Ross McEwan
Chief Executive

RBS

Gogarburn
Edinburgh
EH12 1HQ
Telephone: 0131 556 8555
Direct: 0131 523 2033
Facsimile: 0131 523 5812
www.rbs.com

30 July 2015

Rt Hon Andrew Tyrie MP
Chairman of the Treasury Select Committee
House of Commons, Committee Office
7 Millbank
London SW1P 3JA

Dear Andrew,

I am writing further to my letter to you of 8 July 2015 regarding the IT incident at RBS on 15 and 16 June. The post incident analysis into the root cause of the incident has now been completed and I am now able to deal with the outstanding points from my previous response to you. These are the cause of the problem and how it differs from the 2012 incident. I will take each of these points in turn in this response which should also be read in conjunction with my earlier letter.

What happened and why?

The incident was triggered by the expiry of a digital security certificate used to authenticate encrypted connections between the bank and third-party systems. This interface is known as the Multi Enterprise Financial Gateway (MEFG). This system connects our payments processing systems to the external SWIFT network and on to VocaLink, who as you know, provide the infrastructure underpinning Bacs payments in the UK. The expiry of the certificate prevented the link between our payments processing systems, the external SWIFT network and on to VocaLink for Bank Giro transactions from operating. The failure of this link impacted the functionality of the MEFG and our ability to process inward payments and messages from VocaLink.

The reason the MEFG was impacted by the expiry of this certificate was because the certificate, which was renewed as part of our regular maintenance work on Saturday 6 June (prior to its expiry on Monday 15 June) underpinned two different functions. One of the two functions this certificate carried out was known and documented (the link to the business user interface), so the new certificate was created and configured to address this requirement. The second function (securing the link to the SWIFT network) was not known, had not been documented and consequently, the new certificate had not been prepared to preserve this second requirement. As such, when the old certificate expired, the undocumented functionality stopped working, effectively removing our ability to receive transactions from VocaLink.

RBS

A certificate can be used for more than one function, however all aspects of its use, implementation and renewal must be fully recorded in release and support documentation. The review of the documentation surrounding the implementation of this certificate which dates back to February 2012 has identified no documentary record of the second function of the certificate. The renewal on Saturday 6 June was the first time the certificate had required to be replaced since the implementation of the MEFG several years ago. This also meant that we did not fully understand the nature of the problem quickly enough, and so coming up with a recovery plan took longer than it otherwise would have done.

How does this incident differ from the 2012 IT failure?

As outlined above this incident was caused by undocumented and unknown functionality of a digital certificate. This is completely different to the root cause of the June 2012 incident which, as we have previously updated the Committee, was the result of a software fault in third party supplied software alongside aggravating factors including our processes for testing maintenance patches, a single batch scheduler supporting multiple bank brands, the overall batch size, complexity, organisation and resilience.

Externally assured improvements introduced since 2012 allowed us to contain the impact to Bacs processing with no wider incremental impact. Whilst the core batch was affected by the unavailability of delayed Bacs files, there were no impacts to other payments processes, no broader implications for the daily balance refresh and no additional impact to our readiness for the "start of day". Our ability to isolate the impact to Bacs was due to the benefits delivered by the substantial investment in our system resilience and stability since 2012.

Summary

As I set out in my prior letter, the disruption and inconvenience this incident caused our customers was unacceptable. We fell well short of the standards we set ourselves and we will ensure that no customer finds themselves out of pocket as a result. To that end, we provided emergency cash or temporary credit facilities to any impacted customer who needed them. All fees, charges or interest impacts were resolved centrally, and we also waived any authorised and unauthorised overdraft fees for the five working days following payments being applied.

In addition, as you would expect following an incident of this nature, we have moved quickly to address the points identified in our analysis to ensure a similar incident cannot occur in future. These points range from addressing the root cause through to ensuring that more granular information is available to improve decision making and customer communication during any such incidents. We are introducing a four step process to help mitigate the certificate risk, consisting of an automated inventory tool with supplementary manual inspection, changes to the renewal process and the phasing of certificate renewals.

While we will ensure the learnings from this incident are fully absorbed and implemented I believe that overall our recovery from the incident benefitted from our experience of the 2012 incident allowing us to isolate the issue to one batch process for a shorter period and to ensure that no other payments, other than Bacs payments, were impacted.

RBS

We continue to work closely with the Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA) on this issue and will keep them updated as we address the identified points stemming from the incident. I have copied this letter to the Chief Executive's of both the PRA and FCA.

Yours sincerely,

Ross McEwan

Cc. Martin Wheatley, Chief Executive - Financial Conduct Authority
Andrew Bailey, Chief Executive Office – Prudential Regulation Authority