Tesco Bank's Financial Crime Operations Team also observed unusual activity involving customers' personal current accounts and, at 08:25, sent an email to the Fraud Strategy Team's inbox. As the Financial Crime Operations Team would learn later, no one monitored the Fraud Strategy Team's inbox at weekends and the correct procedure was to telephone the on-call Fraud Strategy Analyst.

4.33. By 10:00 the volume of customer calls to the fraud prevention telephone line had risen to 137% against the volume Tesco Bank forecast for such calls. At 13:45, the Financial Crime Operations Team sent another email to the Fraud Strategy mailbox regarding suspicious transactions. By 14:00 the volume of fraudulent transactions started multiplying.

4.34. At 14:29, a member of Tesco Bank's Customer Services Team asked for further information about the volume of calls going to the fraud prevention telephone line. The member of the Customer Services Team was informed that the Financial Crime Operations Team had "passed" the concerns about the unusual activity on to the on-call Fraud Analyst to investigate".

4.35. In the meantime, the @TescoBankHelp Twitter account started receiving "tweets" about the incident. The first tweet came at 15:24 on 5 November and a further four followed. However, the tweets did not cause anyone at Tesco Bank to raise an incident. Tesco Bank ceased monitoring the tweets at 20:00 and between that time and 00:00 on 6 November, it received a further 29 tweets, 28 of which referred to fraud and to wait times on the fraud prevention telephone line.

4.36. At 15:56, another member of the Financial Crime Operations Team sent a further email about the suspicious transactions to the Fraud Strategy mailbox. At 17:32, a member of the Customer Services Team again raised questions about the suspicious transactions and asked whether they could involve compromised debit cards. The team explained that they had not yet received a response from the on-call Fraud Analyst.

4.37. Later that evening, at 21:30, the out of hours team, concerned about the increasingly high volume of calls to the fraud prevention line, tried to raise a "*P1 Incident*" with Tesco Bank's Service Desk. A P1 Incident is the highest incident level on a four-level scale and includes any incident where customer information security or IT security has been compromised. Tesco Bank's Service Desk declined to raise an incident because the suspicious transactions did not involve IT matters. The Service Desk did, however, contact the Operations Incident Manager.

4.38. At 22:40, the Major Incident Manager tried unsuccessfully to call the Business Incident Manager because the Customer Operations Incident Management Rota for that weekend did not list the correct telephone number for the on-call Business Incident Manager. The Major Incident Manager then telephoned another Business Incident Manager and, at 23:00, that Manager telephoned the on-call Fraud Strategy Analyst. At this point, 21 hours had elapsed since the first suspicious transaction entered Tesco Bank's authorisation systems and almost 15 hours had passed since the Financial Crime Operations Team sent the first email to the Fraud Strategy Team's inbox.

4.39. Alerted to the suspicious activity, the on-call Fraud Strategy Analyst notified others and, working together, they operated as the "Fraud Strategy Team" that weekend.

4.40. In the meantime, the attempted fraudulent transactions continued to rise. By 22:00 on Saturday night they reached a peak of 46,000 with Tesco Bank's systems blocking 74% of them.

Sunday, 6 November 2016

4.41. Having determined that the majority of the suspicious transactions were coming from Brazil, the Fraud Strategy Team, working remotely, decided to block all MSD contactless transactions originating from Brazil. To accomplish this, the Fraud Strategy Team drafted a rule change to the fraud analysis system which they implemented at 01:45. The Fraud Strategy Team then agreed to meet at Tesco Bank's Glasgow offices at 07:00 to review the situation. They did not put in place a system to monitor the effectiveness of the rule change.

4.42. As agreed, the Fraud Strategy Team met at Tesco Bank's Glasgow office at 07:00. They discovered that not only was the rule change not working, but the Brazilian transactions were increasing. It took the Fraud Strategy Team almost four hours to discover their mistake (that they coded the rule using the Euro currency code instead of Brazil's country code) and to re-draft the rule. They took the additional steps of blocking e-commerce transactions in the US which used PoS 81 and of blocking all US transactions excluding PoS 90 and 05 (magnetic stripe read and Chip & PIN).

4.43. At 15:00, Tesco Bank invoked its crisis management procedures.

4.44. Despite these steps the fraudulent activity continued. Unable to understand why the rules they had drafted had not completely blocked the fraudulent transactions, the Fraud Strategy Team asked external fraud experts to review the rules on Tesco Bank's authorisation and fraud detection systems.

Monday, 7 November 2016

4.45. In the early hours of Monday morning, the external fraud experts determined that the authorisation system was not blocking the residual transactions because Tesco Bank had configured the system at customer account level rather than at the individual debit card level. This meant that transactions involving debit cards that Tesco Bank had previously replaced as lost or stolen, were not passed to Tesco Bank's fraud analysis system, for fraud detection.

4.46. At 03:35, Tesco Bank implemented a block which stopped the flow of fraudulent transactions. By that time, the fraudulent transactions had reached a peak of 80,000, although Tesco Bank's systems stopped approximately 90% of them.

Tuesday, 8 November and Wednesday, 9 November 2016

4.47. Throughout Tuesday, 8 November Tesco Bank took steps to resume normal customer banking activities. By 08:00 on Wednesday, 9 November, Tesco Bank could remove the remaining blocks, including the "sticky blocks" that prevented some customers from using Chip & PIN and ATM machines until they provided authentication details, and all debit card customers were able to use their cards again.

The Cyber Attack was foreseeable

4.48. Visa issued a fraud alert to all its members, including Tesco Bank, on 4 November 2015. It warned Tesco Bank about fraudulent PoS 91 transactions occurring in Brazil and the US, exactly the kind of transactions carried out during the attack. Following the alert, Tesco Bank's Financial Crime Operations Team immediately blocked all PoS 91 transactions for Tesco Bank's credit cards, but did not make parallel changes to its debit cards. Visa posted a similar alert on its Global Fraud Information Portal on 5 November 2015. MasterCard sent an email to all its members, including Tesco Bank, on 30 September 2016 warning them of a PoS 91 attack that another UK issuer had suffered. The email said, "*Fraudulent PoS91 (mag-stripe) contactless transactions have been received from merchants in Brazil, often preceded by low value/test transactions on US based (small merchant web-sites). This is a repeat of attacks previously experienced and the subject of advisory bulletins*". Members of Tesco Bank's Fraud Strategy Team received the email, but could not recall taking any action to implement this change on debit cards.

4.49. Although Tesco Bank did not receive the article, Visa Business News published an article in 2014 which forewarned banks of the events that would subsequently transpire as the Cyber Attack. The article, "*Mitigating Fraud Risk Through Card Data Verification*" warned issuers about contactless fraud using compromised magnetic-stripe data (among other things). The article stated: "*A fraudster has counterfeited a magnetic-stripe card onto a contactless interface on a mobile device. When using the contactless interface, the bank should first recognize that this transaction has a PoS entry mode of 91 or 07 (contactless) instead of 90 (magnetic stripe). The expected CVV for a contactless interface should be dCVV or iCVV*". Moreover, Tesco Bank had experienced fraudulent PoS 91 transactions on both its credit cards and debit cards well before the Cyber Attack.

The effect of the Cyber Attack on Tesco Bank's customers

4.50. The Cyber Attack affected 8,261 personal current accounts at Tesco Bank. Personal current account holders received text messages which were likely to cause distress in the early hours of the morning. Some account holders suffered embarrassment and inconvenience when they were unable to make payments using their debit cards and others experienced long call queues and did not always receive the help they needed from call centre staff.

4.51. Tesco Bank's fraud analysis system started sending automatic text messages and emails to personal current account holders at 04:00 on Saturday, 5 November 2016 asking customers to contact Tesco Bank. The system was not configured to stop sending text messages once a pre-defined level was reached nor to send an alert to the Fraud Analysts notifying them that a large volume of alerts had been sent to customers. Tesco Bank disabled the automatic fraud alerts at 09:00 on Sunday, 6 November 2016 when it became clear that customers were not engaging in the transactions and to reduce the load on its call centre teams.

4.52. Once Tesco Bank itself became aware of the Cyber Attack, it sent a series of text messages and emails to customers. The first of those messages sent on Sunday, 6 November 2016 commencing at 13:30 and continuing to 22:30 said, "*Yesterday our fraud prevention systems identified suspicious activity on a number of customer accounts. The suspicious transactions relating to these accounts were immediately blocked to protect our customers and alerts sent. We are dealing with this as a matter of urgency but in the meantime the majority of customers can continue to use their cards using chip and pin functionality. Online servicing, telephony banking and the mobile app will continue to work as normal. We would recommend reviewing your payments and letting us know of any suspicious activity otherwise there is no need to call us at this stage*".

4.53. Tesco Bank sent another series of text messages commencing at 03:00 and continuing to 07:30 on Monday, 7 November 2016. It said, "*Over the weekend, some of our customers' current accounts have been subject to online criminal activity. Our priority is to protect your account so we have taken the precautionary measure of suspending online transactions from your account, this includes contactless transactions. You will still be able to withdraw cash and use chip and pin transactions. We are very sorry for the inconvenience and will let you know as soon as we resume normal service. For more information visit Tescobank.com/your community*".

4.54. Tesco Bank started sending text messages to its customers at 03:00 on Monday, 7 November for two reasons. Limitations in its systems prevented it from sending the text messages to all customers at one time and it wished to ensure that the customers were aware of the Cyber Attack before Tesco Bank's then CEO, Mr Benny Higgins, appeared on the BBC Radio 4's Today Programme at 07:50 on Monday morning.

4.55. It is important to note, however, that while Tesco Bank sent text messages to customers in the early hours of the morning and that those messages alarmed some customers, Tesco Bank later refined its communication strategy and provided clearer messages with more specific information to reassure them.

4.56. Tesco Bank's debit card customers faced long call queues and did not always receive the help they needed from the call centre. For example, on Sunday, 6 November 2016, Tesco Bank's fraud prevention telephone line received 3,887 telephone calls (against a forecasted 61) and that 94.4% (3,669) of the calls were "abandoned" by customers who tried to call, but were placed "on hold" for too long.

4.57. Following customer complaints, Tesco Bank compensated a number of individuals including a 74 year-old customer who tried to call Tesco Bank 11 times concerned that his life savings were lost as a result of the incident; a customer whose account was debited £450, had not slept and waited for three hours on the phone; a customer whose account was defrauded, but did not receive a text and who was advised to check Twitter for the date when funds would be restored; a customer who received a fraud text which woke up his sick child and who was given the PPI phone number to call back and did not receive a call back from Tesco Bank; and a customer with limited lung capacity who had stayed up all night following receipt of an automated text message alert.

4.58. The amount of fraudulent transactions made on individuals' personal current accounts varied. Over 600 customers' personal account balances were temporarily reduced, but not actually debited, by between £500 and £1000. Some 646 customers had fraudulent transactions exceeding £1,000 on their personal current accounts. Twenty-three customers had between £5,000 and £10,000 in fraudulent transactions on their personal current accounts. One customer had 22 fraudulent transactions totalling £65,000 on his account. Over 5,000 customers had £0 transactions "approvals" which included hotel check-in authorisation charges, situations where authorisation was received, but the transaction did not settle and where the merchant or acquirer reversed the transaction.

4.59. Tesco Bank's systems automatically applied around £9,000 in charges and interest to customers' accounts and account balance reductions led to 668 unpaid direct debits on customers' accounts. As set out below, Tesco Bank promptly reimbursed customers for these charges as part of its redress programme.

4.60. The way in which 8,261 personal current accounts were affected was that when a customer reviewed his or her account balance, it appeared to the customer that the account balance had been reduced by the amount of the unauthorised transaction. In fact, Tesco Bank delayed posting most of transactions arising from the Cyber Attack. By delaying the posting, it meant that of the 8,261 accounts affected, Tesco Bank only debited 34 accounts a total of only £1,830 and made good the amounts debited from those customers' accounts by 10 November. The net loss to Tesco Bank was £700,000.

The redress programme

4.61. Following the Cyber Attack, Tesco Bank initiated a consumer redress programme which removed pending debits from being posted to accounts, refunded fees, charges and interest to customers, reimbursed customers for the direct consequential losses they incurred, and paid compensation to customers for distress and inconvenience on a case by case basis. Only three complaints were referred to the Financial Ombudsman Service and those that were referred were upheld in Tesco Bank's favour.

Tesco Bank's governance of cyber crime

Tesco Bank's risk management framework

4.62. The UK Corporate Governance Code (Code) sets standards of good governance for UK firms and requires firms with a premium listing of equity shares in the UK to report how they have applied the Code's provisions. While Tesco Bank is not a premium listed firm and is not required to comply with the Code, the Code sets the context for examining Tesco Bank's approach to the governance of the risk of financial crime and more particularly, the risk of cyber crime.

4.63. According to the Code, a firm's board of directors is responsible for determining the nature and extent of the principal risks it is willing to take to achieve the firm's strategic objectives and for maintaining sound risk management and internal control systems. The board does this by identifying "*the nature and extent of the principal risks" the* firm faces and setting its "*risk appetite*", *the level of "the risks which the organisation is willing to take in achieving its strategic objectives*". A firm's risk appetite is designed to start with its board and to work its way through the business. The way a firm does this is through its risk appetite framework.

4.64. Tesco Bank's Board articulates Tesco Bank's strategic objectives and approves Tesco Bank's risk appetite by identifying the level of risk it is willing to take to achieve its strategic objectives. The Executive Risk Committee (ERC) and the Board Risk Committee (BRC) are responsible for reviewing emerging trends and future risks. The ERC oversees Tesco Bank's risk frameworks and ensures that the three lines of defence model is operating effectively and that they are managing their respective risks. The BRC recommends risk strategy and risk appetite decisions to the Board. The three lines of defence carry out complimentary roles and functions. Each body, in turn, has a role in developing the policies which take the Board's aspirational objectives and translates them into the practical steps required to implement those objectives.

The Board's oversight of financial crime

4.65. The ERC identified "*Cyber Crime / Financial Crime*" as among Tesco Bank's top risks. It defined the risk of Cyber Crime / Financial Crime as "*Financial Crime losses and/or associated reputational impact as a result of data theft, malicious systems outage, information security breach, or material failure of Fraud/AML systems themselves*". Tesco Bank had a standardised "*risk taxonomy*", a regular risk reporting system, operational risk processes, and it undertook annual scenario analyses. The Board is responsible for approving Tesco Bank's Financial Crime Policy which outlines Tesco Bank's approach to financial crime. It also established a variety of committees to monitor and recommend actions to mitigate the risk of cyber crime including a Cyber Crime Steering Group.

The Board's Cyber Intelligence Policy

4.66. At the time of the Cyber Attack, Tesco Bank's Board was operating on a draft Cyber Intelligence Policy. It defined cyber-related fraud or cyber-crime as "*the use of a computer network for crime ...includ[ing]: cyber enabled fraud including malware and phishing; disruption or defacement of services including Denial of Service attacks; content related offences including use of social media to make threatening or offensive comments; unauthorised access of systems; illegal collection, modification, disclosure, dissemination and storage of data; and intellectual property crimes"*. (The policy has since been incorporated into another policy.)

The Board's Financial Crime Risk Appetite

4.67. Tesco Bank's Financial Crime Policy sets out the Board's financial crime risk appetite: "*The Bank is committed to preventing and minimising external fraud losses in keeping with its risk appetite, whilst also considering the implications to customers. Risk appetite limits are approved by the Board and reviewed at least annually, as part of the risk appetite governance process*". Tesco Bank's risk appetite for external fraud risk loss for the 2016/17 financial year was £13m (1.6% of its income). Tesco Bank stayed within its risk appetite for external fraud losses taking into account both the losses arising from the Cyber Attack and all other external fraud losses arising that financial year.

The Three Lines of Defence at Tesco Bank

4.68. Having established its risk appetite for external fraud losses (including losses involving cyber-crime), Tesco Bank's three lines of defence had the job of carrying out the steps necessary to keep Tesco Bank within the risk appetite set by the Board.

The First Line of Defence

4.69. The first line of defence (First Line Business Management) is in the Customer Division. It is supported by the first line of defence risk teams. The first line risk team relevant to the Cyber Attack was the Financial Crime Operations Team which is responsible for Tesco Bank's financial crime and fraud controls, fraud case management and investigations. The Fraud Strategy Team is part of the Financial Crime Operations Team.

The Second Line of Defence

4.70. The second line of defence (Operational Risk) is accountable for the *"ownership, development and maintenance of Operational Risk Framework Policies, tools and methodologies and designing the standards against which effective Operational Risk Management will be assessed"* and is responsible for *"providing specialist advice to the 1st Line of Defence on Operational Risk Management and compliance with the ORF"* (the operational risk framework).

The Third Line of Defence

4.71. The third line of defence (Internal Audit) is responsible for providing the audit plan and an opinion on Tesco Bank's control framework four times a year.

The Three Lines of Defence's work in this area

4.72. Internal Audit raised concerns about the financial crime risks involving the debit card (referred to as the "PCA") as early as its launch date. An internal audit report entitled "*PCA Financial Crime (January 2014)"* found "*weaknesses in the design with unclear accountability for key financial crime risks such as Internal Fraud, Stores and Digital (e-crime)*". More specifically, it noted that there was *"no end to end view of the financial crime risks faced by Tesco Bank as a result of launching PCA"*. It recommended that management should assess the "*end to end financial crime risks associated with launching PCA and agree accountabilities for all of these including those which are out of scope* [of the audit]. *Accountable owners should then provide evidence of how these risks are being managed*". Tesco Bank's senior management acknowledged the issue and instructed Operational Risk to carry out such a review.

PCA Financial Crime Review

4.73. Operational Risk carried out the PCA Financial Crime Review in three phases. The first phase considered the pre-launch PCA Financial Crime Controls. The second reviewed the effectiveness of the controls during a limited "live proving friends/family" trial. The third phase reviewed the effectiveness of the controls following the launch of the PCA to customers.

4.74. The first phase report (5 February 2014) identified a variety of financial crime control deficiencies including that there were minimal internal fraud controls. The induction plan for training did not include sufficient training on how to report suspicions of fraud. The fraud risks and controls were out of date. There was no

fraud response plan in place for the PCA. The roles and responsibilities for monitoring PCA fraud trends and the management of the PCA fraud detection systems were not clear. Tesco Bank recognised the risk that the debit cards could be a target for fraudsters. The resources required to undertake ongoing fraud analysis and the management of the fraud detection systems were not in place. The fraud processes were not adequate and further development was required. On the other hand, the report said that the fraud detection system rules were *"comprehensive and should deliver an adequate level of fraud detection at launch"* although it noted that some *"minor additions and amendments"* were required. The risks were closed on 3 June 2014 following the production of a detailed external fraud risk register completed by the Financial Crime Team.

4.75. The second phase report (23 May 2014) identified two risk issues for resolution. The first finding (outstanding) was that team managers needed training in the fraud analysis systems. The second finding was that the quality assurance approach to the management and oversight of the fraud analysis system and fraud alerts needed to ensure that there was appropriate end to end oversight in place, considering the timeliness of the checks needed to ensure that the system was reviewed.

4.76. The third phase report (23 December 2014) said that volumes of confirmed PCA fraud remained low, but noted that they were unable to validate the extent to which the fraud alerts were working properly; the approach to management quality control checks carried out on the system generated fraud alerts required improvement.

2nd Line Risk Assurance Report Review of Financial Crime Threat Intelligence Review

4.77. Operational Risk carried out a review of the work of Tesco Bank's Cyber Intelligence Team, a team within Tesco Bank's Security Team, was doing to combat cyber-crime. It published its findings in a report entitled, *2nd Line Risk Assurance Report Review of Financial Crime Threat Intelligence Review (23 December 2015)*. The Cyber Intelligence Team was formed in April 2015 and they analysed intelligence gathered from a wide variety of sources and provided that intelligence to appropriate stakeholders across Tesco Bank's business to ensure that Tesco Bank managed financial crime within its risk appetite.

4.78. The report acknowledged that the Cyber Intelligence Team had made significant progress in putting structures in place to bring information about cyber-crime to the attention of senior management and the relevant business areas and in identifying current and emerging cyber-crime threats to Tesco Bank generally.

4.79. The report also identified several concerns. It noted that timely data was "*imperative"* for an effective threat intelligence framework to make provision for the "*immediate assessment and dissemination of data*", but noted that there were no timescales in place for processing threat intelligence data. It also said that there was no clear audit trail to show when intelligence was being received and processed by the Threat Intelligence Team.

2nd Line Risk Assurance Report Review of: Card Not Present (CNP)

4.80. Five months before the Cyber Attack, Operational Risk carried out a review of CNP fraud. It published its findings in a report entitled, "*2nd Line Risk Assurance Report Review of: Card Not Present (CNP)"* dated 8 June 2016. The review looked at CNP fraud affecting both Tesco Bank credit cards and debit cards.

4.81. The report noted that the low alert volumes made it difficult to assess a *"strong pattern of CNP behaviours"* on the debit cards compared to that of credit cards. It warned the Financial Crime Strategy Team to continue to enhance CNP MI and to develop the overall fraud detection rate. The report states that, as at March 2016, there was significant reliance on customers to inform Tesco Bank of fraud on their PCA accounts. The actions outlined in the report were addressed and closed on 31 August 2016.

Fraud & AML Capability Best Practice Review

4.82. Following the Cyber Attack, Tesco Bank commissioned a consultancy firm to assess its financial crime controls, operations and customer experience and to help it develop a plan to address the gaps it identified. The consultants provided its findings and recommendations to Tesco Bank in a report entitled, *Fraud & Capability Best Practice Review (15 August 2017)*.

4.83. The consultants found that Tesco Bank's senior management had a desire to manage financial crime risk, but Tesco Bank's customer security operating model was behind its peers and "*not sustainable*". Among other things, the report observed that there was limited activity to assess and trace risks from end-to-end across the control framework and that work had started on the assessment of the fraud risks and controls in place within each product area, but that work was constrained by current capacity in the Fraud Strategy area.

4.84. The Tesco Bank executive who presented the report to Tesco Bank's Executive Committee thought that the findings were reasonable.

Conclusion

4.85. Tesco Bank's financial crime governance framework was clear and each body within the framework had an appropriate role and each body worked together to achieve the common purpose of mitigating the risk of cyber crime occurring at Tesco Bank. In particular:

(1) The Board identified its strategic objectives and approved Tesco Bank's risk appetite by identifying the level of risk it was willing to take to achieve its strategic objectives. Tesco Bank delegated specific work to the ERC (to oversee the risk frameworks and the three lines of defence) and the BRC (to recommend risk strategy and risk appetite decisions to the Board).

(2) The ERC identified cyber crime and financial crime as among Tesco Bank's top risks. The BRC recommended and the Board ratified a risk appetite for financial crime which it divided into internal fraud (zero tolerance) and external fraud risk which included cyber crime (£13m).

(3) The first line of defence identified the risks from the perspective of the business. Operational Risk, as the second line of defence carried out several risk review and mitigation projects: the PCA Financial Crime Review (a three-phase project designed to identify and resolve financial crime risks before Tesco Bank made the debit card available to customers); and Assurance Reports (one report examined Tesco Bank's security team another card not present fraud). The work of Tesco Bank's internal audit function was not prominent, but Tesco Bank did commission external audit reviews from accountancy firms.

4.86. While Tesco Bank's cyber crime framework was appropriate, the framework is only as good as the individuals who work within it. Tesco Bank was vulnerable to the

attack because individuals failed to exercise due skill, care and diligence to design and distribute the debit card, configure specific authentication and fraud detection rules, take appropriate action to prevent the foreseeable risk of PoS 91 fraud, and respond to the attack with sufficient rigour, skill and urgency.

4.87. According to a National Audit Office report, the true cost of online fraud is unknown, but is likely to be billions of pounds. In the year ending 30 September 2016, there were 1.9 million incidents of cyber-related fraud in England and Wales.

4.88. Financial institutions cannot eliminate the risk of cyber crime. They can, however, take appropriate steps to mitigate the risk of cyber crime occurring and ensure that their cyber-crime controls are well designed, that the individuals who design and manage those controls understand how they work, and that their crisis management plans are clear and well-rehearsed.

5. FAILINGS

5.1. The regulatory provisions relevant to this Notice are referred to in Annex A.

Principle Breaches

5.2. Principle 2 requires a firm to conduct its business with due skill, care and diligence. Tesco Bank is in the business of banking and fundamental to that business is protecting its customers from financial crime. Tesco Bank breached Principle 2 because it failed to exercise due skill, care and diligence to:

(1) Design and distribute the debit card:

(a) *Contactless MSD (PoS 91).* Tesco Bank did not intend for its debit cards to be used for contactless MSD transactions because there was limited support for contactless MSD transactions in Europe and there were difficulties with the dCVV verification method used to authenticate the card. Having taken that decision, Tesco Bank did not take the steps which followed from that decision. It should have included PoS 91 in the Visa test scripts and configured its authorisation and fraud analysis systems to decline PoS 91 transactions. The failure to take these steps left Tesco Bank's personal current account customers vulnerable to fraudulent transactions made using PoS 91. Those transactions accounted for the majority of the fraudulent transactions (£2.24m) which occurred in the attack.

(b) *PAN numbers.* The *attack*ers algorithmically generated authentic debit card numbers to engage in fraudulent transactions on customers' personal current accounts. Tesco Bank was vulnerable to this because it randomly issued PANs to customers within a batch of 50,000 numbers. The next batch of 50,000 numbers would not be used until all 50,000 numbers in the first batch had been issued. The result was that the debit cards in circulation had sequential PAN numbers. This simplified the attackers' work.

(2) Configure specific authentication and fraud detection rules:

(a) *Expiry date.* Tesco Bank configured its authorisation system to check whether the debit card expired on a date in the future, not the exact month and year. This made it easier for the attackers to get through the debit card authentication process.

(b) *Fraud detection rules.* The Financial Crime Operations Team programmed Tesco Bank's fraud analysis system at account level instead of card level. This meant that transactions involving debit cards that Tesco Bank had previously replaced as lost, stolen or expired, did not go through the fraud analysis system. This affected 19,240 debit cards.

(3) Take appropriate action to prevent the foreseeable risk of PoS 91 fraud:

(a) *Foreseeability.* Tesco Bank is a member of both Visa and Mastercard and receives information from both organisations about the operation of their card schemes. On 4 November 2015 Visa issued a fraud alert to its members, including Tesco Bank. It warned Tesco Bank about fraudulent PoS 91 transactions occurring in Brazil and the US, exactly the kind of transactions carried out during the attack. Following the alert, Tesco Bank's Financial Crime Operations Team immediately blocked all PoS 91 transactions for Tesco Bank's credit cards, but they did not make parallel changes to its debit cards. On 5 November 2015 Visa posted a similar alert on its Global Fraud Information Service Portal. Tesco Bank is a subscriber to the service and has access to the portal.

(b) *Preventability.* On 30 September 2016, MasterCard sent an email to all its members, including Tesco Bank, warning them of a PoS 91 attack affecting another UK issuer. The email said, "*Fraudulent PoS 91 (mag-stripe contactless) transactions have been received from merchants in Brazil, often preceded by low value/test transactions on US based (small) merchant web-sites. This is a repeat of attacks previously experienced and the subject of advisory bulletins*". The email advised members to review their fraud and authorisation rules to ensure that members were protected. Members of the Fraud Strategy Team received the email, but could not recall taking any action on the debit cards as a result of it. Moreover, Tesco Bank had experienced fraudulent PoS 91 transactions on both its credit cards and debit cards before the attack.

(4) Respond to the Cyber Attack with sufficient rigour, skill and urgency:

(a) *Failure to follow procedures.* The Financial Crime Operations Team failed to follow appropriate procedures to alert the on-call Fraud Strategy Analyst during the weekend of the attack. The team emailed an in-box instead of telephoning the on-call Fraud Strategy Analyst. In addition, the Customer Operations Incident Management Rota contained an incorrect telephone number which delayed Tesco Bank from reaching the on-call fraud analyst. The consequence of these delays was that the on-call fraud analyst was not alerted until 23:30 on Saturday, 5 November 2016, approximately 21 hours after the attack began and 15 hours after the Financial Crime Operations Team originally emailed the on-call Fraud Analyst. As a consequence, Tesco Bank missed a number of opportunities to identify the severity of the attack at an earlier stage.

(b) *Crisis Management*. Cyber crime is increasing and evolving. Crisis management is a key element in a cyber-incident response framework. Having well documented crisis management procedures is an essential element of a bank's (or any financial institution's) cyber-resilience procedures. It is equally important to ensure that

the individuals responsible for implementing crisis management procedures understand the procedures and have the appropriate training to understand how to use the policies and procedures and that banks rehearse these procedures using a variety of scenarios. While Tesco Bank had documented crisis management procedures, including the criteria for assessing the seriousness and scale of an incident, the training materials explaining the stage at which crisis management should be invoked lacked clarity. The execution of the procedures fell substantially below regulatory requirements. The responsible managers should have recognised the implications of the attack earlier and they should have invoked Tesco Bank's crisis management procedures sooner.

(c) *Coding failures.* Once the Fraud Strategy Team became aware of the high volume of fraudulent PoS 91 transactions, they tried to draft a rule to block them. However, instead of entering the country code for Brazil in the country code field, they entered the currency code for the Euro. This was a mistake and the result was that the rule did not block the fraudulent transactions.

(d) *Failure to monitor.* Having drafted the rule to block the fraudulent transactions at 01:45 on Sunday 6 November 2016, the Fraud Strategy Team failed to monitor the operation of the rule and did not discover it was not working until 07:00. In the meantime, the fraudulent transactions were multiplying reaching a peak of 80,000 by Monday 7 November 2016 with Tesco Bank's systems stopping approximately 90% of them. It took the Fraud Strategy Team over five hours to uncover their mistake and almost four hours to implement the correct rule.

6. SANCTION

Financial penalty

6.1. The Authority has considered the disciplinary and other options available to it and hereby imposes a financial penalty of £16,400,000 on Tesco Bank pursuant to section 206 of the Act.

6.2. The Authority's policy in respect of its decisions whether to impose financial penalties and its calculation of those penalties is set out in Chapter 6 of its Decision Procedure and Penalties manual ("DEPP"). In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

Step 1: disgorgement

6.3. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive the firm of the financial benefit derived directly from the breach, where it is practicable to quantify this.

6.4. The Authority has not identified any financial benefit that Tesco Bank derived from the breach.

6.5. Step 1 is therefore £0.

Step 2: the seriousness of the breach

6.6. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. As made clear in DEPP 6.5A.2G (1), the Authority's starting point is that, in many cases, the amount of revenue generated by the firm in question from the relevant business area or product line during the misconduct period is indicative of the harm or risk of harm arising. DEPP 6.5A.2G (1) also, however, recognises that such revenue may not be an appropriate indicator of that harm or risk of harm. In such a case, the Authority will use an appropriate alternative.

6.7. The Authority considers that the revenue generated by Tesco Bank from its debit cards during the Relevant Period is not an appropriate indicator of the harm or potential harm caused by its breach in this case. This is because the revenue is not related to the amount of funds which were at risk during the attack.

6.8. The Authority considers that the appropriate indicator in this case is the average of the aggregate personal current account balances at risk during the Relevant Period ("ABR"). The Relevant Period began on 1 June 2014 (the date Tesco Bank launched the Debit Card) and ended on 9 November 2016 (the date Tesco Bank resumed normal operations). The Authority has calculated the Step 2 figure in this case in two stages.

(1) Stage A. (1) Identify by reference to the seriousness of the misconduct, any distinct periods of misconduct within the Relevant Period; (2) Weight, having regard to the length of each such period, the seriousness of the misconduct in each period, relative to the other periods; (3) Calculate the resulting weighted ABR for each period; and (4) Add the separate weighted ABRs to calculate the total weighted ABR.

(2) Stage B. Determine the overall misconduct seriousness level and multiply the total weighted ABR by the appropriate resulting misconduct seriousness multiplier.

6.9. The following paragraphs apply the methodology to the facts of this case.

Stage A

6.10. The Authority divided Tesco Bank's misconduct into three periods and weighted the seriousness of the misconduct in each period having regard to the length of each period, as follows:

(1) Period 1 (1 June 2014 – 3 November 2015) covers the design and distribution misconduct of the debit card and the failure to configure specific authentication and fraud detection rules. The ABR during that period was £58.5m. The weighting for that period is 15%. This equals a subtotal weighted ABR for that period of £8.8m

(2) Period 2 (4 November 2015 – 4 November 2016) covers the period when Tesco Bank failed to take appropriate action to prevent the foreseeable risk of PoS 91 fraud and is triggered by the first Visa and MasterCard warnings about fraudulent PoS 91 transactions. The ABR during that period was £191.4m. The weighting for that period is 40%. This equals a subtotal weighted ABR for that period of £76.6m.

(3) Period 3 (5 November 2016 – 9 November 2016) covers the period relating to Tesco Bank's response to the attack itself. The ABR during that period was £307.6m. The weighting for that period is 45%. This equals a subtotal weighted ABR for that period of £138.4m.

6.11. The total weighted ABR exposed to the risk of harm during the Relevant Period was £223.74m.

Stage B

6.12. In deciding the Step 2 figure, the Authority considers the seriousness of the breach and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breach; the more serious the breach, the higher the level. For penalties imposed on firms there are the following five levels, which the Authority considers remain appropriate in this case:

(1) Level 1 – 0%

(2) Level 2 – 5%

(3) Level 3 – 10%

(4) Level 4 – 15%

(5) Level 5 – 20%

6.13. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly. DEPP 6.5A.2G (11) lists factors likely to be considered "level 4 factors or level 5 factors". The following factors are relevant to the Authority's assessment:

(1) The breach caused a significant risk of loss to a large number of individual customers. The attack affected 6% of Tesco Bank's personal current accounts (8,261 out of 131,000) such that, even if the accounts were not actually debited, it appeared to the customers that their account balances had been reduced.

(2) The breach caused inconvenience and distress to a large proportion of Tesco Bank's debit card customers. Personal current account holders received text messages in the early hours of the morning asking them to call Tesco Bank about suspicious activity on their accounts. The text messages were likely to cause distress, some customers were subsequently unable to make payments using their debit cards and 668 unpaid direct debits on customers' accounts were returned unpaid.

(3) The breach revealed serious weaknesses in the operation of Tesco Bank's financial crime controls. The failure to take steps to address these weaknesses left Tesco Bank's personal current account customers vulnerable to fraudulent PoS 91 transactions. Tesco Bank was aware that its debit card systems were vulnerable to PoS 91 transactions but failed to implement specific authentication and fraud detection rules to prevent such transactions. Tesco Bank is in the business of banking and fundamental to that business is protecting its customers from financial crime.

(4) The breach facilitated financial crime: the attackers netted £2.26 million from Tesco Bank's personal customer accounts over a 48-hour period.

6.14. DEPP 6.5A.2G (12) lists factors likely to be considered "level 1, 2 or 3 factors". Of these, the Authority considers the following factors to be relevant:

(1) Tesco Bank made no profits as a result of the breach.

(2) There was no, or limited, actual or potential effect on the orderliness of, or confidence in, markets as a result of the breach.

(3) The breach was committed negligently. There was no lack of integrity or good faith.

6.15. The Authority also considers that the following factors are relevant:

(1) The attack was foreseeable. Tesco Bank received warnings about fraudulent PoS 91 transactions and the fact that cyber criminals were using PoS 91 to engage in fraudulent transactions. PoS 91 transactions accounted for the majority of the fraudulent and attempted fraudulent transactions.

(2) The attack was preventable. Having received warnings, Tesco Bank failed to take any action to configure its debit card systems with specific authentication and fraud detection rules. While Tesco Bank configured its credit card systems to block PoS 91 transactions it failed to make parallel changes to its debit card systems.

(3) Tesco Bank could have brought the attack to a substantially earlier conclusion.

6.16. The Authority has taken these factors into account and considers the overall seriousness of Tesco Bank's breaches to be level 4.

6.17. The total weighted ABR for all three periods of misconduct is £223.74m. Multiplying the total weighted ABR of £223.74m by 15% (Level 4 seriousness), results in a Step 2 figure of **£33,562,404**.

Step 3: mitigating and aggravating factors

6.18. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2 to take into account factors which aggravate or mitigate the breach.

6.19. The Authority considers that there are no factors which aggravate the breach.

6.20. The Authority considers that the following factors mitigate the breach:

(1) Tesco Bank displayed a high level of cooperation during this investigation. It responded promptly and fully to all the Authority's information requirements without creating obstacles to the provision of the information and it brought additional information to the Authority's attention. Tesco Bank's senior management immediately made itself and its third-party experts available to the FCA's investigation team and participated in open meetings in which it answered technical and factual questions.

(2) Tesco Bank immediately took the initiative to commission third party reviews following the attack. It commissioned an external report that confirmed that no personal data was lost or stolen during the attack. It commissioned a root cause analysis of the weaknesses that made Tesco Bank vulnerable to the attack. It commissioned an evaluation of its financial crime controls. It took the initiative to notify the Authority that it was commissioning these reports and promptly provided all the reports to the Authority without claiming privilege over the reports.

(3) Tesco Bank reviewed the third-party reports and raised only one substantive objection to a recommendation in the root cause analysis. It immediately made its management response available to the Authority and senior managers at the highest levels of the bank attended an open meeting with the FCA and the PRA to discuss its response to the root cause analysis and to describe the programme it was instituting to incorporate the experts' recommendations.

(4) Tesco Bank promptly instituted a comprehensive end-to-end review of its financial crime controls and debit card payments systems to identify and ameliorate the deficiencies which made it vulnerable to the attack. It has engaged in an extensive review of those processes and, among other things, it has: changed the way it issues new debit card and generates PANs; enhanced its processes for monitoring and responding to threat intelligence; improved its incident and crisis management capabilities by issuing clearer guidance and training its staff.

(5) Tesco Bank has made significant investments in expanding and training its financial crime and risk teams.

(6) Tesco Bank took the initiative to commence a comprehensive consumer redress exercise.

(7) Tesco Bank stopped approximately 79.79% of the fraudulent transactions.

6.21. Taking all these factors into consideration, the Authority considers that a 30% mitigation credit is appropriate.

6.22. The Step 3 figure is therefore **£23,428,571**.

Step 4: adjustment for deterrence

6.23. Pursuant to DEPP 6.5A.4G if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

6.24. The Authority considers that the Step 3 figure of £23,428,571 represents a sufficient deterrent to Tesco Bank and others, and so has not increased the penalty at Step 4.

6.25. The Step 4 figure is therefore **£23,428,571**.

Step 5: settlement discount

6.26. Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement.

6.27. The Authority and Tesco Bank reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure.

6.28. The Step 5 figure is therefore **£16,400,000**.

Penalty

6.29. The Authority hereby imposes a total financial penalty of **£16,400,000** (**£23,428,571** before Stage 1 discount) on Tesco Bank for breaching Principle 2.

7. PROCEDURAL MATTERS

7.1. This Notice is given to Tesco Bank in accordance with section 390 of the Act.

7.2. The following statutory rights are important.

Decision maker

7.3. The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.

Manner and time for payment

7.4. The financial penalty must be paid in full by Tesco Bank to the Authority no later than 15 October 2018, being 14 days from the date of this Notice.

If the financial penalty is not paid

7.5. If all or any of the financial penalty is outstanding on 15 October 2018, the Authority may recover the outstanding amount as a debt owed by Tesco Bank and due to the Authority.

Publicity

7.6. Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the Authority must publish such information about the matter to which this notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to your or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

7.7. The Authority intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

Authority contacts

7.8. For more information concerning this matter generally, contact Maria Gouvas at the Authority (020 7066 3552).

Bill Sillett

Head of Department

Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A

RELEVANT STATUTORY AND REGULATORY PROVISIONS

1. RELEVANT STATUTORY PROVISIONS

1.1 The Authority has the power to impose an appropriate penalty on an authorised person if the Authority considers that an authorised person has contravened a relevant requirement (section 206 of the Act).

1.2 In discharging its general functions, the Authority must, so far as reasonably possible, act in a way which is compatible with its strategic objective and advances one or more of its operational objectives (section 1B (1) of the Act). The Authority's strategic objective is ensuring that the relevant markets function well (section 1B (2) of the Act). The Authority has three operational objectives (section 1B (3) of the Act).

1.3 Two of the Authority's operational objectives, the consumer protection objective (section 1C of the Act) and the integrity objective (section 1D of the Act), are relevant to this matter.

2. RELEVANT REGULATORY PROVISIONS

2.1 In exercising its powers to impose a financial penalty, the Authority has had regard to the relevant regulatory provisions published in the Authority's Handbook. The Handbook provisions relevant in this matter are the Principles, the Decision, Procedures and Penalties Manual ("DEPP") and the Enforcement Guide ("EG").

2.2 The Principles are a general statement of the fundamental obligations of firms under the regulatory system. They derive their authority from the Authority's rule-making powers set out in the Act. The relevant Principle in this matter is Principle 2:

"*A firm must conduct its business with due skill, care and diligence*".

2.3 DEPP sets out the Authority's policy for imposing a financial penalty. For conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies to financial penalties imposed on firms. The conduct that is the subject matter of this action took place after 6 March 2010.

2.4 EG sets out the Authority's approach to taking disciplinary action. The Authority's approach to financial penalties is set out in Chapter 7 of the Enforcement Guide.