Financial Conduct Authority

FINAL NOTICE

To: **Royal Bank of Scotland Plc**
National Westminster Bank Plc
Ulster Bank Ltd

Reference numbers: **121882, 121878 and 122315**

Addresses: 36 St Andrew Square, Edinburgh, Midlothian EH2 2YB
135 Bishopsgate, London EC2M 3UR
11-16 Donegal Square East, Belfast BT1 5U

Date: 19 November 2014

1. ACTION

1.1. For the reasons given in this notice, the Authority hereby imposes on the Royal Bank of Scotland Plc, National Westminster Bank Plc and Ulster Bank Ltd (insofar as it applies to its operations in Northern Ireland) (together the "Banks"), a financial penalty of £42,000,000 for breaches of Principle 3 between 1 August 2010 and 10 July 2012 ("Relevant Period").

1.2. The Banks 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 £60,000,000 on the Banks.

2. SUMMARY OF REASONS

The IT Incident's effect on the Banks' customers and non-customers

2.1. On Wednesday 20 June 2012 customers of the Banks found that they could not use all of the Banks' online banking facilities to access their accounts or obtain accurate account balances from ATM machines. The events which would develop throughout the day are referred to in this notice as the "IT Incident".

2.2. Customers learned that the problems were not isolated to these facilities, but they discovered that they were unable to drawdown loans, transfer payments to external creditors including credit card companies and mortgage providers or transfer monies using SWIFT payment methods.

2.3. Customers would later find that the Banks had applied incorrect credit and debit interest to their accounts, duplicated entries on their statements and failed to accurately record transactions on their accounts. Customers also learned that the Banks had not processed their standing orders on time.

2.4. The problems affected not only the Banks' customers in the UK. They also affected customers who were abroad. The Banks declined their credit card purchases leaving customers unable to pay bills and make purchases. Some customers found themselves without access to cash in foreign countries.

2.5. The IT Incident also affected individuals who were not customers of the Banks. They were unable to receive monies from the Banks' customers and this prevented them from honouring their own financial commitments.

2.6. The effect on commercial customers included the inability to use Bankline, an internet banking service. This meant that commercial customers were unable to manage payments, verify cheques or make international cash transfers. Other commercial customers were unable to finalise their audited accounts and meet payroll commitments.

2.7. At a broader level, this affected the Banks' ability to fully participate in clearing. Clearing is a system established to settle payments among banks and is the process by which banks ensure that a payee receives the full value of a cheque or standing order. An efficient clearing system is fundamental to the efficient operation of the financial markets.

2.8. The IT Incident affected at least 6.5 million customers in the UK (92% of whom were UK retail customers). This was 10% of the population. Disruptions to the majority of RBS's and NatWest's systems lasted until 26 June 2012, and the disruptions to the majority of Ulster Bank's systems continued until 10 July 2012. Disruptions to other systems, including BankTrade (a system for processing and documenting international bond trades) and IFS (an international currency system), affected all the Banks and those disruptions lasted until July 2012.

The causes of the IT Incident

2.9. The actual cause of the IT Incident was a software compatibility issue between the upgraded software and the previous version of the software. The compatibility issue occurred when Technology Services (the centralised Group IT function which provides IT services to the Banks) backed out a software upgrade that they had installed on Sunday, 17 June 2012. To "back out" a software upgrade means to uninstall the current version of the software and go back to a previous version of software.

2.10. The underlying cause of the IT Incident was the failure of the Banks to meet their obligations to have adequate systems and controls to identify and manage their exposure to IT risks. The Banks' IT risk arrangements were provided at Group level through a number of support and control functions. At the Group level there were failings in Technology Services, in the Three Lines of Defence and in the Group's approach to IT operational risk.

Principle breaches

2.11. Principle 3 requires a firm to take reasonable care to organise and control its affairs responsibly and effectively with adequate risk management systems. On the basis of the facts and matters described in more detail below, the Banks breached Principle 3 because they failed to have adequate systems and controls in place to identify and manage their exposure to IT risks. In particular:

(1) Technology Services did not take reasonable steps to ensure that changes to the Banks' IT systems were carried out in a carefully planned and consistent manner. It did not manage and plan those changes adequately because it did not devise and implement adequate:

(a) processes for identifying, analysing and resolving IT incidents; and

(b) policies for testing software.

(2) The Three Lines of Defence did not carry out their responsibilities adequately:

(a) Technology Services Risk, (the risk function within Technology Services), the First Line of Defence, was responsible for identifying and managing IT risks. It did not carry out its duties adequately because it had a culture of reacting to events and a team with insufficient experience and skills.

(b) Business Services Risk, the Second Line of Defence, was responsible for reviewing Technology Service's view of risks and identifying gaps in the Group's view of risk. It did not carry out these duties adequately because it had limited IT skills and it did not sufficiently challenge Technology Services Risk's view of IT risk.

(c) Group Internal Audit, the Third Line of Defence, was responsible for providing independent assurance on the design and operation of risk management and internal control processes. There were weaknesses in the communications between Group Internal Audit and the First and Second Line of Defence.

2.12. The Banks failed to adequately inform themselves about the nature and effect of IT operational risk. The operational risk appetite relevant to IT was the "Business Continuity & IT Continuity" risk appetite ("IT Continuity Risk Appetite"). This was too limited because, in addition to Business Continuity (recovering from an incident), it should have included a much greater focus on IT Resilience (designing IT systems to withstand or minimise the risks of disruptive events). This appetite directly informed the Group's IT Continuity Policy Standard which had the same limitations.

2.13. The Banks' breaches took place between 1 August 2010 (the date of a Group Internal Audit on mainframe batch processes, which identified the risk of a batch

scheduler failure) and 10 July 2012 (the date most of the Banks' IT systems were functional after the IT Incident).

2.14. As a result, the Authority proposes to impose a financial penalty on the Banks in the amount of £42,000,000 (after the Stage 1 discount) pursuant to section 206 of FSMA.

The redress programme

2.15. Following the IT Incident the Banks initiated a customer redress programme. They compensated both the Banks' own customers and customers of other banks who were affected by the IT Incident. They paid redress to customers, including customers who did not file complaints. Customers (including those of Ulster Bank ROI) filed almost 70,000 complaints and non-customers filed 1,200 complaints.

2.16. The Banks paid approximately £70.3 million in redress to UK customers. In addition, they paid redress of £460,000 to individuals and firms who were not their customers.

Conclusion

2.17. A retail bank's core business function is the provision of financial services. This includes making deposit accounts and loans available to its customers, updating customer balances, giving customers access to their accounts through online banking and ATM machines, processing customers' and third parties' payments.

2.18. The IT Incident affected these core banking functions and, in doing so, it affected two of the Authority's operational objectives.

(1) It affected the FCA's consumer protection objective (securing an appropriate degree of protection for customers) because the IT Incident prevented the Banks' customers from engaging in basic banking functions. Moreover, the IT Incident affected at least 6.5 million customers in the UK. Of those 6.5 million customers, 92% were customers of the Banks in the RBS Group's UK retail division.

(2) It affected the FCA's integrity objective (protecting and enhancing the integrity of the UK financial system) because the Banks, all settlement banks, risked not being able to carry out their core functions and this could have affected financial stability because:

(a) the high tiering of UK payment systems means that an operational failure in one settlement bank can lead to intraday credit and liquidity exposures between settlement banks and the indirect participants that use their services and this can lead to contagion and disruption in the financial system; and

(b) depositors' inability to access their funds prevents them from undertaking economic activity.

3. DEFINITIONS

3.1. The definitions below are used in this Final Notice.

(1) "Authority" means the body corporate previously known as the Financial Services Authority and renamed on 1 April 2013 as the Financial Conduct Authority.

(2) "ATM" means automated teller machine.

(3) "Banks" means the Royal Bank of Scotland Plc, National Westminster Bank Plc and Ulster Bank Ltd (insofar as it applies to its operations in Northern Ireland).

(4) "BankTrade" is a system the RBS Group uses to process the Banks' international documentary trade and domestic (UK) bonds and guarantees business.

(5) "Business Continuity" means the capability of an organisation to continue to deliver products or services at acceptable predefined levels following a disruptive incident.

(6) "Business Services" means the Business Services Division of the RBS Group. It consists of a series of central functions that support the RBS Group's customer facing businesses including Technology Services.

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

(8) "Group" or "RBS Group" means the Royal Bank of Scotland Group Plc and its subsidiaries (including the Banks). The territories this notice refers to are limited to England, Wales, Scotland and Northern Ireland.

(9) "Group Board" means the Royal Bank of Scotland Group Plc Board.

(10) "Group Policy Framework" means the mechanism the Group uses to make its centralised Group policies available to those responsible for managing risk throughout the Group.

(11) "Group Strategic Risk Objectives" are set by the RBS Group Board and are: maintaining stakeholder confidence; maintaining capital adequacy; delivering stable earnings growth; and delivering stable/efficient access to funding and liquidity.

(12) "IFS" means International (Foreign) System, the international payments system the RBS Group used primarily to maintain the details of and process the accounting for the currency accounts held by customers.

(13) "IT Continuity Policy Standard" means "Maintaining Key Services and Processes, IT Continuity", the primary document within the Group Policy Framework that identified the Group policy on IT Resilience and contingency.

(14) "IT Governance" means the actions the relevant bodies within a firm take to fulfil their roles to design and implement appropriate IT policies and strong operational IT risk management to ensure that the firm is not vulnerable to reasonably foreseeable IT risks.

(15) "IT Incident" means the RBS Group's IT failure which affected the Banks' customers from 19 June to July 2012.

(16) "IT Resilience" means the ability of an organisation's IT services and systems to withstand disruptive events or failure whether the cause is attributable to a failure of hardware or software systems, processes, or personnel or a combination of any of these.

(17) "NatWest" means the National Westminster Bank Plc, a subsidiary of RBS.

(18) "Principles" means the Principles for Businesses set out in the Authority's Handbook as were in force during the Relevant Period.

(19) "Relationship Management Platform" means, a credit management system which enables relationship managers to process customers' credit applications for approval.

(20) "RBS" means the Royal Bank of Scotland Plc, a subsidiary of the RBS Group.

(21) "RBS International" means RBS International Limited.

(22) "RBS Risk Management" is the Group's independent risk management function. It is responsible for managing risks on a Group-wide and divisional basis.

(23) "Skilled Person" means the person RBS appointed pursuant to section 166 of FSMA to prepare the independent report concerning the IT Incident and its causes.

(24) "Strategic IT Risk Appetite" means the level of risk the RBS Group is willing to accept if an IT risk materialises that could threaten the Group's Strategic Risk Objectives.

(25) "Technology Services" means the centralised Group IT function which provides IT services to the Banks.

(26) "Three Lines of Defence" means the three lines of defence for IT at the RBS Group which are:

(a) Technology Services Risk (the First Line of Defence for IT);

(b) Business Services Risk (the Second Line of Defence for IT); and

(c) Group Internal Audit (the Third Line of Defence).

(27) "Ulster Bank" means Ulster Bank NI and Ulster Bank ROI.

(28) "Ulster Bank NI" means Ulster Bank Limited, a subsidiary of NatWest, regulated by the Financial Conduct Authority and the Prudential Regulation Authority and registered in Northern Ireland.

(29) "Ulster Bank ROI" means Ulster Bank Ireland Limited, a subsidiary of Ulster Bank NI, regulated by the Central Bank of Ireland and registered in the Republic of Ireland.

4. FACTS AND MATTERS

4.1. This section describes:

(1) the Banks and the RBS Group;

(2) the root cause of the IT Incident;

(3) the IT risk management framework and, in particular:

(a) Technology Services;

(b) the Three Lines of Defence; and

(c) the RBS Group's governance of strategic IT risk.

The RBS Group and the Banks

4.2. The RBS Group is one of the UK's major banking groups and is also an international banking and financial services company. Its headquarters are in Edinburgh and it operates in the Middle East, the Americas and Asia. It serves over 30 million customers worldwide.

4.3. RBS and NatWest are subsidiaries within the RBS Group and have over 26 million UK customers, 4,000 ATMs and 2,120 bank branches. Ulster Bank NI, another subsidiary, has approximately 700,000 customers, 450 ATMs and 90 bank branches in Northern Ireland.

4.4. The IT risk arrangements put in place by the Banks are at Group level. The RBS Group manages risk, including IT risk, through a number of governing entities, support and control functions, frameworks and policies. The Business Services Division provides services and support to the RBS Group and it includes Technology Services, which provides the Group's centralised IT function. It is responsible for designing, building, implementing and supporting global technology services for the RBS Group.

The root cause of the IT Incident

The batch scheduler failure

4.5. Banks generally update that day's transactions in the evening. They use a software tool known as a batch scheduler to process those updates. A batch scheduler coordinates the order in which data underlying the updates is processed. The data includes information about customer withdrawals and deposits, interbank clearing, money market transactions, payroll processing, and requests to change standing orders and addresses. The processes underlying the updates are called "jobs". Batch schedulers place the jobs into queues and ensure that each job is processed in the correct sequence. That day's batch processing is complete when all balances are final.

4.6. On Sunday 17 June 2012 a team from Technology Services upgraded the batch scheduler software that processed updates to customers' accounts at NatWest and Ulster Bank because this software could no longer be sufficiently supported. They upgraded the batch scheduler software from Version 1 to Version 2A. Version 2A contained a modification known as a "patch". (A separate batch scheduler processed updates to RBS's accounts.)

4.7. On the evening of Monday 18 June 2012, the Technology Services team executed the first full batch run (set of updates) for the NatWest and Ulster Bank batch scheduler since the software update. During the evening the team noticed a number of anomalies. The mainframe computer was using a higher than normal percentage of its total processing capacity. This, in turn, caused the system to slow down and to experience several batch terminal failures. This meant that it did not properly update customers' accounts. The team raised the failures with internal IT experts who were able to re-run the failed batches by entering commands into the system manually. This allowed the complete batch to run

that night. The RBS batch scheduler was also affected because of interdependencies with the NatWest and Ulster Bank batch scheduler.

4.8. On Tuesday 19 June 2012, Technology Services backed out the software upgrade. The Technology Services' team was not aware, however, that Version 2A, the upgraded version of the software, was not compatible with Version 1, the version that had been in place prior to the upgrade. The reason it was not compatible was because Version 2A, the upgraded version of the software, contained the "A" patch modification. Technology Services had only tested the consequences of backing out Version 2 to Version 1. They had not tested the consequences of backing out Version 2A to Version 1. This was the underlying cause of the IT Incident.

4.9. As a result of backing out the software upgrade, a significant number of jobs failed to appear in the batch queues and the unprocessed batch jobs began to multiply. The lack of compatibility between Version 2A and Version 1 of the software, which was unknown to Technology Services, and the subsequent release of incomplete batches in Ulster Bank's and NatWest's systems, was the actual cause of the IT Incident.

4.10. To resolve the problem, technical support staff focused on manually re-loading jobs into the batch queues. This process of manual intervention is implemented when a number of batch jobs fail to run. By the morning of 20 June 2012, the NatWest batch for 19 June was largely completed. However, the team had not completed processing Ulster Bank batches by then and that caused a significant backlog at the start of the following working day.

4.11. By 21 June 2012, batch processing for Ulster Bank was more than one day behind. This meant that the next day's batch processing started before the current day's batch processing was complete. The simultaneous processing of Ulster Bank's batches interfered with each other because there were multiple days' files in the processing system and multiple days' jobs in the queues. This caused additional recovery problems and further backlogs.

The effects of the batch scheduler failure

4.12. The IT Incident affected all of the Banks. The effects of the IT Incident on RBS were not as severe as the effects on NatWest and Ulster Bank because a separate batch scheduler controlled the updates to RBS's customers' accounts. However, RBS was affected because some of the information it required to update its accounts was dependent upon receiving accurate and timely information from NatWest and Ulster Bank. That information included management information, finance and risk information as well as payments that customers from those banks were making to each other and to RBS customers as well.

4.13. By the beginning of 25 June 2012, Technology Services had managed to stabilise RBS's and NatWest's batch processes, although both banks' records required some manual updating throughout the week. From 25 June 2012, the focus of effort was on the recovery of Ulster Bank's batches. The Ulster Bank batch scheduler did not return to full functionality until 10 July 2012.

4.14. The IT Incident potentially affected 635 systems at the RBS Group, of those systems 75 were payment related systems, which included the following functions (some systems had more than one function):

(1) The administration or updating of customer accounts (17 systems).

(2) The processing and execution of payments (68 systems).

(3) The application of interest and charges (11 systems).

(4) The reconciliation of accounting entries across the Banks (3 systems).

4.15. The effects of the IT Incident were wide-ranging and affected a number of the Banks' systems and customers. The following are some examples of the ways the IT Incident affected the Banks' systems and customers.

(1) ATMs were generally available, but they presented out of date balances because of missing or duplicate transactions. This meant that some customers were unable to withdraw cash. In addition, some customers ran the risk of overdrawing their accounts when they withdrew cash, particularly if their accounts were close to their limits and credits had not been applied. The IT Incident affected ATMs until:

(a) RBS: 27 June 2012 (system was not fully functional for 8 days);

(b) NatWest: 28 June 2012 (system was not fully functional for 9 days);

(c) Ulster Bank NI: 8 July 2012 (system was not fully functional for 19 days).

(2) Digital Banking is an internet based online banking service for personal and small business customers of RBS, including RBS International customers. The system remained technically available, but there were intermittent periods of outage for logins. Customers were affected if they were unable to login and make online banking transactions, make payments and view correct balances and transaction histories. The IT Incident affected Digital Banking until:

(a) RBS: 25 June 2012 (system was not fully functional for 6 days);

(b) NatWest: 1 July 2012 (system was not fully functional for 12 days);

(c) Ulster Bank NI: 9 July 2012 (system was not fully functional for 20 days).

(3) Direct Banking/Telephony is the Banks' telephone banking service. The system remained available but with intermittent periods of outage. Customers who tried to log-in during the periods of outage were unable to make online banking transactions, make payments and view correct balances and transaction histories. The IT Incident affected Direct Banking/Telephony until:

(a) RBS: 25 June 2012 (system was not fully functional for 6 days);

(b) NatWest: 1 July 2012 (system was not fully functional for 12 days);

(c) Ulster Bank NI: 8 July 2012 (system was not fully functional for 19 days).

(4) Teller service was available at branches, however, the IT Incident meant that transactions from those branches were not updated in the central computer system and that caused the Banks' overnight ledger balance to

be inaccurate for affected customers. Those customers were unable to make or receive payments and could not be provided with their correct balances or transaction histories. The IT Incident affected teller services until:

(a) RBS: Unaffected;

(b) NatWest: 28 June 2012 (system was not fully functional for 9 days);

(c) Ulster Bank NI: 9 July 2012 (system was not fully functional for 20 days).

(5) Bankline Direct is a payments channel which provides customers with a method of making payments. Customers were not able to see up to date account information (balance and transactions). Customers could make payments, although this would be dependent on the account being up to date in some circumstances. The IT Incident affected Bankline Direct until:

(a) RBS: 27 June 2012 (system was not fully functional for 8 days);

(b) NatWest: 28 June 2012 (system was not fully functional for 9 days);

(c) Ulster Bank NI: Unaffected.

(6) Point of Sale is the system which provides a gateway between Visa and its users. It authorises debit card transactions, both domestic and international. The system remained available, however, authorisations were checked against incorrect balances. Customers may have lost the ability to pay for transactions, especially if credit was not applied to accounts leading to lack of available funds. The Banks partially mitigated the problem by arranging a £200 "stand-in" limit for debit cards which gave customers the ability to buy goods up to that limit. The IT Incident affected the Point of Sale systems until:

(a) RBS: 27 June 2012 (system was not fully functional for 8 days);

(b) NatWest: 28 June 2012 (system was not fully functional for 9 days);

(c) Ulster Bank NI: 8 July 2012 (system was not fully functional for 19 days).

(7) The Relationship Management Platform is an IT system RBS International used. The IT Incident affected corporate customers' transactions and account records which in turn affected corporate customers' ability to make payments to corporate accounts, draw invoices and make salary runs. The IT Incident affected the Relationship Management Platform until:

(a) RBS: 6 July 2012 (system was not fully functional for 17 days);

(b) NatWest: 6 July 2012 (system was not fully functional for 17 days);

(c) Ulster Bank NI: 6 July 2012 (system was not fully functional for 17 days).

(8) BankTrade GTS is a system the RBS Group used to process the bank's international trades and UK bonds. Although the system was processing trades, the backlog delayed the processing of the current day's trades. Commercial customers' international transactions were potentially delayed exposing them to risk of non or late payment. The IT Incident affected the BankTrade GTS system until:

(a) RBS: 18 July 2012 (system was not fully functional for 29 days);

(b) NatWest: 18 July 2012 (system was not fully functional for 29 days);

(c) Ulster Bank NI: 18 July 2012 (system was not fully functional for 29 days).

4.16. Following the IT Incident, the Authority required the Banks to appoint a Skilled Person to independently assess the immediate causes, consequences and management of the IT Incident.

The IT risk management framework

4.17. IT systems are the foundation of modern banking operations and a bank's ability to do business and serve its customers. For this reason, it is crucial to have a well-developed operational risk management framework with appropriate IT policies, objectives and risk appetites. If the framework is clear and well-designed, those who are responsible for planning, testing and implementing changes to the bank's IT systems can take these actions in a manner that minimises the risk of failure. As discussed in more detail below, the RBS Group put in place a flawed policy standard. The policy standard was limited in scope because its focus was on Business Continuity (reacting to or recovering from IT failures) and should have included a much greater focus on IT Resilience (designing IT systems to withstand or minimise the risk of disruptive events). The IT functions within the RBS Group were required to follow the strategy set by the policy standard.

4.18. The RBS Group manages risk through a number of governing entities, support and control functions, frameworks and policies.

4.19. Broadly, those entities and control functions and their responsibilities are:

(1) Technology Services which provides IT services to the Banks.

(2) Three Lines of Defence:

(a) The First Line of Defence (including Technology Services Risk within Technology Services) which is responsible for identifying and managing IT risk across the Banks.

(b) The Second Line of Defence (Business Services Risk) which is responsible for challenging the First Line of Defence.

(c) The Third Line of Defence (Group Internal Audit) which independently assesses and reviews IT risks including IT infrastructure and systems risks.

(3) The Group Board approves the overall Group Risk Appetite Framework.

Technology Services

4.20. This section explains:

(1) Technology Services' role;

(2) Technology Services' deficiencies which contributed to the IT Incident; and

(3) Technology Services' management of the IT Incident.

Technology Services' role

4.21. Technology Services is part of the RBS Group's Business Services Division and is responsible for providing IT services for the Banks.

4.22. These responsibilities include implementing Group IT policies in the Banks, ensuring that they are consistent throughout the Group and, on a practical level, updating the software that runs the Banks' IT systems and upgrading the hardware. These changes require careful planning and testing to ensure minimal disruption to the Banks' operations and their customers.

4.23. Technology Services did not carry out these responsibilities adequately. Examples of its general deficiencies are:

(1) Technology Services did not check that the IT policies and procedures it was implementing were consistent with each other.

(2) Technology Services' processes for making IT changes were not adequate because they did not ensure that IT changes could be made in a controlled way. Moreover, the information in the records Technology Services kept did not always show the changes Technology Services was making and it was not always complete and accurate.

(3) Technology Services did not have a complete view of IT risk, particularly in relation to IT operations. For example, it selected areas to review based upon the Group Policy Framework instead of considering all IT risks across the RBS Group. This means that its view of risks was limited and that its planned reviews were not extensive enough in certain areas. For example, it did not include IT operations (including mainframe batch processing) or IT incident and problem management in its planned reviews.

Technology Services' deficiencies which contributed to the IT Incident

4.24. The particular deficiencies of Technology Services which had a direct role in the events which led to the IT Incident were:

(1) Batch scheduling software is fundamental to the Banks' core banking function. As discussed above, the batch scheduler processes updates to customers' accounts, but despite the importance of the batch scheduler to the Banks, Technology Services did not sufficiently identify, understand or mitigate the risk of a batch scheduler failure.

(2) Technology Services could have reduced or limited the effect of the batch scheduler failure if had it taken some or all of the following actions:

(a) reduced the number of jobs each batch scheduler managed;

(b) ensured that interdependencies between the RBS batch scheduler and the Nat West and Ulster Bank batch scheduler were reduced;

(c) used separate batch schedulers for NatWest and Ulster Bank. Instead, it used the same batch scheduler for both NatWest and Ulster Bank. This concentrated the risk of harm to both NatWest and Ulster Bank because any batch scheduler software problem would affect both banks.

(3) Technology Services failed to adequately test the consequences of backing out the batch scheduler software. It made at least two testing errors:

(a) First, Technology Services had only tested backing out the unmodified version of the upgrade (Version 2). In those tests, Version 2 was compatible with the previous version of the software (Version 1). Technology Services had not tested backing out the modified upgraded version of the software (Version 2A) to the previous version (Version 1).

(b) Second, its back-out tests did not use representative data in the queues. It should have conducted these tests using a volume of data representative of the business-as-usual batch volumes and data types.

Technology Services' management of the IT Incident

4.25. Although Technology Services bears considerable responsibility for the risk and control failures that led to the IT Incident, its response to the IT Incident was satisfactory. It mobilised additional staff and resources to manage the technical problems and used innovative approaches to accelerate the processing of batch jobs.

The Three Lines of Defence

4.26. This section explains the RBS Group's approach to using the Three Lines of Defence and the deficiencies in each which contributed to the IT Incident. It examines these issues in more detail below:

(1) the approach to using the Three Lines of Defence;

(2) the First Line of Defence (Technology Services);

(3) the Second Line of Defence (Business Services Risk); and

(4) the Third Line of Defence (Group Internal Audit).

The RBS Group's approach to using the Three Lines of Defence and its deficiencies

4.27. The RBS Group's overall approach to identifying and managing operational risk and the role of each of the Three Lines of Defence was clear. However, the way in which the Three Lines of Defence applied to IT was not clear. For example:

(1) The Three Lines of Defence were not able to explain clearly how Three Lines of Defence and risk forums fitted together as part of the RBS Group's overall IT governance model.

(2) The Three Lines of Defence were not working together to identify, review, manage and challenge IT risks.

(3) The level of interaction and challenge between the Three Lines of Defence was insufficient.

The First Line of Defence

The First Line of Defence's role

4.28. Within the First Line of Defence, Technology Services Risk was responsible for identifying and managing IT risk across the Banks. It worked with the business units themselves to identify IT risks. The business units were responsible for managing the risks in their area within a defined risk appetite.

Deficiencies in the First Line of Defence which contributed to the IT Incident

4.29. Technology Services Risk was ineffective in so far as it concentrated on developing processes to report risk information upward for Group sign-off rather than considering, understanding and managing the overall range of risks relevant to Technology Services.

4.30. Technology Services Risk's culture was ineffective in so far as it was based on a past history of reacting and responding to incidents, rather than forward looking identification of risk.

4.31. Technology Services Risk had insufficient risk experience and skills. For example:

(1) The Technology Services Risk team did not have substantial experience at the RBS Group. Over half of the team had been appointed within the two years preceding the IT Incident; and

(2) No one on Technology Services Risk's senior management team had a risk or an IT audit qualification.

The Second Line of Defence

The Second Line of Defence's role

4.32. The Second Line of Defence (Business Services Risk) was responsible for challenging the First Line of Defence.

Deficiencies in the Second Line of Defence which contributed to the IT Incident

4.33. At the time of the IT Incident, Business Services Risk had very limited IT skills, it did not challenge Technology Services Risk's failure to carry out a risk assessment in relation to the software upgrade nor did it challenge Technology Service's view of IT risk or identify the gaps in the Group's view. Its emphasis was on systems and processes rather than understanding risk.

4.34. Prior to the IT Incident, Business Services Risk had identified its concerns about the level of skills and resourcing with its team and had planned to review these.

4.35. However, at the time of the IT Incident, the IT risk team within Business Services was understaffed and its level of skill and resource was insufficient.

The Third Line of Defence

The Third Line of Defence's role

4.36. The Third Line of Defence (Group Internal Audit) provided independent assurance on the appropriateness of the design and operational effectiveness of risk management and internal control processes.

Deficiencies in the Third Line of Defence which contributed to the IT Incident

4.37. The Group Internal Audit IT team had a good range of skills and experience, but it was understaffed.

4.38. While the Third Line of Defence had a more complete view of IT risks than the First or Second Lines of Defence, it did not explain its differences with them effectively. As a result, TS Risk did not understand these differences and did not act on them.

4.39. Group Internal Audit had identified concerns regarding the level of skills and resourcing within the IT internal audit team and had planned to review these prior to the IT Incident. In comparison with its peers at similar institutions, it was understrength by 20-40%.

4.40. In 2011, the year before the IT Incident, Group Internal Audit did not complete its IT Internal Audit plan, carrying forward 30% of actions.

4.41. Group Internal Audit finalised an audit of the mainframe batch processes in August 2010. This included the back out procedures for changes to the relevant batch scheduler software. Group Internal Audit's terms of reference and its scoping documents for that project correctly identified the potential for a batch processing failure.

4.42. Group Internal Audit's report was deficient because the testing documented in its working papers noted it was not possible to fully test the implementation of relevant controls because there was a lack of documented evidence recording the steps taken in previous back outs and changes. Group Internal Audit took the view that as evidence of control points were present in the change management system, the lack of underlying documentation did not itself present a sufficiently material risk to merit inclusion in the final report and that there were risk mitigants in place. No issue was raised in its final audit report about the fact that testing was not based on a complete audit trail. It is unclear whether Group Internal Audit made Technology Services, the party responsible for updating the batch scheduler software, aware that the relevant controls could not be tested.

The RBS Group's governance of strategic IT risks

4.43. This section describes:

(1) the RBS Group Board's role;

(2) the Risk Appetite Framework ("RAF") and operational risk;

(3) the IT Continuity Policy Standard and explains why it was flawed; and

(4) the FCA's conclusion.

The RBS Group Board's role

4.44. The RBS Group Board is the Group's main decision making forum, ultimately responsible for the decisions taken by the Group. The Group Board sets the Group Risk Appetite Framework and is accountable for the Group's Strategic Risk Appetite. The Group Board's responsibilities include:

(1) determining and reviewing the Group's strategic direction including, as appropriate, the strategies for each of the principal business units;

(2) reviewing, approving and monitoring the Group's risk appetite and strategic risk policies;

(3) considering and approving the Group's procedures for reviewing and monitoring risk; and

(4) receiving and considering high level reports on matters material to the Group, among other things, information systems and technology and disaster recovery.

4.45. In discharging its responsibilities the Group Board operates through a number of committees, divisions and support functions, including its Risk Management Function, and has oversight responsibility for the RBS Group putting in place adequate IT systems and controls.

4.46. In discharging its responsibilities for risk the Group Board:

(1) agrees a Risk Appetite Framework; and

(2) delegates responsibilities to committees and executive management.

The Risk Appetite Framework and operational risk

4.47. The Risk Appetite Framework explains how the RBS Group determines its strategic risk appetite and the responsibilities of the relevant bodies in the framework to identify:

(1) the Group's Strategic Risk Objectives;

(2) the way to measure the risk the Group is willing to take to achieve those objectives; and

(3) the risk appetite, the level of risk the Group is willing to take to achieve those Group Strategic Risk Objectives.

4.48. The Group's strategic risk framework focuses on four Group Strategic Risk Objectives set by the Board which are to maintain capital adequacy, deliver stable earnings growth, stable/efficient access to funding and liquidity, and maintain market confidence. The RAF shows that operational risk underlies all of the Group Strategic Risk Objectives except one, stable/efficient access to funding and liquidity.

4.49. The Group Board approved the RAF and in doing so approved the operational risk appetite metrics pursuant to which the operational risk appetite was set.

4.50. The Group Board did not review or approve the operational risk appetite. The Executive Risk Forum ("ERF"), a committee of ExCo, approved the operational risk appetite. The IT Continuity Risk Appetite, set in accordance with the operational risk appetite, should have had a much greater focus on IT Resilience. This, in turn, informed the IT Continuity Policy Standard which had the same limitations.

The IT Continuity Policy Standard

4.51. The Group's IT Continuity Policy Standard is the primary document that sets out the Group's approach to managing IT resilience and continuity risk. The IT Continuity Policy Standard was drafted and approved by a member of ExCo in accordance with the RAF. In June 2011 the Group commissioned a third party expert to carry out a review of a previous version of the IT Continuity Policy Standard. The third party expert found that the policy's control requirements were at an adequate overall level and were comparable with similar policies among the RBS Group's peers.

4.52. The Group's IT Continuity Policy Standard was not adequate because, although it was consistent with the operational risk appetite, it was limited in scope because it addressed recovering from a single low probability but high impact event of the total loss of a data centre. The policy should have included a much greater focus on IT Resilience, that is designing IT systems to withstand or minimise the risk of disruptive events (such as software failures) that are more probable and that can potentially have an equivalent effect.

4.53. The RBS Group published its IT Continuity Policy Standard in its Group Policy Framework, the mechanism the Group uses to make its centralised Group policy standards available throughout the Group. Those individuals who were responsible for designing IT architecture and testing, and systems and controls at the RBS Group did so in accordance with an IT Continuity Policy Standard which took into account a too limited range of risks.

4.54. IT underpins three of four of the RBS Group's Strategic Risk Objectives and is therefore of strategic importance. The RBS Group did not sufficiently recognise and address its strategic IT risks, in particular in the IT Continuity Policy Standard. The RBS Group had IT experts throughout Technology Services, but Technology Services did not have a sufficient business profile or direct involvement in business prioritisation and decision making. While senior representatives of Technology Services attended divisional committee meetings, they were not represented at divisional board level or at the senior spending review committees. Had the RBS Group given its senior technology representatives more appropriate roles at these levels, the Group might have had a more complete and accurate appreciation of the IT risks the Banks faced.

4.55. In 2010 the RBS Group Board identified a need to improve the strength and depth of Group Internal Audit's IT experience. However a permanent Head of Audit for Technology Change and Corporate Services was only appointed by the Group in September 2013, more than a year after the IT Incident.

Conclusion

4.56. The IT Incident was not the result of insufficient investment in IT generally or in its IT infrastructure. Indeed, the RBS Group spends over £1 billion annually to maintain its existing IT infrastructure, its mainframe technology is under five years old and it uses up-to-date software.

4.57. Rather, the underlying cause of the IT Incident was weakness in the Group's IT risk management and in its IT controls, controls which failed to formally identify and actively manage IT risks and to implement prudent testing controls. Central to these deficiencies was the IT Continuity Policy Standard which complied with a narrowly focussed operational risk appetite. Both the policy and the risk appetite focussed on Business Continuity and on low probability and high impact events instead of more probable events (like software failures) that could have an equally disruptive effect.

4.58. Shortly after the IT Incident, the Group Board recognised the limitations of the approach in a Group Board meeting in July 2012. In that meeting the Group Board stated that the Group had not taken the care and attention it needed to address its IT operational risks. These observations are set out in the Group Board minutes:

(1) "with hindsight, batch processing was taken for granted and attention was focussed on technology that had failed or future developments".

(2) "Rather than focussing on backward looking events, consideration should be given to broader risk issues and potential 'black swan' events".

4.59. Early in 2013, senior RBS Group executives reviewed an internal paper which criticised the Group's approach to IT and its IT continuity policy. The paper made the following observations:

(1) "Technology resilience remains a key concern" and "Current Business Continuity and IT Continuity policies focus on recovering divisions and data centres within each country from physically disruptive events (e.g. fires, floods and power outages)".

(2) "Whilst this approach is aligned with the RBS Group's industry peers, it is reactive and not customer-centric".

(3) the Group needs to make the "cultural shift" away from Business Continuity ("recovering" from "disruptive events") towards "resilience" which "demands" that "we pre-occupy ourselves with ensuring the activities most critical to our customers are well protected to withstand the impact of disruptive events when they do occur".

5. FAILINGS

Principle 3

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

5.2. Principle 3 states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

5.3. There were failings in Technology Services, the Three Lines of Defence and in oversight of IT Risk within the Group.

5.4. The Banks breached Principle 3 because they failed to have adequate systems and controls to identify and manage their exposure to IT risks. In particular:

(1) Technology Services did not manage and plan changes to the RBS Group IT systems adequately. In particular, it did not:

(a) check that the IT policies and procedures it was implementing were consistent with each other;

(b) ensure that IT changes could be made in a controlled way;

(c) keep accurate and complete records which documented the changes it was making;

(d) have a complete view of IT risk, particularly in relation to IT operations;

(e) sufficiently identify, understand or mitigate the risk of a batch scheduler failure; and

(f) consider reducing or limiting the effect of the batch schedule failure by, for example:

(i) reducing the number of jobs each batch scheduler managed;

(ii) reducing interdependencies between the RBS batch scheduler and the Nat West and Ulster Bank batch scheduler;

(iii) using separate batch schedulers for NatWest and Ulster Bank; and

(iv) adequately testing the consequences of backing out the batch scheduler software upgrade in a representative testing environment.

(2) The Three Lines of Defence did not take sufficient care to control IT risks responsibly and effectively for the following reasons:

(a) Technology Services Risk (part of the First Line of Defence) did not:

(i) devote sufficient time and attention to specific risk management activity instead it concentrated on reporting risk upward and obtaining "sign-off" instead of understanding and managing IT risk; and

(ii) take the initiative to identify risks, instead it reacted and responded to incidents.

(b) Business Services Risk (part of the Second Line of Defence) did not:

(i) appropriately challenge the completeness and depth of the First Line of Defence's coverage of IT risk;

(ii) understand the breadth and depth of its work because it concentrated on collating and reporting of risk information; and

(iii) understand IT risk well enough, instead it focused too much on systems and processes rather than understanding IT risk.

(c) Group Internal Audit (the Third Line of Defence) did not:

(i) explain its different view of IT Risk to the First and Second Lines of Defence;

(ii) close IT audit issues in a timely fashion, instead, it brought forward incomplete IT audit plans from previous years; and

(iii) explain in its final audit report that it lacked the documentation it needed to fully test the controls for backing out the batch scheduler software.

(3) The RBS Group:

(a) had a limited understanding of IT operational risk:

(i) it did not ensure that Technology Services, the function with the broadest view of IT risk in the RBS Group, had a sufficient role at divisional board level or direct involvement in business prioritisation; and

(ii) its IT risk appetite focussed on recovering from disruptive incidents rather than on incidents that are more probable and can potentially have an equivalent effect.

(b) exposed the Banks to a greater risk of IT failures because it approved an IT Continuity Policy Standard which:

(i) focused on low probability events (e.g., total loss of a data centre) rather than on more probable events (e.g., software failures) which could have a potentially equivalent effect; and

(ii) should have included a much greater focus on IT Resilience and the need to ensure that the activities most critical to its customers could withstand the effect of disruptive events.

6. SANCTION

Financial penalty

6.1. The Authority's policy for imposing a financial penalty is set out in Chapter 6 of 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. The Relevant Period in this case is from 1 August 2010 to 10 July 2012, so the five-step penalty framework applies here.

Step 1: disgorgement

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

6.3. The Authority has not identified any financial benefit that the Banks derived from the breaches.

6.4. Step 1 is therefore £0.

Step 2: the seriousness of the breach

6.5. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

6.6. A wide range of the Banks' product lines and banking services were potentially at risk of serious disruption because of the Banks' failure to have adequate IT risk management systems during the Relevant Period. Those banking services and product lines were severely disrupted during the IT Incident. The revenue generated by the business areas affected by the IT Incident during the Relevant Period was £20.5 billion. The Authority considers that a financial penalty based on revenue of £20.5 billion would be disproportionate to the harm caused by the breach.

6.7. To arrive at a penalty, the Authority has adopted the approach set out in DEPP 6.5A.2G (13) and has taken the following factors into account to determine the Step 2 amount:

(1) The IT Incident affected at least 6.5 million customers.

(2) The IT Incident caused the Group to pay:

(a) £70.3 million in redress to UK customers; and

(b) £460,000 to consumers who were not customers of the Banks.

(3) The IT Incident caused distress to customers and non-customers.

(4) The Banks received 69,500 complaints (including the 17,800 complaints Ulster Bank ROI received).

(5) The IT Incident caused the Banks to take corrective action on 7 million accounts (this includes 1.9 million accounts at both Ulster Bank NI and ROI).

(6) The weaknesses in the Banks' IT governance and control processes, as provided by the RBS Group, were serious.

(7) The Banks, through the RBS Group's IT functions, had the opportunity to identify and correct the failures which led to the IT Incident well before the risk crystallised.

(8) The IT control deficiencies contributed to the IT Incident and revealed serious weaknesses in the Bank's procedures, management systems and internal controls.

(9) The breaches were neither deliberate nor reckless.

(10) The penalty needs to act as a credible deterrent.

6.8. Taking all of these factors into account, the level of seriousness is 4 and the Step 2 figure is £60 million.

Step 3: mitigating and aggravating factors

6.9. 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, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach.

6.10. The Authority has considered the Banks' previous disciplinary record and general compliance history as an aggravating factor. That history is as follows:

(1) In August 2014 the Authority fined RBS and NatWest £14,474,600 for serious failings in their advised mortgages business.

(2) As at the first quarter of 2014, RBS Group Plc's provision for compensating customers who were mis-sold PPI was £3.1bn.

(3) In February 2013, the Authority fined RBS £87.5m in relating to LIBOR submissions. This involved an assurance to the Authority that the systems and controls in relation to LIBOR submissions were adequate (when they were not).

(4) In July 2013, the Authority fined RBS (and the Royal Bank of Scotland N.V) £5.6m for failing to report transactions it was required to report in an accurate and timely manner. It was noted in this case that the systems and controls failures were not adequately prioritised when it was apparent significant work was needed to ensure they were effective. In March 2012, the Authority fined Coutts & Co (a wholly owned subsidiary of the RBS Group) £8.75m for breach of anti-money laundering rules.

(5) In November 2011, the Authority fined Coutts & Co £6.3m in relation to the mis-selling of AIG bonds. In this matter, Coutts & Co failed to undertake an effective compliance review in a timely manner and failed to take prompt and effective action to address the issues raised.

(6) In January 2011, the Authority fined RBS and NatWest £2.8m in relation to complaints handling.

(7) In August 2010, the Authority fined RBS, NatWest, Coutts & Co and Ulster Bank Ltd (a wholly owned subsidiary of the RBS Group) £5.6m for breach of anti-money laundering rules. Actions to address the issued identified by the firm were not taken in a timely manner.

(8) In December 2002, the Authority fined RBS £730,000 for breach of anti-money laundering rules.

6.11. The Authority considers that the following factors are mitigating:

(1) The Group took the initiative to commence the customer redress exercise.

(2) The Group have not only paid redress to customers, but they have also made good-will payments to some of them.

(3) The Group made payments to non-customers through an innovative centralised solution for non-customer redress which the Skilled Person said "represents a first in the financial services marketplace".

(4) The Group is taking steps to put in place an IT Resilience programme and significant software improvements to reduce the risk of similar problems arising in the future.

6.12. Having considered these factors, the Authority does not believe that an increase or decrease to the Step 2 figure is appropriate.

6.13. The Step 3 figure is therefore £60 million.

Step 4: adjustment for deterrence

6.14. 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.

6.15. In the Authority's view, the Step 3 figure of £60 million represents a sufficient deterrent to the Banks and others and so has not increased the penalty at Step 4.

6.16. The Step 4 figure is therefore £60 million.

Step 5: settlement discount

6.17. 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.

6.18. The Authority and the Banks reached agreement at Stage 1. A 30% discount applies to the Step 4 figure.

6.19. The Step 5 figure is therefore £42 million.

Penalty

6.20. The Authority therefore hereby imposes a financial penalty of £60 million (before the Stage 1 discount) on the Banks for their breaches of Principle 3.

7. PROCEDURAL MATTERS

Decision maker

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

7.2. This Final Notice is given under, and in accordance with, section 390 of FSMA.

Manner and time for Payment

7.3. The financial penalty must be paid in full by the Banks to the Authority by no later than 4 December 2014, 15 days from the date of the Final Notice.

If the financial penalty is not paid

7.4. If all or any of the financial penalty is outstanding on 5 December 2014, the Authority may recover the outstanding amount as a debt owed by the Banks and due to the Authority.

Publicity

7.5. 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 you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

Authority contacts

7.6. For more information concerning this matter generally, contact Anna Couzens (020 7066 1452) or Maria Gouvas (020 7066 3552) of the Enforcement and Financial Crime Division of the Authority.

Megan Forbes
Project Sponsor
Financial Conduct Authority, Enforcement and Financial Crime Division

ANNEX

1. JOINT INVESTIGATION

1.1. On 1 April 2013, a new "twin peaks" regulatory structure came into being under which the Financial Services Authority was replaced by Financial Conduct Authority ("FCA") and the Prudential Regulatory Authority ("PRA"). The effective date of that change, 1 April 2013, is known as Legal Cutover ("LCO"). Following LCO both the FCA and the PRA have an enforcement remit and are able to exercise a range of enforcement powers and impose sanctions under FSMA.

1.2. Although the conduct to which this matter relates occurred prior to LCO, Part 5 of the Financial Services and Markets Act 2012 (Transitional Provisions) (Enforcement) Order 2013 ("Order") permits the PRA and/or the FCA to take action to address contraventions occurring pre LCO but for which the PRA and/or FCA would have been an appropriate regulator had the contravention occurred on or after LCO. Both the PRA and the FCA therefore have the ability to take action in this matter.

1.3. In April 2013, the FCA and PRA agreed to undertake a joint investigation into the IT Incident. The FCA and the PRA are both permitted to take action pursuant to the Order.

1.4. The FCA and PRA considered a joint investigation necessary because the failings encompassed both conduct and prudential issues and therefore had implications for the statutory objectives of both regulators. In particular, the matter is relevant to:

(1) The FCA's overarching strategic objective of ensuring that the relevant markets function well and the advancement of the FCA's operational objectives of (i) securing an appropriate degree of protection for consumers and (ii) protecting and enhancing the integrity of the UK financial system; and

(2) The PRA's general objective of promoting the safety and soundness of PRA authorised persons by "seeking to ensure that the business of PRA-authorised persons is carried on in a way which avoids any adverse effect on the stability of the UK financial system" under section 2B(3)(a) of FSMA; specifically where adverse effects may result from the disruption to the continuity of financial services.

2. RELEVANT STATUTORY PROVISIONS

2.1. 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 FSMA).

2.2. 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) FSMA). The Authority's strategic objective is ensuring that the relevant markets function well (section 1B(2) FSMA). The Authority has three operational objectives (section 1B(3) FSMA).

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

3. RELEVANT REGULATORY PROVISIONS

3.1. In exercising its power to issue a financial penalty, the Authority must have regard to the relevant provisions in the Handbook of rules and guidance ("Handbook"). The Handbook provisions relevant in this matter are the Principles, the Decision, Procedures and Penalties Manual ("DEPP"), and the Enforcement Guide ("EG").

3.2. The Principles are a general statement of the fundamental obligations of firms under the regulatory system. They derive their authority from FSMA's rule-making powers and reflect the Authority's regulatory objectives. The relevant Principles in this matter is Principle 3:

> *"A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems".*

3.3. 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 in respect of financial penalties imposed on firms. The conduct that is the subject matter of this action took place after 6 March 2010.

3.4. EG sets out the Authority's approach to taking disciplinary action (Chapter 2) and issuing financial penalties (Chapter 7).

(1) EG 2.1 states that:

(a) The FCA's effective and proportionate use of its enforcement powers plays an important role in the pursuit of its statutory objectives, including its operational objectives of securing an appropriate degree of protection for consumers, protecting and enhancing the integrity of the UK financial system. For example, using enforcement helps to contribute to the protection of consumers and to deter future contraventions of FSMA. It can also be a particularly effective way because publication of enforcement outcomes raises awareness of regulatory standards.

(2) EG 7.1 states that:

(a) The effective and proportionate use of the Authority's powers to enforce the requirements of FSMA will play an important role in the FCA's pursuit of its statutory objectives.

(b) Imposing financial penalties shows that the FCA is upholding regulatory standards and helps to maintain market confidence and deter financial crime.