Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Data Protection Act 1998
Undertaking follow-up

Royal Bank of Scotland
ICO Reference: RFA0603388

On 15 May 2017 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Royal Bank of Scotland (RBS) in relation to the undertaking it signed on 4 November 2016.

The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented. We believe that appropriate implementation of the undertaking requirements will mitigate the identified risks and support compliance with the Data Protection Act 1998.

The follow-up assessment consisted of a desk based review of the documentary evidence RBS supplied to demonstrate the action it had taken in respect of the undertaking requirements. This included:

- MyKnowledge data protection pages
- Training material
- Fax process
- Copy of thematic review questions
- Results of Assurance thematic review
- Copy of Branch Daily Checklist
- Security Policy

The review demonstrated that RBS has taken appropriate steps and put plans in place to address some of the requirements of the undertaking. However, further work needs to be completed by RBS to fully address the agreed actions.

RBS confirmed that it has taken the following steps:

1. **Procedures are put in place to ensure any reported breach of security relating to personal data is acted upon promptly and**

any containment and remedial measures are swiftly enforced;

- The already established process for breach reporting within the retail bank has been reviewed and amended to make it easier for staff reporting a data protection breach, including instances where communications have been sent to a recipient in error. An amended ereporting form to log any data protection (DP) breach was introduced in December 2016.

- RBS has provided evidence of the guidance it has issued on MyKnowledge; which is an online tool and is the front line's / branch staff's first port of call for guidance on processes. This process has made it easy for staff to report a data protection breach. This guidance includes how to recognise a breach and contains a step by step guide including timescales which stipulates that all breaches require to be reported within 24 hours and where a breach meets the criteria for notification to the regulator, notification is to be submitted to the regulator within 72 hours.

2. **Fax procedures are implemented consistently across all branches and regularly monitored to ensure consistent standards. Compliance with any associated fax policy and guidance should be monitored on an ongoing basis and appropriate steps taken to ensure any failings are rectified with minimal delay by no later than 24 February 2017;**

- For those activities where there is currently no alternative to using faxes, RBS has provided evidence of the new fax procedure implemented in January 2017. The fax process includes the requirement to use pre-programmed numbers and any number added to the list must be double checked by a colleague.

- RBS has provided information on how the new process acts to enforce any remedial measures resulting from a fax data breach. As part of the new fax process, branch managers carry out a weekly check for any faxes sent in error to the wrong recipient and log them as a DP breach. The DP breach logs are continuously monitored by the business, via 'Privacy Champs' who sit throughout RBS' retail businesses. They check that appropriate corrective action is taken when DP breaches arise in their area and escalate any issues as required. The Privacy team further assesses all submissions on a monthly basis to spot trends and root causes, allowing for the identification of additional training and awareness needs. Monthly meetings are held with representatives across the retail bank. RBS states that attendees have been tasked with

ensuring that Privacy matters are understood by their business areas with any areas of concern discussed and escalated to the Privacy team for guidance. However we have not been provided any evidence to support this.

- Evidence has been provided to show how RBS' Assurance teams have checked that the new fax process communication has been understood and is being implemented by their retail business, in form of an Assurance thematic review which was conducted on 16 January 2017, three weeks after the implementation of the new fax process. This activity was completed by Control Quality Managers with support of the Business Embedding & Execution Managers across NatWest, Royal Bank of Scotland & Ulster Bank. The teams have visited 187 branches and spoken to 460 staff members.

- RBS has also provided a copy of the Faxed Themed Review Outcome dated February 2017. The results show that 88% of staff were aware of the new fax process, 96% of staff were able to locate the policy and 78% of staff were aware of the process to follow if they were informed by a customer or a third party of a data protection breach. A check of the pre-programme numbers showed 67% were inputted correctly and 32% incorrectly and of the numbers not pre-programmed, only 39% followed exceptions. According to RBS, the themed review failings in these areas have been addressed by either the CQM during their visit or through local actions plans, however no evidence has been provided to support this.

3. To ensure any alternative revised processes are fully tested for security and reliability and any related guidance is disseminated to all staff

- At the time of the review, this action had not been completed. However, whist no evidence has been provided to support the progress of this action, RBS appears to be considering more secure methods for transferring personal data.

- Work is presently under way to explore technical solutions which will allow switching from fax processes to electronic processes to allow for increased paperless processing within their branch network and telephony business – for example, the implementation of an email scanning solution is being pursued as the long-term alternative to using faxes.

- A phased roll-out is underway and is planned to complete in the first half of 2018. This project is a priority project for the retail bank.

Before introduction of any new technical solution it will be fully tested in line with the Bank's standard processes and procedures and adequate controls put in place to protect customer data.

- RBS should ensure that as soon as practical, all staff handling personal data are provided with relevant guidance in relation to any newly implemented technical solution and trained in those new procedures, in order to safeguard customer's personal data.

4. The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

- RBS carries out ongoing security awareness and education activities. Through these RBS promote and maintain a "security aware" culture across the Bank that educates employees, contractors, third-party users, and business partners on how to protect bank information throughout its lifecycle. Employees are required to complete mandatory manual computer based training, guiding and reminding them of best practice.

- The need for security and confidentiality is addressed through Bank policy (such as the Bank's Security Policy and Privacy & Client Confidentiality Policy) including reminders to staff that data breaches must be promptly and fully internally reported once identified. A snapshot of the Security policy dated 15 December 2016 has been provided, however this is not evidence of the above.

- In addition RBS's Security Policy requires the principles of least privilege and least access to be applied, to ensure that access is not authorised or available if there is no justified business requirement. Customers and Bank employees are identified and authorised before systems access is granted and access is regularly validated to ensure it remains appropriate.

However, RBS should take further action to fully address the agreed steps:

- RBS has provided evidence of the content of a new training session which is available online to staff to highlight the revised breach reporting process and the importance of logging DP breaches. Managers can access this material and deliver it to staff as and when a need for particular staff training is identified. However, no

evidence has been provided to show how many staff have received this training. RBS should implement monitoring and recording processes to assure that all staff who handles personal data receives this training and that it is included in any mandatory refresher training.

- RBS has confirmed that staff are tested on their understanding of, and compliance with, the fax process on an ongoing basis. However, no evidence has been provided to confirm what percentage of staff have been tested, or whether any signed declarations are required from staff confirming their understanding of the new policy. RBS should therefore consider asking staff to sign a declaration to confirm their understanding of the new fax process and breach reporting procedure to ensure all staff are familiar with the new processes.

- RBS has confirmed that a further Assurance review into the new fax process will take place once adequate time has passed for recommended updates to be implemented, however no evidence has been provided as to when this review will take place and how often monitoring of compliance will be undertaken. Whilst we note that progress has been made in this area, we would strongly advise that the follow up review is conducted as soon as possible to ensure the identified failings are addressed promptly.

A copy of this report will be passed to the Enforcement Department.

Date Issued: 18 May 2017

refraining from acting as a result of any information contained in this report.