RBS Group

Summary in relation to the major IT systems failure affecting the RBS Group in June/July 2012, response and remediation plans

March 2013

This document was produced with the input of Clifford Chance.

Contents

1. Introduction

1.1 On Tuesday 19 June 2012, RBS, NatWest and Ulster Bank (the "Group") suffered a major IT Incident affecting the Group's overnight batch processing systems, which caused severe disruption to many of its IT systems serving operations in the UK and Ireland (the "IT Incident").

1.2 The IT Incident resulted in the Group being unable to update customer account balances, process payments or participate fully in clearing within normal timeframes.

1.3 We sincerely apologise to all those affected for the impact that the IT Incident had on our customers and other parties. The IT Incident shows our continuing need to improve our risk and control systems and it is important that we fully analyse and understand the causes of the IT Incident.

1.4 The IT Incident had unacceptable consequences for many of our customers in the UK and the Republic of Ireland. We have sought to ensure that customers who were affected were appropriately compensated and have worked hard to improve the underlying causes of the IT Incident as identified by various internal and external reviews undertaken by experts.

1.5 The Group did everything it could to recover from the IT Incident as quickly as possible. Thousands of employees were involved both in recovering from the technical issue and in supporting customers. They worked tirelessly. The response of staff in branches, call centres and elsewhere in dealing with the problems was outstanding.

1.6 While RBS, NatWest and Ulster Bank were impacted, the effects of the IT Incident were particularly severe for Ulster Bank due to the duration of the recovery. Ulster Bank made significant efforts to help customers who were affected, extending branch hours, tripling call centre staff and providing full redress.

1.7 This summary document summarises the background to the IT Incident, the Group's response and its improvements to the IT infrastructure.

2. Description of the IT Incident, our response and customer redress

Background

2.1 Each evening, thousands of individual processes involving the Group's various back office and banking systems need to be completed in sequence, primarily in order to implement the previous day's banking business and bring all account balances and transaction information up-to-date. The different processes, which include processing counter transactions, interbank clearing, affecting money market transactions, payroll processing and making changes to standing orders or to customer addresses are individually referred to as "batch jobs" and each batch job performs a specific task within the bank's systems.

2.2 Each batch job needs to be performed in the correct logical sequence, relative to the other batch jobs. A "batch job schedule" is the defined sequence of batch jobs that needs to run on a certain day (collectively referred to as a "batch"), including the order they run in, and the data resources (such as files and databases) they require. The batch job schedule comprises a large and complex series of batch jobs which run in accordance with pre-determined time-driven and/or event-driven triggers, with certain batch jobs required to be undertaken before others can follow.

2.3 A "batch scheduler" is software that executes the sequence of the batch by placing batch jobs into queues and ensuring that the batch jobs are processed in the correct order.

2.4 The Group uses multiple instances of the same batch scheduler software package within its IT environment. In June 2012, there were two instances of the software for the main banking brands within the Group: one for RBS, and one which was shared by NatWest, Ulster Bank in Northern Ireland ("Ulster Bank NI") and the Republic of Ireland ("Ulster Bank RoI"). These instances are periodically upgraded to newer versions of the batch scheduling software.

The batch scheduler upgrade

2.5 By June 2012, thirty-five instances of batch scheduler software package in use at RBSG had been successfully upgraded to a newer version, a process which had begun in Autumn 2011. The NatWest and Ulster Bank instance of the batch scheduler, as the largest instance in the Group, was upgraded last, on Sunday 17 June 2012. The upgraded version included two maintenance releases provided by the supplier. During the evening of Monday 18 June 2012, after the upgrade and maintenance releases were applied, the NatWest and Ulster Bank instance was observed to be using significantly more processing capacity than usual. This resulted in long response times and failures known as "batch terminal failures" occurring.

2.6 These issues indicated that, following the upgrade, the NatWest and Ulster Bank instance of the software was not operating as it should. Consequently, and in accordance with RBSG standard practice in such situations, on Tuesday 19 June 2012, it made a technical decision to reverse the upgrade until the performance issues were resolved. In more technical language, the decision was to roll back the batch scheduler software package to a "stable known state" by "backing out" the upgraded software to revert to the previous version.

Missing batch jobs

2.7 The back out process began after normal business hours on Tuesday 19 June 2012. Following the back out process, it was discovered that the schedule of batch jobs in the batch job scheduler was not complete: some batch jobs were missing and others were out of sequence. Having identified that batch jobs were missing, RBSG technicians attempted to restore the batch jobs manually.

2.8 At approximately 11pm, RBSG discovered that there were significantly more jobs missing than originally identified. At this stage, recovery became far more complex and a "major red" alert was initiated by the Group.

2.9 The batch schedule was complex and included dependencies between the Group brands. As a result, the RBS brand was affected as well as the brands running on the NatWest and Ulster Bank instance. Failures and delays to the batch schedules for NatWest, Ulster Bank and RBS increased in number and complexity, creating a snowball effect.

2.10 Upon subsequent investigation it became apparent that the upgrade had reformatted data in the batch jobs such that the software was not capable of reading the data properly following the back out process to the earlier version. The ability to reverse an upgrade is sometimes referred to as "backwards compatibility", and is a standard feature in sophisticated software products.

Recovery

2.11 As soon as it became apparent that jobs were missing from the batch queues, RBSG technical staff focussed on re-loading jobs into the queues. The first night of recovery was critical. By the morning of Wednesday 20 June 2012, the NatWest batch for Tuesday 19 June 2012 was largely completed, achieving the key deadline of having account balances up to date for the coming day (known as "NAP turnaround") albeit more than four hours later than the normal target time. However, Ulster Bank batches did not reach NAP turnaround on Wednesday.

2.12 Of key significance in understanding the additional delay to Ulster Bank is that Ulster Bank NI and Ulster Bank RoI started the business day on Wednesday 20 June 2012 with a significant backlog to batch processing. The Ulster Bank batch reached a point in the early morning of Thursday 21 June 2012 where NAP turnaround was more than one day behind, referred to as T-1. This meant that the next day's batch started processing before the completion of the current day's batch. The two batches interfered with each other because there were multiple days' files in the system and multiple days' jobs on the queues. This caused additional recovery problems and further backlogs.

2.13 By the beginning of the second week, 25 June 2012, NatWest was generally considered to have recovered from a critical business deadline perspective. RBS, although affected, never came close to becoming a full day behind.

2.14 Ulster Bank achieved NAP turnaround for 19/20 June 2012 on Sunday 24 June 2012. Ulster Bank did not return to T-0 until Tuesday 10 July 2012.

2.15 Recovery was achieved by the use of forecasting functionality within the system which enabled RBS Technology Services (the centralised Group IT function which provides IT services to the Bank) to accelerate processing of batches through increased automation.

2.16 Thousands of RBSG employees were involved in the technical recovery, many of whom worked extremely long hours.

The Group's response

2.17 From the start of the IT Incident the Group focused substantial effort at all levels on resolving it and remediating the impact on all customers.

2.18 The Group implemented key operational changes across the Group including extending branch opening hours, providing additional cash advance limits, delivering additional cash to branches and ATMs, and establishing urgent payment processing solutions including solicitors' indemnity arrangements for key mortgage transactions.

Customer Redress Programme

2.19 The Group initiated an extensive customer redress programme in response to the IT Incident. The IT Incident affected many Group customers and non-customers. The redress programme covered both the Group's own customers as well as affected customers of other banks.

2.20 The key purpose of the customer redress programme was to limit the impact on customers where practical and put every customer back to the position that would have existed absent the IT Incident, erring in the customer's favour in providing redress when in doubt.

2.21 The customer redress principles were developed centrally with each business developing and implementing its own redress programme in line with the principles. The approach to customer redress was substantively structured around two core components:

(a) Proactive redress – whereby customer accounts were automatically corrected for incorrect charging and debit/credit interest; and

(b) Reactive redress – responding to complaints from impacted customers.

2.22 RBSG also established a non-customer redress approach to allow those who were not its customers but who had been impacted by the IT Incident to seek redress. We worked with the Payments Council in the UK and the Irish Payment Services Organisation in Ireland to develop principles for these approaches.

3. How the Group will fix the issues identified

3.1 The external experts have made recommendations to help prevent a similar incident occurring in the future. The Group has implemented a large number of these recommendations already and has put in place plans to implement the remainder. A number of external partners are working with the Group to implement its responses to the recommendations, and this work is being progressed as a priority.

3.2 The Group has made changes over recent months to improve IT resilience, which means that RBSG's systems are now able to get up and running a lot faster than would previously have been the case.

3.3 A new Group Chief Administrative Officer will be appointed. They will continue the programme of work initiated following the IT Incident.

3.4 The Group's remediation efforts have been divided into three workstreams:

(a) RBS Technology Services;

(b) Business Resilience; and

(c) Customer Redress.

(A) RBS Technology Services

3.5 The Group's work in relation to RBS Technology Services has been designed to minimise both the probability and potential impact of another technology incident. Since some of the more complex components of this work will extend into 2014, immediate steps have been taken to strengthen prevention capabilities. This will significantly improve the Group's risk management capability, as well as increasing both the resilience and the recoverability of legacy technology.

3.6 This work will be RBS Technology Services' foremost priority throughout 2013. The programmes have been formulated to meet three equally important goals:

(a) The first is to identify lessons learned from the IT Incident itself. Based on analysis of root cause and the subsequent recovery, the Group has implemented a series of improvements to the way it monitors and recovers systems. A review of how mainframe software is deployed is being undertaken to improve the risk assessment process.

(b) The second is to reduce quickly the Group's exposure to the risk of another high impact incident. Risk management and some preventative technology processes have now been strengthened, and will continue to be so during the first half of 2013. These improvements are being implemented in parallel with less complex enhancements to systems, and are taking place well in advance of longer-term technical re-engineering.

(c) The third is to target and prioritise higher risk findings, which include a range of short, medium and long-term objectives.

3.7 Work on four co-ordinated projects has begun to address the recommendations of the external experts:

(a) A Risk Transformation Programme is being planned. The Group will set processes by which technology risks are proactively and systematically managed to meet wider goals, and discussions of technology risks with other business divisions will be strengthened.

(b) A Batch Transformation Programme is underway. This is designed to improve and optimise batch scheduling systems to improve the Group's ability to recover from similar incidents. Risks associated with batch processing are being reduced by carrying out more processing in real time or near-real time.

(c) A Technology Resilience Programme is underway. The programme will ensure that the approach to IT resilience uses best industry practices, and delivers improved customer services by providing more resilient systems.

(d) An IT Critical Processes Programme is at the planning stage. The aim is to review and strengthen critical technology processes, and ensure that they all work together to support the Group.

3.8 A number of organisational changes have been made to strengthen the Technology Services Risk function. The RBS Technology Services Risk organisation has been simplified and a new executive post of Chief Risk Officer, RBS Technology Services created, reporting directly into the Chief Information Officer (CIO). A new senior technical role, Head of Production Change, has been created within RBS Technology Services. Additional Senior Management capability has been recruited to strengthen the Business Services Risk team and a specialised Head of Technology Audit is being hired into the Group's Internal Audit function.

3.9 The projects outlined above are being overseen by the Chief Information Officer of the Business Services division.

3.10 The Group will invest significantly in these programmes, which will deliver benefits and improvements both to the Group and its customers.

Improvements made to date

3.11 Between August 2012 and January 2013, a number of steps were taken to mitigate specific batch processing risks, improve future recoverability, strengthen the way the Group approaches changes to systems and assess wider technology resilience.

3.12 A range of improvements have been delivered:

(a) Greater flexibility in running batch processes – batch processes can now run outside their normal time window, which improves the ability to recover from batch scheduling problems.

(b) Emergency procedures to separate key banking brands – a procedure to break the dependency between the key banking brands of the Group in an emergency has been formalised.

(c) Improved monitoring of batch processing – automated monitoring tools for some of the critical batch processing now exist which allows identification of missing transaction files at an earlier stage.

(d) Improved ability to update customer balances – updates to customer balances can

be effected for a limited number of financial transactions even if problems with batch processing systems are encountered.

(e) File dependencies – implementation of a new technical utility which reduces the potential for conflicts between batch and online processing has started. This will reduce the complexity within the environment and lessen the impact of any problems with the batch scheduling systems.

(f) New testing framework introduced for application development – the scope and depth of testing has been clarified and enhanced.

(g) New Production Change Board instituted – a panel of experienced and senior technology leaders has been formed to scrutinise project implementation plans for potentially high impact changes to production systems.

What will be done in the medium and longer term?

3.13 Many of the most significant structural improvements fall within the Batch Transformation and Technology Resilience programmes. These technical streams address legacy platform risks within the IT environment. The Batch Transformation and Technology Resilience programmes are currently underway and will deliver a number of improvements throughout 2013 and 2014 to reduce legacy platform risk.

3.14 The Batch Transformation Programme will deliver benefits and improvements including:

(a) Independent batch scheduler – today, the NatWest, Ulster Bank NI and Ulster Bank RoI batches run on the same system, although they can be run separately in an emergency. By the end of 2013 each brand will run on a separate system. This will significantly reduce the risk of a single batch scheduler incident impacting multiple brands. This change is an important component of RBSG's plans to reduce the risk of an incident of this type reoccurring.

(b) Customer balance updates – today, in the event of a batch issue, the Group has the ability to update customer balances on a "real time" basis for a limited number of financial transactions normally processed via the batch. By the end of 2013, the Group will have the ability to update customer balances for the majority of financial transactions on a real time basis. This ability will protect customer services in the event of a batch incident.

(c) Batch complexity – the batch is being restructured so that the Group can run critical elements on their own in the event of a significant batch failure. This will allow parts of the batch that are not essential to customer services to be put to one side whilst recovery from the failure is effected. This will be completed by the end of 2014.

(d) Batch and online interaction – currently the Group's online and batch systems are not directly linked, leading to a risk of online transactions being impacted by any batch incident. By the end of 2013, the management of online environments for key online services will be directly linked to the batch scheduler, removing the complexity and lessening the impact of any problems with the batch scheduling systems.

(e) Batch monitoring – the Group continues to develop software tools to monitor critical payments feeds. By the end of 2013, this work will be complete for all 150 critical payment feed processes.

3.15 The Technology Resilience Programme will deliver benefits and improvements including:

(a) Improving disaster recovery capabilities – during disaster recovery testing of mainframe systems, the Group has always switched to the backup system on the Saturday and reverted to the production systems before the Monday morning. This is partly because weekday testing would affect ongoing development capability (although it would not prevent RBSG from invoking disaster recovery in a real disaster scenario). The Group will introduce new functionality and enhanced capability to allow a switch to a backup system as well as continuing to run production services from the backup systems by the end of 2013, and this capability will be fully operational by the end of 2014.

(b) Expansion of disaster recovery policies and capabilities – currently the IT continuity policy and capability primarily address the risk of a data centre loss. Throughout 2013 and 2014 the Group will expand the policy and capability to deal with other failure scenarios such as a loss of key retail banking services or key payments services.

(c) Third copy of key data – the Group's key systems data is currently replicated in real-time between production systems and back-up systems. This is to address the risk of a data centre failure. To protect against data corruption, the Group will build the infrastructure for an asynchronous (i.e. non real-time) third copy of its key systems data by the end of 2013, and this capability will be fully operational during 2014.

(d) Simplifying non-key systems – a number of the infrastructure services that support customer facing systems are complex. By the end of 2014 the Group will have simplified and upgraded or separated non-key systems, enabling sufficient resilience and resilience testing in customer facing systems.

(e) Demonstrating data centre resilience – disaster recovery testing processes will be extended to include infrastructure such as networks. By the end of 2013 the Group will be able to demonstrate that resiliency of networks in data centres.

3.16 By the end of 2013 the parts of the Batch Transformation Programme that are not dependent on significant application development will be materially complete. Thereafter the foundations for longer term improvements during 2014 will also have been laid.

3.17 By the end of 2013, the Risk Transformation Programme will have completed a review of the capability and capacity of the current RBS Technology Services Risk function and implemented any changes to ensure the team is appropriately sized and focused. External support has been engaged for the existing RBS Technology Services Risk function while this work is underway.

3.18 An IT Risk Framework which conforms to industry standards will be implemented to review, document and strengthen the majority of the Group's critical IT processes by the end of 2013. Where appropriate, training and accreditation for staff and an extensive programme of cultural change will be initiated.

3.19 In 2014, the work requiring longer term technical design will be completed. The cultural change with respect to risk management and critical processes will continue to be embedded. Some parts of the Batch Transformation Programme that require work on applications will conclude in 2014. The Group intends to have implemented all proposals across all four technology programmes by the end of 2014.

(B) Business Resilience

3.20 RBSG recognises the importance of being resilient so as to withstand disruptive events but also to support longer term thinking about new risks and opportunities. Prior to the IT Incident, a Business Resilience function was formed which is driving business continuity to ensure the resilience of the most critical customer systems.

3.21 Before the IT Incident, a commitment to improving resilience capability had already been made and a number of additional steps are now being taken to address the recommendations made by the external experts:

(a) A Group-wide single point of failure analysis was completed in 2012.

(b) A new approach to assess the resilience of critical economic functions was developed, which has been successfully piloted and will be rolled out across customer critical activities.

(c) The Business Continuity and IT Continuity policies is being strengthened and this work is expected to be completed by the end of June 2013.

(d) A deeper culture of resilience across the Group will be embedded to help ensure that customer-critical activities are better protected to withstand the impact of disruptive events should they occur.

3.22 The Group's Incident Management Framework stood up well during the IT Incident. As with all major incidents, there are lessons to be learned from the IT Incident for the incident management processes, and appropriate actions. Any gaps in capability that were identified during the IT Incident will be closed.

(C) Customer Redress

3.23 Overall the Customer Redress programme was found to have delivered appropriate outcomes for affected customers of the Group and customers of other banks.

3.24 Steps have been taken to enhance redress documentation where the review recommended that this would be appropriate.

3.25 The Customer Redress programme was closed on 30 January 2013 after each divisional redress programme had fulfilled certain pre-agreed exit criteria. These criteria included the resolution of any quality assurance findings, implementation of recommended actions from the reviews, and completion of project close-down documentation.

3.26 RBSG is formalising a Group-level policy on dealing with vulnerable customers, including customers in financial difficulties. This is part of the new Conduct Risk policy framework and is intended to be implemented by the end of June 2013.


RBS