Rt Hon Nicky Morgan MP
Chair of the Treasury Select Committee
House of Commons
Committee Office
London
SW1A 0AA

28 September 2018

Dear Chair,

Re: NatWest and RBS Service Failure 21st September 2018

Thank you for your letter of 21st September regarding the NatWest, RBS and Ulster Bank service disruption that prevented some of our customers from accessing their accounts. Firstly can I say that this does not meet the standards we set ourselves for customer service and I would like to use this opportunity to apologise again to all customers affected by the incident. I would also like to assure you that no customer will be left out of pocket as a result of this outage and we have investigated thoroughly what went wrong and continue to liaise with our regulators to explain how and why the incident happened.

I understand the role the Bank plays as a key supporter of the UK economy and as a result we need to ensure that businesses and personal customers are able to access their accounts through their preferred channels. In this case our contingency procedures worked effectively and we were able to contain the incident, resolve it as swiftly as possible, keep our customers and regulators informed of what was going on and ensure our customers were able to access their accounts by 09:30.

As an overview of the incident, our own monitoring systems identified a problem at 05:03 on the 21st September and customers started contacting our telephony agents at 05:05 to make us aware of a problem accessing their accounts online and through the mobile app. The cause was quickly recognised as the result of an incorrect implementation of a network firewall rule update. We update our firewall rules around 800 times annually and it is very rare for an incident like this to occur.

We have investigated the incident thoroughly and, in the short term, we will implement an extra check to try to avoid the same problem occuring again. For the longer term we are already migrating to a new generation of network infrastructure which, we believe, will increase the resilience of our systems. Overall this year we are investing around £300 million on improving our infrastructure. This represents the continuation of a period of major investment in improving the resilience and recoverability of our systems over the last 6 years.

During the period of the incident, our customers had access to cash via ATMs and cashback at Point of Sale. Our emergency cash process was available to support vulnerable customers. Although call volumes increased, Telephone Banking was also available for customers to undertake banking and make any payments. We have also confirmed that payment processing was not directly impacted by this issue, although our digital channels were not able to take payment instructions from customers.

I hope this gives you the overall context of the incident. Turning to the specific questions in your letter:

When did RBS first become aware of the system failure; when were you personally informed of it; when did you first inform the Financial Conduct Authority?

Our own monitoring systems identified a problem at 05:03 on the 21st September and customers started contacting our telephony agents at 05:05. After initial investigations by onsite technicians, senior managers within our Technology Services area were informed around 25 minutes later, and our Chief Administration Officer, Simon McNamara, was advised at 06.31 and I was informed at 07.01. The Financial Conduct Authority was informed verbally at 08:30 and this was followed up with a written notification, after which there was regular dialogue between both parties. A PSD2 report was submitted to the FCA at 09:18 and after further calls, another written update was provided to the FCA at 14:51 which contained high level information about the incident trigger, root causes and recovery actions. We also contacted the PRA at 08:30 verbally and then followed up with an e-mail and we also contacted our regulators in Jersey, Guernsey, Isle of Man and Gibraltar at around 09:00 with subsequent updates. The Central Bank of Ireland was also contacted by Ulster Bank Regulatory Affairs at 08:11.

For how long was RBS aware of the system failure before issuing its first public statement on the incident? What subsequent steps did you take to inform customers about the incident and its impact on them?

Our telephony agents were on hand to help customers throughout the incident and our first public statement was issued at 06:30, when we updated our service status pages for eBanking and Mobile Banking. This was followed by a blanket tweet which was issued at 07:00. Both statements identified alternative services to support impacted customers.

What services were unavailable, either wholly or partially, as a result of the failure, and for how many hours in each case?

The primary customer facing services affected were Mobile Banking, eBanking (online banking) and Bankline (our business online banking system). They were unavailable for around four and a half hours. In addition to the above a number of other websites and internal systems were also impacted. These include Open Banking, New Bankline, Bankline Direct & Exchange and Customer Account Opening. See Appendix for more details.

How many and what proportion of (a) business and (b) personal accounts were affected?

Because this was not an intermittent problem, all our customers attempting to use the impacted services were potentially affected. We estimate, based on normal usage patterns, that:
a) in the region of 60,000 Bankline (Business user) logins would also typically have occurred during the impacted period and
b) the volume of requested logins for Mobile and Online Banking during this period would typically have been nearly 2,000,000.

In your assessment, has the risk of fraud to customers been raised as a result of this incident? If so, what have you done to highlight this risk to customers?

When an incident like this occurs our contingency planning ensures that we continue to monitor fraud risk. However it does take slightly longer and resulted in referred customer accounts being blocked until they had been reviewed and authenticity established. This prevents fraud but regretably inconveniences affected customers until the blocked transactions are cleared, where appropriate. This issue affected around 2,000 customers. Our emergency cash service was available to support these customers during the period affected.

What arrangements have you put in place to compensate customers who have lost out as a result of this failure? How, in particular, do you intend to deal with consequential loss claims from business customers?

We have been very public about the fact that no customers will be left out of pocket as a result of this issue. Given that all recovery actions to restore service were completed at 09:31, and the fact we have confirmed that no payment deadlines were missed, we believe it unlikely that there has been any consequential loss. However I would like to take this opportunity to, once again, communicate to our customers that if any of them were left out of pocket we will look into compensating them.

What was the cause of the service failure? Are you completely confident that the causes have been addressed, and that your services are now working as they should?

The root cause of this incident was the incorrect implementation of a network firewall rule update. Once this was identified as being the cause of the issue, the change we had made was reversed and the impacted services were restored.

What controls were in place to mitigate against such a failure, and why did these controls fail to prevent the failure?

We have a primary and secondary peer review control for all network firewall changes. In this case both the reviews incorrectly concluded that the change to be implemented was valid, and would not cause any negative impacts. Therefore, the implementation was progressed. We have investigated the incident thoroughly and, in the short term, we are implementing an additional check to try to avoid the same problem occuring again.

What steps will you be taking to ensure such similar system failures do not happen again?

For the longer term we are already migrating to a new generation of network infrastructure which, we believe, will increase the resilience of our systems. Overall this year we are investing around £300 million on improving our infrastructure and the resilience of our systems. In the immediate term we will implement an additional check in the end to end process for firewall rule changes.

What discussions have you had with the Financial Conduct Authority regarding the incident?

As outlined above we notified the Financial Conduct Authority verbally at 08:30 and communications were ongoing during Friday 21st September. We provided similar updates to our other regulators including the Prudential Regulation Authority and regulators in Jersey, Guernsey, Isle of Man and Gibraltar. The Central Bank of Ireland was also contacted by Ulster Bank Regulatory Affairs at 08:11.

As is common practice, these notifications are co-ordinated by our Corporate Governance and Regulatory Affairs team who will continue to liaise with regulators to ensure any follow-up information is made available.

I hope this provides you with answers to your questions. We will provide the PRA with a comprehensive account of the incident, as well as summarising the steps we are taking to minimise the risk associated with changing our systems. We continually add new functionality and innovative digital capability to support our customers. This generates over 73,000 technical changes, required to both maintain and improve our systems every year and only 0.04% of these result in any unplanned impact to the continuity of our service to customers.

However that does not detract from the fact that we let our customers down for a period of time and I would once again like to apologise to our customers for any inconvenience caused. I hope my answers show that we responded quickly and thoroughly to the incident and managed to restore full banking facilities by 09:30, while also keeping our regulators and customers informed of what was going on.

As finance becomes increasingly digital as a result of consumer demand, we will continue to invest in, improve and build the resilience of our systems. We hold ourselves to high standards when it comes to customer service and while we may not always get it right, we will always strive to ensure we react to problems when they occur in an efficient and professional way.

Yours sincerely,

Ross McEwan, Chief Executive Officer

Appendix: Service Impact

The customer facing services affected were;

Mobile Banking, eBanking, Open Banking, Bankline, New Bankline, Bankline Direct & Exchange and Customer Account Opening

In addition to the above a number of websites and internal systems were also impacted by the issue including;

Websites
https://www.lombard.co.uk/
https://lombard.ie/
https://www.rbsif.co.uk/
https://www.natwestmarkets.com/
https://www.business.natwest.com/
https://www.business.rbs.co.uk/
https://www.tools-rbs.co.uk/personal/borrowing-needs/borrowing-needs.html
https://tools.natwest.com/personal/borrowing-needs/borrowing-needs.html
http://www.intermediary.natwest.com/
https://www.rbs.com/
https://www.rbsremembers.com/
https://digital.ulsterbank.co.uk/
https://digital.ulsterbank.ie/
https://personal.natwest.com/
https://personal.rbs.co.uk