ICO Ref: **COM0542736**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Office Holdings Ltd

Classic House
Martha's Buildings
180 Old Street
London
EC1V 9BP

I, Brian McCluskey, Chief Executive of Office Holdings Ltd ('Office'), for and on behalf of Office, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Office Holdings Ltd 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 Office 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 on 29 May 2014 that a member of the public had hacked into an unencrypted historic Office database that was being stored on a legacy server outside the core infrastructure of the current website. This individual had managed to gain potential access to personal data relating to over a million Office customers, including contact details and website passwords. However, the data controller has confirmed that it does not store customers' bank details, so financial information was not compromised. Moreover, there is no evidence to suggest that the information accessed has been further disclosed or otherwise used.

3. The data controller explained that there were several technical measures in place to minimise the risk of such an attack, although the hacker managed to bypass these measures to gain access to the legacy servers undetected. Office has also confirmed that whilst penetration tests were carried out on the new websites before migration, only a single such test was completed on the old system, the results of which were

not concluded or recorded, due to the legacy system being in the process of being decommissioned.

4. Office has explained that removing the historic customer data from the database before migration to the new system was believed to add complexity and a material risk of data mismatches, operation downtime and customer disruption, so as to put the project at risk. However, Office has since accepted that in hindsight, the risks of removing these details before migration were less than originally thought. As such, it would appear that the retention of this historic data, some of which may now be inaccurate, was over-cautious and not strictly required. However, amongst other remedial measures taken by Office since the incident, the servers in question have now been decommissioned, and a new hosting infrastructure is in place.

5. At the time of the incident, Office's public facing privacy policy did not contain any specific reference to retention periods, and no formal data protection training was provided to staff. Office has since confirmed that both these matters are being addressed and that new policies will be formalised early in 2015.

6. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions of the Act are the fifth and seventh Data Protection Principles. These Principles are set out in Schedule 1 Part I to the Act.

7. 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 his 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 fifth and seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

(1) the data controller shall ensure that all of its websites and servers are subject to regular penetration testing;

(2) the data controller shall implement its new data protection policy documents within three months of the date of this Undertaking. These should link to or include a retention and disposal policy for customer data, the requirements of which should be monitored on an ongoing basis;

(3) the data controller shall provide formal data protection training to all Office employees and should introduce regular refresher training to reinforce this provision;

(4) the data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage, and to ensure that any such information is only retained for as long as necessary in relation to the purposes of the processing.

Signed:……

Brian McCluskey
Chief Executive
Office Holdings Ltd

Dated:…….

Signed:……

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated:…….