POL00393766

SCHEDULE 22

PCI COMPLIANCE

1. SCOPE AND INTERPRETATION

1.1 This Schedule sets out Post Office's high level requirements and the Supplier's obligations in relation to Payment Card Industry ("PCI") compliance in respect of card and cardholder data in the Services.

1.2 For the purposes of this Schedule:

"**PCI Failure**" means any failure (other than a trivial failure) by the Supplier or any of its subcontractors to comply with The Supplier's obligations under paragraph 2.2 below; and

"**PCI Standards**" means the PCI Security Standards as they change from time to time (including, without limitation, its PCI Data Security Standard ("PCI DSS"). PIN Transaction Security ("PTS") standard and Payment Application Data Security Standard ("PA DSS"), as such standards are published by the PCI Security Standards Council on its website www.pcisecuritystandards.org.

2. SUPPLIER COMMITMENT

2.1 The Supplier represents and undertakes that it supports all the requirements contained in the PCI Standards.

2.2 Throughout the term of the Agreement the Supplier shall ensure that its relevant subcontractors shall comply with all the requirements contained in the PCI Standards in the performance of its obligations under this Agreement.

3. REPORTING AND MONITORING

3.1 The Supplier shall provide to Post Office evidence of its compliance with the PCI Standards on an annual basis.

3.2 The Supplier will ensure that the relevant Subcontractors attest their compliance with the PCI standards and evidence it, at least annually, including, where relevant (as a minimum), the following:

3.2.1 completion of a self-assessment questionnaire by the subcontractor covering its compliance with the PCI Standards;

3.2.2 an on-site audit of the subcontractor's compliance with the PCI Standards carried out by the Supplier's personnel or agents;

3.2.3 the development of a documented action plan with each subcontractor detailing improvement actions required, and the subsequent implementation of that plan; and

3.2.4 if Post Office so requires, an independent audit of the subcontractor by a recognised and qualified organisation covering the subcontractor's compliance with the PCI Standards. Where that subcontractor already holds certification of its compliance

POL00393766

with the PCI Standards (from a recognised and qualified organisation), the cost of any further audit required by Post Office shall be met by Post Office.

The Supplier will provide the results of each of items (3.2.1) to (3.2.4) above to Post Office promptly following their completion.

3.3 The Supplier will ensure that all Subcontractors who process or store payment card information are in possession of the relevant PCI DSS certifications and complete and evidence the relevant security scans to the timeframes required by PCI DSS for the duration of the Agreement.

3.4 Post Office shall be entitled to audit the Supplier and its Subcontractors' compliance with its obligations under this Schedule in accordance with clause 29.

4. REMEDIES FOR PCI FAILURES

4.1 The Supplier shall advise Post Office immediately on becoming aware of any PCI Failure. In such circumstances or if Post Office otherwise becomes aware of a PCI Failure, Post Office may discuss the PCI Failure with the Supplier.

4.2 The parties acknowledge the potentially serious effect of any PCI Failure and the likelihood that a PCI Failure will be a material breach. Accordingly, the Supplier and the Post Office shall use all reasonable endeavours to agree an improvement plan (including actions and timescales) to remedy any PCI Failure as soon as reasonably possible.