ICO Ref: **RFA0603388**

# DATA PROTECTION ACT 1998

## UNDERTAKING

Data Controller: The Royal Bank of Scotland plc
36 St Andrew Square
Edinburgh
Midlothian
EH2 2YB

I, Les Matheson, CEO of Personal and Business Banking at The Royal Bank of Scotland hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The Royal Bank of Scotland is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the Royal Bank of Scotland and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed of an incident initially taking place in October 2014, whereby dozens of faxes containing personal data were sent to an incorrect fax number belonging to a third party organisation. Whilst the data controller was informed on repeated occasions it is evident that faxes were being sent to the incorrect number on a regular basis over a significant period of time spanning over 14 months.

3. Whilst the information contained in the faxes was not sensitive, a number did contain customer account information including account number and sort code. The Commissioner's investigation determined that there was a lack of urgency on the part of the data controller in addressing, managing and recovering the fax disclosures. There was little action taken by the data controller to contact the unintended recipient for copies of the faxes in order to investigate the matter and to identify the specific branch concerned. It was only when the Information Commissioner made contact with the data controller that they investigated further and took steps to address the issue. Furthermore the data controller took no proactive steps to confirm that the recipient securely destroyed the faxes.

4. Despite sending a communication to all branch staff to raise awareness of the issue, the faxes continued to be sent to the

incorrect recipient. As these statements are sent on multiple occasions throughout the day and from different branches, the measures and controls introduced are not considered by the Commissioner to be sufficient on a wider organisational basis.

5. The Commissioner has considered the data controller's compliance with the provisions of the Act in light of this matter. The relevant provisions of the Act are the Seventh Data Protection Principle. This Principle is set out in Schedule 1, Part I to the Act.

6. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising her powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

**The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:**

**(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;**

**(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 and by no later than 20 March 2017;**

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

**(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.**

Signed ……
Les Matheson, CEO of Personal and Business Banking
The Royal Bank of Scotland plc

Dated ……

Signed ……
Ken Macdonald, Head of ICO Regions
For and on behalf of the Information Commissioner

Dated ……