7) Service Provider's Key Personnel:

Name & Position	Contact Details	Area of Responsibility
Jonathan Hawkins	Direct Dial: [redacted] Mob: [redacted] Email: [redacted]	Service Provider Contract Manager
Nicholas Leadbeater	Direct Dial: [redacted] Mob: [redacted] Email: [redacted]	Service Provider Incident Manager

8) Notice period in accordance with Clause 34.7 (termination without cause):

The notice period for termination for convenience is 90 days

9) Address for service of notices in accordance with Clause 45:

For the Authority:

Transport for London, Windsor House, 42-52 Victoria Street, LONDON, SW1H 0TL
E-mail Address (where permitted): SMBCEDocumentControl@tfl.gov.uk

For the attention of: Andy Barrie

For the Service Provider:

CyberSource, Reading International Business Park, Basingstoke Road, Reading, RG2 6DH

E-mail Address (where permitted): [redacted]

For the attention of: Jonathan Hawkins

SCHEDULE 2 – OVERVIEW OF THE CONTRACT

1. Introduction

1.1. Scope and Purpose

1.1.1. This Schedule provides an introduction to and an overview of the Contract documentation and the concepts behind both its structure and the approach and language adopted within the Contract and the Schedules.

1.1.2. This overview is intended to introduce and expand on the information provided elsewhere within the Contract to ensure that the concepts and approach underlying the main provisions are easily and properly understood. It is not intended to contain specific obligations on either Party.

1.1.3. The overviews within this Schedule are intended to provide a high level picture only and should not be interpreted as being complete or comprehensive. In the event of any inconsistency or conflict between the contents of this Schedule and any other part of the Contract, that other part of the Contract shall take precedence.

1.2. Service Continuity

1.2.1. The Authority has developed a reputation for delivering a high quality, reliable and consistent service to its customers through a portfolio of contracts and systems under its control. It is essential that this continues and this overview seeks to explain how the Service Provider will operate as part of this portfolio to deliver excellent and potentially more integrated services.

1.2.2. Specific requirements covering transition from the Authority's Existing Service Providers, 'fix first and deal with responsibility later' obligations, Required Variations (whereby the Authority can instruct Variations to proceed, with the cost and other impacts to be determined afterwards) , enhanced co-operation obligations, Service management and flexible handback obligations (including the potential for the Authority to instruct phased handback and/or handback continuing over a period beyond the initial or extended contractual period) have been included to re-enforce and support the need for service continuity.

1.3. Assurance

1.3.1. The Authority has engaged the Service Provider on the basis of the Service Provider's experience, expertise and proposed solution to the delivery of the Services and other obligations under the Contract. The Authority wishes to give the Service Provider latitude to manage its operations effectively; however, the operation of the CE Systems Portfolio is critical to the Authority's business operations and consequently the Service Provider needs to demonstrate to the Authority that it is complying with the principles and specific requirements and obligations set out in the Contract. This process is called Assurance and is principally set out in Schedule 14 (Assurance).

1.3.2. Assurance is an activity performed by the Service Provider to demonstrate compliance to the Authority and includes, but is not limited to, the submission of documents, responding to questions and comments, and

witness testing. Assurance is frequently an incremental process that provides confidence to both parties of successful delivery. It should not, however, be confused with approval from the Authority and does not relieve the Service Provider of its responsibilities or liability under the Contract.

2. Document Architecture

2.1. Basic Contract Structure

2.1.1. The Contract is constructed from three mutually supporting elements:

2.1.1.1. **Main Terms & Conditions** – this contains the main rights and obligations of the Parties expressed in Clauses;

2.1.1.2. **Schedules** – these contain further obligations, the Service Scope Specification, Service Levels and contract processes expressed in paragraphs or in the case of the Specification and the standard forms, sections and

2.1.1.3. Supporting Documents – these are documents (if any) which are incorporated into the Contract by reference.

3. [NOT USED]

4. The Services

4.1. Overview

4.1.1. The services to be delivered by the Service Provider are set out in Clause 4 (The Services) and further defined along with the Service Levels in Schedule 8 (Service Management).

4.1.2. The Service Levels and requirements set out in Schedule 4 (Service Scope Specification) and Schedule 8 (Service Management) have been developed from the following key metrics which underpin the Authority approach to Service management:

4.1.2.1. **Event Management** - where possible all parts of the Contract System, Service metrics and deliverables will be proactively monitored. This could be by the Authority's CE operational support system or by the Service Provider's equivalent monitoring system to provide a central command and control function across all service suppliers in the CE Systems Portfolio;

4.1.2.2. **High Availability** - the Contract System, particularly the customer touch-points must be fully functional and available for use during relevant operating hours. This should be enabled through high, but achievable performance regimes combining reliability, resilience, proactive fault identification and resolution;

4.1.2.3. **Data Completeness** - it is essential to revenue security and a quality customer experience that no Data is lost. Accordingly all Data is to be properly captured and transmitted using robust and resilient processes and protocols; and

4.1.2.4. **Low Latency** - delayed Data transmission adversely affects the customer experience and could lead to revenue loss and Data must be transmitted with the minimum of delay both to and from the customer touch-points.

4.2. Service Management

4.2.1. In order to standardise its approach, the Authority has chosen to adopt elements of the Information Technology Infrastructure Library (ITIL) into its operations and this is reflected in the Contract.

4.2.2. Specific requirements on service management, service design, service transition, service operations, incident management and change management are described in Schedule 3 (Transition) and Schedule 8 (Service Management).

SCHEDULE 3 - TRANSITION

1. Introduction

1.1. Purpose

1.1.1. The purpose of this Schedule 3 (Transition) is to set out the Service Provider's obligations in relation to Transition and in particular:

1.1.1.1. the preparations by the Service Provider to take over responsibility for the delivery of the Services;

1.1.1.2. Assurance to be provided by the Service Provider to the Authority that the Service Provider is ready for each phase or stage of Transition and delivery of the Services;

1.1.1.3. the carrying out of a smooth transition of Existing Services (so far as relevant to the Services) to the Service Provider;

1.1.1.4. the preparation, definition and then delivery of the change activities required to successfully transition the Services; and

1.1.1.5. the carrying out of the necessary activities to ensure that the system integrator responsibilities are supported or delivered by the Service Provider.

1.2. Authority Objectives

1.2.1. The objectives of this Schedule 3 (Transition) are to:

1.2.1.1. achieve a smooth handover of responsibility from the Existing Service Provider to the Service Provider on and/or following the Service Commencement Date;

1.2.1.2. ensure that there is no adverse impact on customers during Transition;

1.2.1.3. minimise any disruption to the Authority during Transition;

1.2.1.4. ensure that there is no degradation to the Services during Transition and all transferred Services are delivered by the Service Provider pursuant to the Service Levels from the respective date of transfer of such Services;

1.2.1.5. minimise the costs of Transition (although for the avoidance of doubt, the Charges already include and provide for the Service Provider's costs in respect of Transition, except where and to the extent that the right to any additional payment is explicitly provided in the Contract;

1.2.1.6. ensure timely development and agreement of Transition Plans and the Service Provider's compliance with those plans;

1.2.1.7. ensure that effective business controls are implemented by the Service Provider to manage risks during Transition;

1.2.1.8. ensure that Transition activities are effectively monitored and reported;

1.2.1.9. ensure effective communications between all parties involved in Transition activities; and

1.2.1.10. ensure that the Authority is fully aware of the Service Provider's Transition approach and activities at all times throughout the Transition Period.

1.3. Overview of this schedule

1.3.1. This Schedule sets out:

1.3.1.1. the Transition Phases, Transition Plans and Transition Milestones in paragraph 2;

1.3.1.2. the obligations and responsibilities of the Service Provider relating to Transition during:

1.3.1.2.1.1. the Pre-Transition Phase in paragraph 3;

1.3.1.2.1.2. the Transition Phase in paragraph 4; and

1.3.1.2.1.3. the Post-Transition Phase in paragraph 5;

1.3.1.3. the requirements for managing and governing the Transition activities in paragraph 6 and Appendix 1 (High-Level Governance Structure) to this Schedule;

1.3.1.4. the Service Provider's High-Level Transition Plan in Appendix 2 (High-Level Transition Plan) to this Schedule; and

1.3.1.5. the Authority Transition Dependencies and Existing Service Provider Transition Dependencies relating to Transition in paragraph 7.2 (Transition Dependencies) of this Schedule.

2. Transition Phases, Plans and Milestones

2.1. The Transition Phases

2.1.1. Transition comprises of three phases:

2.1.1.1. the period from (and including) the Contract Commencement Date to (but excluding) the date of transfer of any part of the Services at the Service Commencement Date (the "**Pre-Transition Phase**");

2.1.1.2 the period from (and including) the Service Commencement Date to (and including) the date of completion of the transfer of all of the Services from the Existing Service Provider to the Service Provider at the actual achievement of the Transition Milestone Criteria for the Final Service Transition Milestone (the "**Transition Phase**"), and

2.1.1.3. the period following the achievement of the Transition Milestone Criteria for the Final Service Transition Milestone until any and all outstanding issues relating to Transition have been resolved and/or completed to the Authority's reasonable satisfaction (the "**Post-Transition Phase**").

2.1.2. [NOT USED]

2.2. The Transition Plans

2.2.1. The Transition Plans consist of the:

2.2.1.1. High-Level Transition Plan attached in Appendix 2 (High-Level Transition Plan); and

2.2.1.2. Detailed Transition Plan to be developed by the Service Provider in accordance with the provisions of this Schedule and consistent with the High-Level Transition Plan.

2.2.2. The Service Provider shall ensure that all Transition Plans contain all the deliverables required under the Contract to meet the Transition Milestone Criteria including but not limited to those set out in Appendix 3 (Milestone Criteria).

2.3. Assurance Events and Transition Milestones

2.3.1. The Assurance Events and Transition Milestones are set out in the High-Level Transition Plan in Appendix 2 and include:

2.3.1.1. a series of Assurance Events to Assure the Authority that preparations are on track culminating in a Transition Milestone for the Service Provider to take over responsibility for the Services or a particular part of the Services;

2.3.1.2. the Transition Milestones and associated Transition Milestone Dates that include:

2.3.1.2.1. the Service Commencement Date when the initial set of the Services and/or responsibility for all Services shall transfer to the Service Provider;

2.3.1.2.2. if applicable, the Interim Service Transition Milestones when subsequent sets of Services shall transfer to the Service Provider;

2.3.1.2.3 the Final Service Transition Milestone at which point the Service Provider shall deliver all of the Services; and

2.3.1.2.4. other Transition Milestones as set out in the High-Level Transition Plan and/or the Detailed Transition Plan.

2.4. Milestone achievement process

2.4.1. Not less than twenty-eight (28) days prior to the Transition Milestone Date for each Transition Milestone the Service Provider shall submit a Transition Milestone Completion Plan to the Authority that shall include:

2.4.1.1. details of the proposed programme for meeting the Transition Milestone Criteria for the Transition Milestone by the relevant Transition Milestone Date;

2.4.1.2. details of all extensions of time arising from Authority Events requested or agreed or determined in accordance with Clause 50 (Authority Event) of the Contract and any consequent changes to the Transition Milestone Date;

2.4.1.3. details of all aspects of the Transition Milestone Criteria already achieved in whole or in part prior to the Transition Milestone Date and achievement of such criteria; and

2.4.1.4. a timetable for achieving all outstanding aspects of the Transition Milestone Criteria,

and the Service Provider shall subsequently provide the Authority with satisfactory evidence of delivery of such outstanding aspects of the Transition

Milestone Criteria in all cases within two (2) Business Days of such delivery or achievement, as applicable.

2.4.2. The Service Provider shall provide the evidence of achievement of the Transition Milestone Criteria in accordance with the timetable provided to the Authority pursuant to paragraph 2.4.1 above and shall submit an application in writing to the Authority for a Compliance Certificate for each Transition Milestone on the date from which the Service Provider believes that it is entitled to that Compliance Certificate, provided that in relation to each Transition Milestone not more than one application for a Compliance Certificate may be submitted to the Authority and be outstanding at any one time.

2.4.3. The Service Provider shall provide such additional information and assistance as the Authority and any nominee may reasonably require to satisfy the Authority that the Service Provider has achieved the Transition Milestone Criteria. Within ten (10) Business Days of the provision of all such information and assistance, the Authority shall in its absolute discretion issue either:

2.4.3.1. a **Compliance Certificate** dated as of the date the Transition Milestone Criteria were achieved by the Service Provider, which shall confirm that the Service Provider has achieved the Transition Milestone Criteria and that it is entitled to the Charges associated with that Transition Milestone from the date of the Compliance Certificate;

2.4.3.2. a **Qualified Compliance Certificate** dated as of the date the Authority considers sufficient Transition Milestone Criteria were achieved and which confirms that the Service Provider is provisionally entitled to the Charges associated with that Transition Milestone from the date of the Qualified Compliance Certificate, but that there are other outstanding criteria which the Service Provider must still achieve in order to retain such payments pursuant to paragraph 2.4.17.3.2; or

2.4.3.3. a **Non-Compliance Certificate** dated as of the date the Service Provider stated in its application that it believed it was entitled to the Compliance Certificate, which shall state that the Service Provider has not fully achieved the Transition Milestone Criteria for the applicable Transition Milestone and that it is not entitled to the Charges associated with that Transition Milestone or any part of such payments.

The Authority's entitlement to exercise its discretion under this paragraph shall not be limited or otherwise impaired due to a Compliance Certificate having been issued in relation to a different Transition Milestone.

Dispute Procedure

2.4.4. Where the Service Provider disputes the issue of a Qualified Compliance Certificate or a Non-Compliance Certificate, it may refer the matter for resolution to the Transition Governance Group and/or the Service Provider may refer the matter for resolution in accordance with Clause 33 (Dispute Resolution).

Non-Compliance Certificate

2.4.5. The Authority shall only be entitled to issue a Non-Compliance Certificate in circumstances where the Service Provider has failed to complete the Transition Milestone Criteria for the Transition Milestone and/or a Non-Compliance Certificate is issued after the Consultation Period in accordance with paragraph 2.4.16.2.

2.4.6. Where the Authority issues a Non-Compliance Certificate, it shall include on the certificate specific reasons for the Service Provider's failure to obtain a Compliance Certificate which the Service Provider must address to obtain a Compliance Certificate.

2.4.7. As soon as reasonably practicable after the receipt of a Non-Compliance Certificate and in any event within ten (10) Business Days, the Service Provider shall provide the Authority with full details of a revised programme for remedying as soon as possible its failure to satisfy the Transition Milestone Criteria together with a new date by which the failure to satisfy such Transition Milestone Criteria shall be remedied and the terms of any Corrective Action Notice(s) shall be complied with.

2.4.8. Subject to paragraph 2.4.9, the Service Provider shall carry out the actions in the revised programme referred to in paragraph 2.4.7 by the new date and the Authority and the Service Provider shall comply with this paragraph 2.4 accordingly in relation thereto.

2.4.9. The Authority may, at its discretion, reject a revised programme and/or new Transition Milestone Date submitted in accordance with paragraph 2.4.7, whereupon the Service Provider shall resubmit a further revised programme and/or new Transition Milestone Date in accordance with paragraph 2.4.7 and paragraph 2.4.8 and this paragraph 2.4.9 shall then apply.

Qualified Compliance Certificate

2.4.10. Where the Authority issues a Qualified Compliance Certificate, it shall include on the certificate specific reasons for the Service Provider's failure to obtain a Compliance Certificate which the Service Provider must address to obtain a Compliance Certificate.

2.4.11. Following the issue of a Qualified Compliance Certificate, the Service Provider shall provide the Authority with all information and assistance as the Authority may reasonably require to confirm that the outstanding Transition Milestone Criteria and Corrective Action Notice(s) (if any) have been or are being properly resolved.

2.4.12. The Service Provider shall address the reasons for failure to obtain a Compliance Certificate and, within fourteen (14) days of the issue of the Qualified Compliance Certificate (or such longer time period as the Authority may in its absolute discretion grant), shall provide the Authority with evidence to the Authority's satisfaction that each of the reasons for failure to obtain the Compliance Certificate and each issue specified in any Corrective Action Notice(s) have been fully resolved.

2.4.13. The Authority shall confirm within five (5) Business Days of the expiry of the time period granted by the Authority for the resolution of the outstanding Transition Milestone Criteria pursuant to paragraph 2.4.12

whether all such outstanding Milestone Criteria have been properly resolved within the time period.

2.4.14. If the Service Provider has resolved all outstanding Milestone Criteria to the Authority's satisfaction within the time period set out in paragraph 2.4.12, The Authority shall endorse the Qualified Compliance Certificate issued pursuant to paragraph 2.4.3.2 with the word "Compliant" and the date of such endorsement. Such Qualified Compliance Certificate shall then be deemed for all purposes to be a Compliance Certificate as if it had been issued as of the date of the Qualified Compliance Certificate.

Consultation process

2.4.15. If the Service Provider has failed to comply with all outstanding Transition Milestone Criteria and any Corrective Action Notice(s) within the time period set out in paragraph 2.4.12, the Authority, in its absolute discretion, shall either:

2.4.15.1. grant the Service Provider such additional time to satisfy the Transition Milestone Criteria as The Authority in its absolute discretion may decide, subject to such additional or amended requirements as the Authority considers in its absolute discretion to be appropriate, whereupon the Qualified Compliance Certificate issued pursuant paragraph 2.4.3.2 shall be amended by the Authority to reflect such additional time and the provisions of this paragraph 2.4 shall apply to such Qualified Compliance Certificate as if such additional time had been included in the original time period granted pursuant to paragraph 2.4.12 for resolution of the outstanding Milestone Criteria; or

2.4.15.2 notify the Service Provider in writing:

2.4.15.2.1. that it intends to issue a Non-Compliance Certificate in accordance with paragraph 2.4.16 upon the expiry of twenty eight (28) days (or such longer period as the TfL Director of Customer Experience in his absolute discretion determines in accordance with paragraph 2.4.16.2) from the date of such notification; and

2.4.15.2.2. the name of the TfL Director of Customer Experience to whom the Service Provider may make a representation in writing in relation to the intention referred to in paragraph 2.4.15.2.1 above.

2.4.16. Upon receipt of notification pursuant to paragraph 2.4.15:

2.4.16.1. the Service Provider may within fourteen (14) days (the **"Submission Period"**) submit in writing to the TfL Director of Customer Experience such details of the situation which resulted in the notification pursuant to paragraph 2.4.15.2 as it, in its absolute discretion, determines are relevant together with a proposal for resolving the situation; and

2.4.16.2. the TfL Director of Customer Experience shall make himself reasonably available to consult with a member of Service Provider Personnel during a period of fourteen (14) days from the end of the Submission Period or such longer period as the TfL Director of Customer Experience in his absolute discretion determines (the **"Consultation Period"**).

2.4.17. Without prejudice to the Authority's other rights and remedies under the Contract, upon expiry of the Consultation Period, the Authority may:

2.4.17.1. endorse the Qualified Compliance Certificate with the word "Compliant" and the date of such endorsement, whereupon such Qualified Compliance Certificate shall be deemed for all purposes to be a Compliance Certificate as if it had been issued as of the date of the Qualified Compliance Certificate;

2.4.17.2. grant such additional time to satisfy the Transition Milestone Criteria as the Authority in its absolute discretion may decide, subject to such additional or amended requirements as the Authority considers in its absolute discretion to be appropriate and the provisions of this paragraph 2.4 shall apply as if such grant of additional time had been made pursuant to paragraph 2.4.15.1; or

2.4.17.3. endorse the Qualified Compliance Certificate with the words "Non-Compliant" and the date of such endorsement, such endorsement having been countersigned by the TfL Director of Customer Experience, whereupon:

2.4.17.3.1. such Qualified Compliance Certificate shall be deemed to be a Non Compliance Certificate as if it had been dated as of the date of the Qualified Compliance Certificate and the provisions of this paragraph 2.4 shall apply accordingly and for the purposes of paragraph 2.4.7 the date of receipt of such Non-Compliance Certificate shall be the date of endorsement pursuant to this paragraph 2.4.17.3; and

2.4.17.3.2. the Service Provider shall not be entitled to the Charges associated with the Transition Milestone and within thirty (30) days of the date of such endorsement the Service Provider shall repay to the Authority all or a proportion of any such payments that the Authority in its absolute discretion shall specify at the date of such endorsement.

2.4.18. Where the Service Provider obtains a Compliance Certificate in accordance with this paragraph 2.4, the Charges associated with that Transition Milestone shall be payable to the Service Provider from the date written by the Authority on the Compliance Certificate.

2.5. Further consequences of not achieving milestones

2.5.1. Without prejudice to other provisions of the Contract, if any of the events in the following table occur, then the consequences associated with the event specified in the table shall apply.

Milestone Event	**Milestone consequences**
Subject to Clause 50 (Authority Events), the Service Provider does not achieve the Service Commencement Date within 60 days of the originally planned date (**"the SCD Long-Stop Date"**).	The Authority shall have the right to terminate the Contract in accordance with Clause 34.1.7).
Subject to Clause 50 (Authority Events), the Compliance Certificate for the Final Service Transition Milestone is not achieved prior to four (4) months of the originally	The Authority shall have the right to terminate the Contract in accordance with

planned date (**"the Transition Long-Stop Date"**).	Clause 34.1.8.

3. Pre-Transition Phase

3.1. Preparation and Assurance activities

3.1.1. To prepare for Transition and Assure the Authority that the Service Provider has prepared for Transition, the Service Provider shall:

3.1.1.1. carry out the activities defined in the Transition Plans to prepare for Transition and achieve the Transition Milestone Dates set out in the High-Level Transition Plan and/or the Detailed Transition Plan in accordance with the process set out in paragraph 2.4;

3.1.1.2. carry out detailed Transition planning in accordance with paragraph 3.2 and the High-Level Transition Plan;

3.1.1.3. demonstrate, within the proposed Transition Plans, that relevant and sequential milestones have been set that provide on-going Assurance to the Authority as to the quality and completeness of the Transition Plans and the Service Provider's delivery against such plans;

3.1.1.4. carry out contingency planning; and

3.1.1.5. meet the associated Milestone Criteria in accordance with the High-Level Transition Plan and/or the Detailed Transition Plan.

3.2. Detailed Transition planning

3.2.1. Commencing on the Contract Commencement Date the Service Provider shall carry out detailed Transition planning and the Service Provider and the Authority shall work together to agree the Detailed Transition Plan which shall define the detail of the activities and deliverables required to perform Transition and which shall reflect and expand on the High-Level Transition Plan.

3.2.2. The Service Provider shall be responsible for drafting the Detailed Transition Plan and shall submit the draft Detailed Transition Plan to TfL within twenty eight (28) days after the Contract Commencement Date, and the Authority shall, and shall use reasonable endeavours to procure that the Existing Service Provider shall, provide reasonable input in relation to the detailed Transition activities to be set out in the Detailed Transition Plan.

3.2.3. The Authority and the Service Provider shall use reasonable endeavours to agree the Detailed Transition Plan as soon as reasonably practicable following submission of the draft Detailed Transition Plan to the Authority pursuant to paragraph 3.2.2 and in any event within twenty eight (28) days of the submission, or such later date as the Parties shall agree in writing.

3.2.4. If the Parties do not agree the Detailed Transition Plan within the time periods set out in paragraph 3.2.3 above, the matter shall be treated as a Dispute and resolved in accordance with paragraph 6 (Transition Governance and Management) and Clause 33 (Dispute Resolution)

3.2.5. Without prejudice to other provisions of the Contract, the Detailed Transition Plan shall be consistent with the High-Level Transition Plan and shall include, at a minimum:

3.2.5.1. detail that is deemed sufficient by the Authority in relation to each of the Transition Milestones, activities, deliverables, criteria and other items covered under the High-Level Transition Plan and the Service Provider shall ensure that additional detail is included in the Detailed Transition Plan in relation to any of the aforementioned at the Authority's reasonable request;

3.2.5.2. the detailed allocation of responsibilities between the Service Provider and any sub-contractors-, and any instances where cooperation of the Authority and/or of the Existing Service Provider is required;

3.2.5.3. detailed and clear dependencies on the Authority and the Existing Service Provider in relation to each Transition Milestone or Transition Milestone Criteria provided that unless otherwise agreed by the Authority in writing, such dependencies shall not be more extensive than the Transition Dependencies;

3.2.5.4. detailed safeguards to minimise disruption to the Authority's business, customers and/or the Authority's relationship with Third Parties; and

3.2.5.5. clear analysis of Transition risks and justifications for the implementation approaches taken in the Detailed Transition Plan.

3.2.6. Once the Detailed Transition Plan has been agreed by both Parties pursuant to paragraph 3.2.3, the Service Provider shall comply with and implement such Detailed Transition Plan. Any changes to the agreed version of the Detailed Transition Plan shall be subject to the Authority's prior written consent, such consent not to be unreasonably withheld or delayed.

3.2.7. The Service Provider shall take part in joint planning activities with the Existing Service Provider and the Authority in accordance with the High-Level Transition Plan.

4. Transition Phase

4.1. Transition principles

4.1.1. The Service Provider shall deliver Transition in accordance with the Transition Plans.

4.1.2. Without prejudice to other provisions of the Contract, the Service Provider shall co-operate with the Existing Service Provider in an effective and timely manner to deliver Transition.

4.1.3. The Service Provider shall ensure that Transition does not rely on any periods of unavailability or degradation of the Services and/or Existing Services.

4.1.4. The Service Provider shall carry out its Transition activities in such a way that:

4.1.4.1. the Transition activities do not adversely affect the Existing Services and/or Services being delivered;

4.1.4.2. the Transition activities do not impact the Service Levels throughout Transition, and

4.1.4.3. The Authority and the Existing Service Provider are kept informed of Transition progress and status of Transition.

4.1.5. The Service Provider shall only Transition and operate any part(s) of the Services from the Transition Milestone Date for those part(s) of the Services and only after the Service Provider has received a Compliance Certificate or Qualified Compliance Certificate with respect to those part(s) of the Services.

4.1.6. The Service Provider acknowledges and agrees that continuity of the Existing Services and the Services (as applicable) is of paramount importance to the Authority and the Service Provider shall not compromise the continuity of such services in its Transition Plans or activities.

4.1.7. The Service Provider shall manage data security in accordance with industry principles and best practice. The Service Provider shall manage health, safety, quality and the environment in accordance with Schedule 12 (Quality, Environment, Safety and Health).

4.1.8. The Service Provider shall carry out training in accordance with Schedule 5 (Training) and the Transition Plans, and shall carry out any training as is reasonably required for the efficient Transition of the Services.

4.1.9. The Service Provider shall notify the Authority in writing if any Key Personnel become unavailable (due to any period of paid or unpaid leave, illness or otherwise) for more than two (2) weeks during the Transition Period. Where such notification is made then the replacement of Key Personnel should be made in accordance with Clause 15.1.4 (Key Personnel).

4.2. Transition of Services

4.2.1. [NOT USED]

5. Post-Transition Phase

5.1.1. [NOT USED]

5.1.2. [NOT USED]

6. Transition Governance and Management

6.1. Transition management and reporting

6.1.1. The Service Provider shall manage and report on Transition.

6.1.2. The purpose of the Transition Governance Group is to review progress of Transition and address any matters relating to Transition. The Transition Governance Group shall meet each month or on such other more frequent basis as required by the Authority. The Parties agree that in the lead-up to the Transition Milestones such meetings will be held every week and/or as required by the Authority.

6.1.3. The Authority shall prepare the meeting agenda and the TfL Transition Manager shall chair the meeting. At the end of each meeting there shall be an agreed set of actions which the Authority shall circulate within one (1)

Business Day and, where necessary, the Authority shall subsequently produce formal minutes of the relevant Transition Governance Group meeting which shall be circulated within three (3) Business Days of each meeting.

6.1.4. Without limiting the earlier provisions in this paragraph 1, the following table summarises the required arrangements in respect of Transition Governance Group meetings.

ATTENDEES		
Authority	**Service Provider**	**Third Parties**
TfL Transition Manager TfL Service Operations Manager	Transition Project Manager Service Operations Manager	Existing Service Provider: Nominated representative responsible for handback Nominated representative responsible for service operation

FREQUENCY AND LOCATION
Once each month, or on such other more frequent basis as required by the Authority, in London at a location determined by Authority. In the lead-up to Service Transition Milestones these meetings will be held as a minimum every week.

TRANSITION MANAGEMENT ROLE	
Review of last meeting	• The Parties shall review and approve the previous Transition Governance Group meeting minutes and action log (if applicable). • Authority shall notify the Service Provider if it deems any outstanding actions in the action log to be closed (otherwise, such actions shall remain open until closed by Authority and notified to the Service Provider in writing).
General	The objectives of the Transition Governance Group meetings are to: • review and update the risk register for Transition; • review the Programme Report for Transition; • review progress against the Transition Plans; • review and resolve Transition issues, conflicts and discrepancies; • review upcoming Transition activities and opportunities; • ensure good team/Service Provider relationship with

	clarity of roles, responsibility and communications; and • ensure that Services are being Transitioned and delivered to achieve the required outcomes for users.

INPUTS AND OUTPUTS	
Required Inputs	• a risk register for Transition; • Programme Report for Transition; • Transition Plans; • Discrepancies; and • escalated Transition issues.
Required Outputs	• meeting actions; • meeting minutes where necessary, and • updated project risk register for Transition.

7. Transition Dependencies

7.1. General

7.1.1. Any failure by the Authority and/or the Existing Service Provider (as the case may be) to meet a Transition Dependency shall be dealt with pursuant to Clause 50 (Authority Event).

7.2. Transition Dependencies

[NOT USED]

7.3. Existing Service Provider Transition Dependencies

Appendix 1 – High-level Governance Structure

[NOT USED]

Appendix 2 – High-Level Transition Plan

[NOT USED]

Appendix 3 – Milestone Criteria

[NOT USED]

SCHEDULE 4 – SERVICE SCOPE SPECIFICATION

1. Introduction

1.1. This Schedule outlines the Service Scope Specification of the Contract

1.2. The scope of work includes, but is not limited to:

1.2.1. Payment processing and transaction services, fraud management, managed Service (Support), tokenisation, system reporting, audit service, general requirements and documentation.

2. Payment Processing and Transaction Services

2.1. The Authority shall use the Contract System to process payment card authorisations, payment card refunds and payment card settlements as described below and as detailed in the Schedule 8.

2.2. The Contract System shall:

2.2.1. request either a zero value or positive value authorisation from the payment card issuing bank;

2.2.2. request a settlement against a previously authorised amount;

2.2.3. provide an Authorised User with functionality to manually reverse an approved authorisation;

2.2.4. provide an Authorised User with functionality to record a chargeback against a payment transaction;

2.2.5. be compatible with all major merchant acquirers as listed on the UK Card Association's website at the following link: www.theukcardsassociation.org.uk/retailer_resources/index.asp;

2.2.6. provide an interface which allows the Sales Website to automatically reverse an approved authorisation;

2.2.7. process a refund to a specified payment card, via a dedicated Merchant ID (MID);

2.2.8. when processing a refund, limit the refund to no more than the original settlement value;

2.2.9. support recurring payments from a pre-registered payment card; including payments for which the date and frequency of the recurring payment will be ad-hoc and not on a set date;

2.2.10. accept payments from all major payment card schemes, including but not limited to Visa, MasterCard, Delta, Maestro, JCB and American Express with potential to add more schemes as necessary;

2.2.11. The Contract System shall be able to accept payments from online payment systems and digital wallets;

2.2.12. support payments made from a mobile device by integrating the Contract System into a native mobile application;

2.2.13. support payments made from a mobile device through a responsive website.

2.2.14. support payments across a range of currencies, including but not limited to payments made in Sterling, US Dollars & Euros;

2.2.15. support batch processing of ad-hoc refunds to payment cards;

2.2.16. be fully compliant with PCI DSS and all published card scheme rules and mandates and co-operate with the Authority to implement any future scheme rules and mandates.

3. Fraud management

3.1. The Contract System shall:

3.1.1. support the creation of customisable payment profiles which group together a set of pre-defined fraud screening business rules by an Authorised Admin User;

3.1.2. be able to automatically trigger a specified payment profile depending upon the information passed to it by the Sales Website;

3.1.3 support the creation of a set of standard fraud screening business rules which can be applied to all or selected payment profiles;

3.1.4. support the creation of definable fraud screening business rules which can be applied to individual payment profiles by an Authorised Admin User;

3.1.5. provide a graphical user interface to enable an Authorised Admin User to create fraud screening business rules with little or no knowledge of programming languages;

3.1.6. be able to publish fraud screening rules into a live environment immediately without intervention or approval from the Service Provider;

3.1.7. allow an Authorised Admin User to publish fraud screening rules in a 'passive' state to allow the Authority to monitor how the rules would behave when applied to live payment transactions. Rules in this state must be applied to live payment transactions from the Sales Website but must not affect the outcome of the transaction. The outcome must be logged and the Authority must be able to report on how the rule would affect payment transactions if it were to be published in a 'live' state;

3.1.8. support the Address Verification Service (AVS) and allow the Authority to use the result of the AVS check when determining whether to accept or reject a payment card transaction;

3.1.9. support the International AVS and allow the Authority to use the result of the AVS check when determining whether to accept or reject a payment card transaction;

3.1.10. support credit card validation number checks and allow the Authority to use the result of the check when determining whether to accept or reject a payment card transaction;

3.1.11. check and identify End-User IP address location and allow the Authority to use the result of this check when determining whether to accept or reject a payment card transaction.

3.1.12. support payer enrolment and authentication for card scheme specific validation (3D secure) including Verified by Visa, MasterCard SecureCode and American Express SafeKey and any future 3D secure service as and when they are launched;

3.1.13. identify the specific configuration of the device used by an End-User to submit each payment card transaction (commonly referred to as the device fingerprint) and must allow the Authority to use the device fingerprint, when determining, whether to accept or reject a payment card transaction;

3.1.14. analyse each payment transaction and assign it a score based on the risk of the transaction being fraudulent. To determine the score, the supplier must factor in all known information about the End-User (e.g. device fingerprint, IP address, payment velocity) from the current and previous transactions both from the Sales Website and the Service Provider's other merchants;

3.1.15. allow the merchant to set a score threshold for each payment profile. If a transaction exceeds its assigned score threshold, the system must reject the payment;

3.1.16. allow new fraud screening business rules to be retrospectively applied to the Authority's historical payment transactions and inform an Authorised User how the new rule would have affected the outcome of historical transactions if the rule was in place at the time the transaction was processed;

3.1.17. support positive and negative lists and allow the placing of, and checking against, End-User specific information against those lists;

3.1.18. where a piece of information (e.g. an email address) has been placed on one of these lists, it shall always either accept (positive list) or reject (negative list) future payment card transactions, irrespective of whether other rules are met or not. Where a piece of information is on both lists, the positive list must take precedence;

3.1.19. automatically add any pre-defined associated pieces of information to the negative list, where a transaction has been rejected because a specific End-User piece of information is on the negative list;

3.1.20. allow Authorised Admin User to;

3.1.20.1.1. add Customer specific information (e.g. an email address or account number) to the positive or negative lists manually;

3.1.20.1.2. remove customer specific information (e.g. an email address or account number) from the positive or negative lists manually;

3.1.20.1.3. add a trusted customer to the positive list and have them removed automatically at a specified future date and time;

3.1.20.1.4. add or remove details from the positive or negative lists by uploading a file (e.g. CSV) containing the details to be added or removed;

3.1.21. support a manual screening workflow where payment transactions, based on predetermined business rules, are added to queues for manual review by an Authorised User;

3.1.22. allow an Authorised User to approve or reject transactions within the manual screening workflow and must allow approved transactions to progress through to settlement;

3.1.23. provide a review service to the Authority to manually review transactions which have triggered specified thresholds;

3.1.24. route payment transactions to different manual screening workflow queues depending upon the Authority's specified criteria;

3.1.25. allow an Authorised User to sort manual screening workflow transactions into a priority order based on any of the transaction attributes;

3.1.26. allow an Authorised User to add notes to a transaction within the manual screening workflow;

3.1.27. record an audit of each manual change made within the system by Authorised and Authority Users;

3.1.28. support custom information fields passed to it by the Sales Website (e.g. Oyster card number, order number, first issue card flag) and support a minimum of 100 custom fields, which must be available for use when creating new fraud screening rules;

3.1.29. allow an Authorised Users to search for payment transactions using custom fields;

3.1.30. provide address confirmation checking using third parties such as 192.com;

3.1.31. confirm that the billing address supplied by an End-User corresponds to an authentic address location (e.g. by looking up the address on a digital mapping service),

4. Managed Service (Support)

4.1. The Service Provider shall provide a managed service and as part of this shall:

4.1.1. actively monitor and analyse the Authority's and its other merchants payment transactions;

4.1.2. each month, proactively advise and suggest ways the Authority could use the Service Provider's fraud screening system to minimise payment card fraud;

4.1.3. provide the Authority with a quarterly report which summarises fraudulent transaction trends both for the Authority's transactions and for transactions across the Service Provider's other merchants and suggest ways in which the Authority could update its systems to mitigate each identified trend;

4.1.4. set up and manage fraud screening rules within the Service Provider's fraud screening system by working closely with The Authority to

propose, implement, test and Assure each change to the fraud screening rules;

4.1.5. implement fraud screening rule changes, which have been agreed between both Parties within two (2) Business Days of the requirements being agreed;

4.1.6. maintain a record of all agreed changes to the fraud screening rules carried out by the Service Provider.

5. Tokenisation

5.1. The Service Provider shall provide a tokenisation service to securely substitute a payment card's Primary Account Number (PAN) with a unique identifier (token) whilst maintaining a link between the token and the original PAN.

5.2. The Service Provider shall provide a web-based facility to securely capture payment card details during online sales transactions.

5.3. The tokenisation service shall:

5.3.1. integrate into the existing payment flows and must ensure payment card details (specifically the PAN, expiry date and CVV) can be submitted for tokenisation directly to the Service Provider without those details passing through the Sales Website;

5.3.2. be designed to work effectively on the three main screen categories - desktop, tablet and mobile;

5.3.3. allow the Authority to customise the fonts, colours and design of any customer-facing web interface provided.

5.4. The Service Provider shall provide a facility to capture payment card details for tokenisation via an iFrame interface.

5.5. The Contract System shall;

5.5.1. return a unique token for each submitted PAN and expiry date, even if the same PAN and expiry date has been previously tokenised;

5.5.2. submit the same or an additional billing address at the point a token is submitted for authorisation;

5.5.3. accept a previously generated token for an authorisation request and substitute the token with the associated payment card details at the point the request is sent to the Authority's merchant acquirer;

5.5.4. accept a unique identifier (in place of PAN & expiry date) for a tokenised transaction when a settlement request is submitted;

5.5.5. support recurring payments from a previously generated token;

5.5.6. provide the Authority with the following information once a token has been generated;

5.5.6.1.1. Token ID

5.5.6.1.2. Last 4 digits of the payment card

5.5.6.1.3. Expiry date of payment card

5.5.6.1.4. Payment card type (e.g. Visa or MasterCard);

5.5.7. support a minimum of 20 concurrent transactions during normal operation and a minimum of 100 concurrent transactions during data migration periods;

5.5.8. process refunds to tokenised payment cards;

5.5.9. support the major card updating services;

5 5.10. retain tokens until the Authority requests for the tokens to be deleted;

5.5.11. be able to generate a token against a specific Authority merchant ID and be able to accept this token for authorisation and settlement against any other of the Authority's merchant IDs.

5.6. In the event that the Authority moves to a new tokenisation service provider in the future, the Service Provider shall;

5.6.1. provide a secure API to enable the Authority to export the tokens and their associated data fields (e.g. PAN, billing address etc.) to the new service provider.

6. Additional Services

6.1. The Service Provider shall provide consultancy and ad-hoc training over and above the managed service to the Authority as and when needed, subject to the agreement of a Variation, chargeable at the rate(s) specified in Schedule 7.

7. Reporting requirements

7.1. The Service Provider shall provide to the Authority, at no additional cost to the Authority, such reports on the provision of the Services as the Authority may reasonably request, including details of all transactions, sales, successful settlements, failures, fraud results, etc.

7.2. The Service Provider shall provide an Invoice Report to the Authority which shall:

7.2.1. summarise the transactions that appear on the Service Provider's invoice for each of the Authority's Merchant IDs;

7.2.2. summarise the transactions that appear on the Service Provider's invoice based on the types of Charges as detailed in Schedule 7;

7.2.3. be provided in the Excel and PDF format;

7.2.4. be provided to the Authority no later than five (5) business days after the end of each month

7.3. The Contract System shall;

7.3.1. allow Authorised Users to create and configure new reports directly within the Contract System;

7.3.2. allow Authorised Users to obtain reports from one day to the sixth previous months and at one day increments, in-between in XML or CVS formats, allowing for data mining and bespoke report creation ;

7.3.3. allow Authorised Users to export reports in a variety of formats including on-screen, CSV, Excel and PDF;

7.3.4. provide a data feed to allow the Authority's reporting software to access and download the Authority's transactional information directly from the Contract System;

7.3.5. provide an interface to allow the Authority to extract the Authority's transactional data held within the Contract System.

7.4. The Service Provider shall set up detailed reports within the Contract System and make the reports available for download by Authorised Users. Unless otherwise agreed, all reports shall be available to view or download in at least one of the following formats where applicable: PDF, XML, CSV and Excel formats. The reports to be provided shall include but shall not be limited to the following:

7.4.1. Invoice Summary Report

This report shall provide a summary of the Services to be invoiced and as a minimum showing:

- the transaction costs per card scheme;
- the supports costs per card scheme; and
- any other relevant costs.

This report shall be provided per month.

7.4.2. Payment Submission Detail Report

This report shall show transaction details, values and currency for all payment transactions and as a minimum shall include:

- credit/debit card transactions;
- electronic check transactions;
- bank transfer transactions;
- recurring payment transactions; and
- any other payment types the Authority may use in the future.

This report shall be provided per day.

7.4.3. Payment Batch Summary Report

This report shall show transaction details, values and currency of batched payment transactions screened by the fraud management tool and as a minimum shall include:

- credit/debit card transactions;
- recurring payment transactions; and
- any other payment types the Authority may use in the future.

This report shall be provided per day.

7.4.4. Payment Transaction Analysis Report

This report shall provide an analysis of payment transactions and as a minimum shall include:

- the breakdown of the transaction amount, transaction count and percentages against AVS values; and

- the breakdown of the transaction amount, transaction count and percentages against reply messages from payment processors

This report shall be provided per week and per month.

7.4.5. Risk Score Distribution Report

This report shall detail the distribution of risk scores for all payment transactions and as a minimum shall include:

- the score distribution against transaction counts; and
- the score distribution against percentage of total transactions

This report shall be provided per day, per week and per month.

7.4.6. Transaction Detail Report

This report shall detail the complete information available for each payment transaction and as a minimum shall include:

- cardholders' account information including: name, address, email and IP address;
- payment transaction details including: amount, date of transaction, merchant ID, authentication results and transaction type;
- transaction processing status; and
- fraud screening results.

This report shall be provided per day.

7.4.7. Transaction Exception Detail Report

This report shall identify payment transactions that have been flagged by the Service Provider or by the payment processor/merchant acquirer, either because of errors in requests for follow-on transactions or payment incidents that occur after a transaction is sent to the payment processor/merchant acquirer. As a minimum, it shall include:

- error or incident details associated with the payment;
- payment transaction details including: amount, date of transaction, merchant ID and transaction type.

This report shall be provided per day.

7.4.8. Fraud Management Detail Report

This report shall provide the complete information of each payment transaction screened by the fraud management tool. As a minimum, it shall include:

- cardholders' account information including: name, address, email and IP address;
- payment transaction details including: amount, date of transaction, order channel, transaction type and card issuer; and
- fraud screening profiles, rules and results.

This report shall be provided per day and per week.

7.4.9. Payer Authentication Detail Report

This report shall detail the status of the payer authentication process for payment transactions, as a minimum it shall:

- categorise the payment transactions by the following statuses: 'successful', 'attempted' and 'incomplete' authentication; and
- report against each type of card and currency.

This report shall be provided per day, per week and per month.

7.4.10. Conversion Detail Report (for management review purposes)

This report shall show the results of converted orders allocated to each Authorised User and their decisions. It shall provide an overview of all orders that were not immediately 'accepted' (i.e. orders initially marked for 'review' or 'rejected'). As a minimum, it shall include:

- status of each order before and after review;
- name of Authorised User;
- queue assignment;
- order details; and
- Authorised User's comments and notes.

This report shall be provided per day.

8. Audit Services

8.1. The Service Provider shall provide as part of the Services reports that show;

8.1.1. changes made to transactions, by who and when they occurred;

8.1.2. changes made to the fraud profiles, including by who and when;;

8.1.3. permissions related to Authorised User accounts, including an Authorised User's recent log in, and what permissions they have, or provide tools or information that allow this information to be captured.

9. General Requirements

9.1. The Service Provider shall provide a test environment to the Authority to allow up to 20 concurrent Authorised Admin Users to trial new actions without affecting the live system. The testing environment must contain a real time copy of the same data used within the production environment.

9.2. The Contract System shall;

9.2.1. allow Authorised Users to search for and view transactions within the Contract System. As a minimum, Authorised Users must be able to search using email address, merchant reference ID, truncated PAN, full PAN, name, Service Provider reference number and any custom field provided by the Sales Website (e.g. account number or Oyster card number).

9.2.2. provide a visual representation of all entities linked to a particular payment card transaction (e.g. other Authority online accounts linked to the same payment card, other email addresses linked to the same payment card, previous transactions made using the same payment card and other payment cards with the same PAN);

9.2.3. when viewing a transaction by a Customer, provide Authorised Users alternative views of transactions made by the same Customer. As a minimum, provide alternative views based on transactions with the same payment card, account number and email address of the Customer;

9.2.4. provide help links as additional first line support on all web pages for Authorised Authority Users to use;

9.2.5. comply with the Authority's accessibility standards by supporting or progressing toward the support of W3C's WCAG 2.0 Guidelines Level A or above for all graphical user interfaces provided by the Service Provider.

9.2.6. provide a secure batch facility for the processing of settlement files;

9.2.7. be able to process up to 1,000,000 live and batch transactions a day.

9.3. In its provision of the Services, the Service Provider shall meet the requirements of the following recognised quality standards: ISO27001/2 and ISO9000 or similar standards.

9.4. All times reported by the Service Provider shall be GMT or BST as appropriate.

10. Authorised Admin Users

10.1. The Contract System shall allow Authorised Admin Users to;

10.1.1. keep the emergency contact details of Authority Personnel up to date;

10.1.2. create, delete and modify an Authority User's, roles & permissions;

10.1.3. assign each Authority User to a user group;

10.1.4. create, delete and modify user groups within the system;

10.1.5. apply system permissions to each user group. As a minimum, it should be possible to set the following permissions;

10.1.5.1.1. Admin (to allow full access to all functions within the system)

10.1.5.1.2. Read only (to allow users to access payment information without the ability to alter any information within the system);

10.1.5.1.3. Reporting (to allow users to download all. or selected reports from within the system);

10.1.5.1.4 Reset threshold (to allow users to reset specified fraud screening thresholds).

11. Documentation

11.1. The Service Provider must provide up to date online reference documentation for the Contract System from the Contract Commencement Date.

SCHEDULE 5 – TRAINING

1. Introduction

1.1. Scope and Purpose

1.1.1. This Schedule 5 (Training) sets out the requirements for the Service Provider to plan and conduct training of:

1.1.1.1. Service Provider Personnel for the delivery of the Services; and

1.1.1.2. Authority and Third Party trainers and/or Authority Personnel in relation to the delivery of the Services (and in this Schedule5, references to "Authority Personnel" shall include any such Authority and Third Party trainers).

1.2. Documents to be Submitted by the Contractor

1.2.1. The Contractor shall prepare, submit and maintain as appropriate the following documents in accordance with the provisions of this Schedule:

1.2.1.1. a Training Plan;

1.2.1.2. a Training Programme;

1.2.1.3. training materials.

2. Training of Personnel

2.1. General

2.1.1. The Service Provider shall be responsible for:

2.1.1.1. ensuring Service Provider Personnel are properly trained to:

2.1.1.1.1. perform their required duties; and

2.1.1.1.2. become and remain familiar with the conditions and processes within the Contract that are relevant to their role.

2.1.1.2. ensuring Authority Personnel (as the context requires) are adequately trained to deliver the Services; and

2.1.1.3. notifying the Authority in sufficient time of any training requirements which are Transition Dependencies (being training to be delivered by the Authority or any other party for whom the Authority is responsible under the Contract) to enable such training to be provided without any adverse impact on the delivery of the Service Provider's obligations under the Contract.

3. Management of Training

3.1. Training Plan

3.1.1. The Service Provider shall prepare and submit for Assurance a "**Training Plan**" which shall set out the scope, methods, means, and timing of all training for Authority Personnel.

3.1.2. The Training Plan shall include a list of equipment and applications on which training is to be given.

3.1.3. The scope of training as set out in the Training Plan shall include as a minimum:

3.1.3.1. the objectives of the training to be undertaken;

3.1.3.2. the operation of the equipment, and applications;

3.1.3.3. if applicable, the procedure for manual handling by Service Provider Personnel and, Authority Personnel, during delivery of Services;

3.1.3.4. Site safety;

3.1.3.5. the Authority Personnel (as the context requires) to be trained; and

3.1.3.6. the training documentation to be made available to Authority Personnel (as the context requires)

3.1.4. If applicable, the Training Plan shall specify the tests for the equipment and applications that need to be undertaken by Authority Personnel on completion of the training. Where equipment requires Authority Personnel to hold a licence, then details of the relevant licensing regime(s) shall be included in the Training Plan

3.1.5. The Service Provider shall, for each of the tests specified in the Training Plan pursuant to paragraph 3.1.4, propose an objective pass or fail criteria for Authority Personnel and shall maintain details of this within the Training Plan. The Service Provider's proposal shall be subject to the Authority's comments which the Service Provider shall incorporate into the relevant objective criteria

3.1.5.1. The Service Provider shall identify the methods that it will use to train Authority Personnel from both a theoretical and practical perspective.

3.1.5.2. Where applicable the Service Provider shall ensure that Authority trainers are trained and tested to the same levels of competency as the members of Service Provider Personnel providing the training.

3.1.5.3. The Training Plan shall contain an organisational statement including details of the members of Service Provider Personnel who will carry out the training, their qualifications, experience and competence.

3.1.6. The Service Provider shall set out in the Training Plan full details of the proposed training resources including:

3.1.6.1. training materials;

3.1.6.2. locations, which must always be within the UK; and

3.1.6.3. mock ups or trial installations including computer simulations.

3.2. Training Programme

3.2.1. The Training Plan shall include a "**Training Programme**" which shall set out the timing of all training.

3.2.2. The Training Programme shall be developed and provided to the Authority for Assurance.

3.2.3. The Service Provider shall ensure that all training necessary for the delivery of and/or associated with any project or programme shall be

included in the relevant project or programme Plan and show any associated dependencies on the Authority.

3.3. Review and Updating

3.3.1. The Service Provider shall submit the Training Plan and Training Programme at least 1 month prior to the Service Commencement Date. The Service Provider shall maintain the Training Plan as current and make it available to the Authority upon request.

3.4. Reports and Meetings

3.4.1. The Service Provider shall report progress on training in relation to projects and in relation to Services in the Service Performance Report in accordance with Schedule 8 (Service Management), with matters of concern to be discussed at the corresponding review meeting.

SCHEDULE 6 – SYSTEMS INTEGRATION [NOT USED]

SCHEDULE 7 – PRICING SCHEDULE

1. Introduction

1.1. This Schedule outlines the applicable Charges payable by the Authority to the Service Provider for the provision of the Services, which shall be invoiced in accordance with Clauses 10 (Charges) and 11 (Payment Procedures and Approvals).

2. Charges

2.1. The following Charges shall be applicable for the performance of the Services:

2.1.1. Payment processing, transaction services and Fraud Management

	Charge Per Transaction
Monthly Volume Tiers*	[redacted]
Payment Processing and Transaction Services	
Credit Card Transactions (Authorisation and Refunds) [1]	[redacted]
PayPal Transactions	
Credit Card Settlement	
Fraud Management	
Decision Manager Transactions (including Replay) [2]	[redacted]
Card/Payer Authentication Transactions) [3]	

[redacted]

[3] Applicable for Payer Authentication Enrolment.

2.1.2. Managed service (Support)

	Charge Per Month
Managed Service [4] [5] [6] [7]	[redacted]

[4] Performance Monitoring with Guarantees includes

- Decision Manager Service Monthly Fee
- Assigned Dedicated Risk Analyst
- Configuration Changes: rule/profile creation
- Service Level Agreement for fraud loss
- Premier Support

[5] Decision Manager Transaction fees are charged separately

[6] Customer must also purchase Decision Manager Setup & Training or Start Right as provided under separate agreement.

[7] Fees are quoted for each implementation of Decision Manager on a per CyberSource Merchant ID basis or for multiple CyberSource Merchant IDs underneath the same Decision Manager hierarchy configuration. Each additional Merchant ID requiring Managed Services will be charged at the same Monthly Fee.

2.1.3. Tokenisation

	Charge Per Token
Assisted Upload [8]	Subject to Variation
Token Storage	Free
Token Retrievals (Record Retrieval Calls) [9]	[redacted]

[8] The Authority is to enquire about a Professional Services engagement via a Variation.

[9] Charged on each retrieval transaction for extraction or purge. Please inquire about bulk Record Retrieval fees.

2.1.4. Additional Services

	One-Time / As Required	Rate Per Month
Account Management & Configuration		
Initial Registration [10]	N/A	N/A

Professional Services [11] [12]	[redacted]
Additional Gateway Login	
EBC Logins - Initial 10 Logins	
EBC Logins - Additional Logins thereafter (each)	
Decision Manager Setup & Training [13]	
Decision Manager Service Monthly Fee [14]	
Payer Authentication Setup and Compliance [15]	
Transaction Monthly Minimum [16]	
Premier Support [17]	

[10] Each Customer Affiliate will be charged a separate Initial Registration Fee.

[11] Fees and full engagement description to be detailed within a Statement of Work document.

[12] Professional Services engagement for existing customers providing consultancy and guidance on best practice integration to CyberSource Services with the addition of bespoke solution design and support.

[13] Customer must also purchase Decision Manager Setup & Training where Start Right is not purchased as provided under separate agreement.

[14] Not charged when Managed Services is taken.

Each Customer Affiliate will be charged a separate Decision Manager Service Monthly Fee.

[15] Where JEF testing is required this fee is charged per JEF testing session. Merchants are required to successfully complete the JEF testing session to CyberSource's satisfaction before using this service. Where further JEF testing sessions are required an additional Payer Authentication Setup and Compliance fee will be due for each session.

[16] In the event that Customer's transaction fees total less than the Transaction Monthly Minimum in any one month, Customer will be charged the Transaction Monthly Minimum for transactions processed during that month. Each Customer Affiliate will be charged a separate Transaction Monthly Minimum where applicable.

[17] Each Customer Affiliate will be charged a separate Ongoing Support Fee. Support Fees are included in the Managed Services fee. Support fees are charged if Managed Services are not taken.

2.1.5. Others

N/A

2.2. All prices exclude applicable taxes.

SCHEDULE 8 – SERVICE MANAGEMENT

1. Overview

1.1. Definitions and Interpretation

1.1.1. The following definitions and acronyms appear throughout this Schedule and are related to the Services requested within the Contract.

"Authority Service Operations Team"	Team of Authority Personnel whom manage the suppliers in line with contractual Service Levels;
"Availability"	a calculated measure whereby the performance of one or more devices, components, modules and parts of the Service shall be measured on the basis of their availability during the relevant Support Service Day. The proportion of the Support Service Day during which the device, module, component or element of the Services delivers its functionality, as defined in Schedule 4 (Service Scope Specification), represents its "Availability". The calculation of Availability shall exclude any Planned Maintenance Window;
"Priority 1 Major Incident"	shall have the meaning given in Appendix 3 (Major Incident Categories) of Schedule 8 (Service Management);
"Change Advisory Board"	means the committee chaired by the Change Manager and attended by the Authority Change Manager that reviews Change Requests;
"Change Management"	has the meaning set out in paragraph 7.2.1 of Schedule 8 (Service Management);
"Change Manager"	shall have the meaning given in paragraph 7.2.4 of Schedule 8 (Service Management);
"Change Request"	means a proposal to implement a Change;
"Configuration Management"	the process that identifies and records all of the configuration items that makeup the Contract System and Services and tracks their status and relationships in a Configuration Management database;
"Dashboards"	shall have the meaning given in paragraph 6.1.1 of Schedule 8 (Service Management);

"Early Life Support"	the process of support provided for a new or changed Service, for a period of time defined by the Authority, after it is released and/or deployed;
"Emergency Change"	a Change that is required immediately to either prevent or restore a service affecting outage;
"For Reporting Purposes"	Shall have the meaning given in paragraph 2.1.4 of Schedule 8 (Service Management)
"Major Incident Categories"	the categories of Major Incidents which are detailed in Appendix 3 (Major Incident Categories) of Schedule 8 (Service Management);
"Major Incident List"	shall have the meaning given in paragraph 9.3.1 of Schedule 8 (Service Management);
"Major Incident Report"	Shall have the meaning given in paragraph 9.7.1 of Schedule 8 (Service Management);
"Operational Baseline"	shall have the meaning given in paragraph 5.2 3 of Schedule 8 (Service Management);
"Planned Maintenance Schedule"	shall have mean given in paragraph 2.2.1 of Schedule 8 (Service Management);
"Planned Maintenance Window"	a pre-planned period of time, agreed in advance with the Authority in accordance with the process set out in paragraph 1.2 Planned Maintenance Window, when the Service Provider may conduct planned maintenance on the Contract System and which shall not be taken into account in the calculation of the Availability of the relevant Module;
"Preparedness Tests"	shall have the meaning given in paragraph 9.6.1 of Schedule 8 (Service Management);
"Problem Management"	the process used to determine the root cause of one or more Incidents and to develop workarounds and/or permanent fixes in order to minimise the frequency and/or impact of the Incidents;
"Problem Report"	a report issued as part of the investigation of a Problem which would include a summary of the Problem, related Incidents, root cause analysis, workaround and permanent resolutions;

"Problem Ticket"	means the ticket that has been raised in the Trouble Ticketing System for a given Problem;
"Problem"	the cause of one or more Incidents;
"Resolver Group"	the technical group assigned to resolve an Incident, Alert or event;
"Service Desk"	the technical help desk to be provided by the Service Provider in accordance with paragraph 3 of Schedule 8 (Service Management);
"Service Management"	shall have the meaning given in paragraph 1.2.1 of Schedule 8 (Service Management);
"Service Performance Report"	shall have the meaning given in paragraph 13.1.2 of Schedule 8 (Service Management);
"Support Service Day"	shall be twenty-four (24) hours per day, seven (7) days per week including all Bank Holidays and Christmas Day, unless otherwise agreed with the Authority
"Target"	Shall have the meaning given in paragraph 2.1.4 of Schedule 8 (Service Management)
"Trouble Ticketing System"	A system used to record and manage Alerts, Incidents, Problems and Changes;
"Trouble Tickets"	The tickets that are logged in the Trouble Ticketing System that represent an Incident, Alert or Problem;

1.2. Scope and Purpose

1.2.1. This Schedule sets out the scope and requirements in respect of the management, performance monitoring and reporting for the delivery of the Services. Schedule 4 (Service Scope Specification) sets out the additional specific functional and non-functional requirements.

1.2.2. The management of the Service comprises of:

1.2.2.1. provision of all Service Management and other activities set out in this Schedule;

1.2.2.2. maintaining, modifying, operating, monitoring and reporting of the Contract System to deliver its full functionality as set out in Schedule 4 (Service Scope Specification);

1.2.2.3. monitoring, reporting on and ensuring the continued integrity of the Contract System and the operation of its interfaces

1.2.2.4. managing and delivering Changes;