10.8. The Service Provider shall report on all Customer commendations received in a Period by 8:00 pm of the first Thursday of the following Period. The report shall include the following details:

10.8.1. nature of the commendation;

10.8.2. date the commendation was received;

10.8.3. name of Service Provider Personnel that handled the commendation; and

10.8.4. name and details of the person the commendation relates to.

10.9. Any suspicious applications for a replacement Oyster card shall be reported to the Authority within one (1) day of the request being made.

10.10. The Authority may request additional ad-hoc reports from the Service Provider from time to time.

10.10.1. Where an ad-hoc report request is made by the Authority before midday, the Service Provider shall, by 20:00 of that same Business Day, acknowledge such request and agree (acting in good faith) with the Authority a reasonable timeframe by when the report will be provided to the Authority.

10.10.2. Where an ad-hoc report request is made by the Authority after midday on a Business Day or is made on a day that is not a Business Day, the Service Provider shall, by 17:00 of the following Business Day, acknowledge such request and agree (acting in good faith) with the Authority a reasonable timeframe by when the report will be provided to the Authority.

11. Knowledge Sharing and Communication

11.1. The Service Provider shall ensure that Service Provider Personnel are updated on any information required to service Customer enquiries in line with processes and procedures, provided by the Authority.

11.2. The Service Provider shall provide a plan and report on how changes are to be managed and communicated to the Service Provider Personnel on a quarterly basis for the Authority to Assure.

12. Complaints

12.1. The Service Provider shall manage other types of complaints in addition to the Ticketing related complaints listed in Appendix 1 (Process Document Register).

12.2. The Service Provider can expect to receive complaints from Customers regarding but not limited to:

12.2.1. the Authority's services;

12.2.2. the Service Provider's Personnel;

12.2.3. the Authority's Personnel; and

12.2.4. Privacy and Data protection

12.3. Complaints in relation to paragraph 12.2.1 shall be transferred to the Authority's operated contact centre.

12.4. Complaints in relation to paragraph 12.2.2 shall be logged and passed on to the Service Provider's duty manager and subsequently to the Authority if the issue cannot be resolved.

12.5. Complaints in relation to paragraph 12.2.3 shall be logged and passed onto the Authority's duty manager within 24 hours.

12.6. Complaints in relation to paragraph 12.2.4 shall be logged and passed to the Authority's Privacy and Data Protection Team.

12.7. All general Ticketing related complaints shall be resolved in accordance with the processes listed in Appendix 1 (Process Document Register).

12.8. All complaints and commendations shall be reported in accordance with paragraph 10.

13. Hotlisting Process

13.1. The Service Provider shall Hotlist Oyster cards to deactivate the cards from the Authority's Central System, using the Authority provided applications.

13.2. The Service Provider shall Hotlist Oyster cards that where:

13.2.1. the Oyster card is being replaced due to the Oyster card being reported as lost, stolen or failed;

13.2.2. a refund of the balance is being paid to the Customer; or

13.2.3. the Oyster card is no longer being used.

14. Fraud and Suspicious Activities

14.1. The Authority undertakes regular checks on fraudulent and suspicious activities. The Service Provider shall assist the Authority on any investigation into fraud or suspicious activities.

14.2. The Authority shall provide, and the Service Provider shall comply with, guidelines for investigating irregular or suspicious activity where the cases are in relation to the Service Provider Personnel.

14.3. The Authority shall provide any evidence of irregular activity identified in the Authority's systems and applications to the Service Provider for full investigation. The outcome of the Service Provider's investigation shall be sent to the Authority within 10 Business Days of the Authority providing the evidence. The Service Provider shall review such evidence on a case by case basis and will promptly agree a course of action with the Authority's Internal Audit Department and the Service Provider to correct the irregular activity and prevent the reoccurrence of the irregular activity.

15. Quality Audits

15.1. The Authority shall undertake Periodic quality and compliance to Ticketing process audits on the Agents. In addition to this, the Authority shall also perform quality and compliance audits on the Agents through an independent third party.

15.2. The audit assessments shall be based on the criteria detailed in Appendix 5 (Quality Measurement Criteria). The Agents shall be measured against the criteria set by the Authority and the criteria set by Top 50 Mystery Shopper Survey.

15.3. The Authority and the Service Provider will review the results of the audits, discuss and plan for actions for resolving any ongoing issues at the Service Review Meeting every Period to be implemented at the Service Provider's cost.

16. Secure Disposal

16.1. Disposal of materials, including all personal Data (as applicable), must be carried out at the Service Provider's premises using crosscut shredding equipment, or other secure disposal method approved by the Authority.

16.2. The sub-contractor, if any, used for this process, must be approved by the Authority fraud and security department.

17. Data Retention

17.1. The Service Provider shall retain and dispose of all Data, including Personal Data, in accordance with Clause 24 (Records, Audit and Inspection).

17.2. Data retention rules may be changed by the Authority from time to time.

18. Security

18.1. The Service Provider shall ensure that any premises to be used to deliver the Services, will adopt such physical security measures, as Assured by the Authority, to reduce the risks of any criminal, or other, activity to the detriment of the Authority, to an agreed level, as low as reasonably practicable.

18.2. The Service Provider shall have and maintain written practices and procedures, to be approved by the Authority. These will include but not be limited to:

18.2.1. levels of logical security to be applied and maintained in order to protect the software process, such that 'end to end' security of the process is achieved. Access and password levels shall be devised for Service Provider Personnel, with any attempt at unauthorised access being referred automatically to management, with a distinct transaction audit trail being maintained;

18.2.2. physical security, including intruder detection;

18.2.3. fire prevention/detection; and

18.2.4. actions to be taken to suspend and/or investigate any Service Provider Personnel or site suspected of aiding fraudulent and/or criminal activity or aiding a breach of security.

18.3. The Service Provider shall demonstrate that these policies, systems and processes have been designed to comply with BS7799 (Part 1)/ ISO/IEC 27001, PCI DSS Level 1 and any other industry best practice that may be issued from time to time.

18.4. The Service Provider shall ensure Service Provider Personnel have undertaken Disclosure and Barring Service in England ("**DBS**") or Basic Disclosure Scotland in Scotland ("**BDS**") checks before providing any of the Services under the Contract, and as directed by the Authority.

18.5. Pursuant to Clause 24 (Records, audits and inspection) the Authority reserves the right to conduct audit checks on DBS or BDS certificates annually or at such other time as may be reasonably required by the Authority. The Service Provider shall maintain and provide a report containing a list of all Service

Provider Personnel requiring access to the Authority's systems and applications on a Periodic basis.

18.6. The Service Provider will take all possible steps to limit the potential for loss or misuse of any Authority Assets. The Service Provider shall be responsible for any losses caused by fraud, misuse, negligence or wilful default by Service Provider Personnel.

19. Payment processing and accounting

19.1. The Service Provider shall be Payment Card Industry Data Security Standard ("**PCI-DSS**") Level 1 compliant and will ensure that they act in a PCI-DSS Level 1 compliant manner. Pursuant to Clause 30.12, the Service Provider shall:

19.1.1. Inform the Authority within 24 hours, if the Service Provider should suffer a card Data breach.

19.1.2. Provide a plan within 30 days for remediation, should the Service Provider fall out of PCI-DDS Level 1 compliance. Failure to maintain Level 1 compliance may result in termination at the Authority's discretion.

19.2. The Service Provider shall be liable for any costs arising and penalties issued by the card schemes (Visa, MasterCard, American Express) in relation to non-compliance with the PCI-DSS standard.

19.3. Payment cards are to be processed using the Authority's merchant acquirer as appointed from time to time. All transactions shall be authorised online and shall utilise Address Verification System ("**AVS**") and Card Verification Value ("**CV2**") security code verifications. Transaction charges shall be borne by the Authority.

19.4. The Service Provider shall accept only Amex, Electron, Maestro, MasterCard and Visa payment cards.

19.5. All payment card transactions are to be authorised and cleared prior to issuing any Oyster cards. Any failure to carry out this requirement will be at the cost of the Service Provider.

APPENDIX 1 - PROCESS DOCUMENTS AT THE DATE OF THE CONTRACT

Process Ref	Title	Version No.
A1.1	Replacement Adult Card Fulfilment	Version 0.2
A2.1	New Issue Season Ticket / Bus Pass	Version 0.2
A2.2	New Issue PAYG	Version 0.2
A2.3	Gold Card	Version 0.3
A2.4	Damaged Cards	Version 0.2
A2.5	Reissue Replacement Card (Lost in Post)	Version 0.3
A2.6	Returned Cards	Version 0.1
A2.7	Received Without Oyster Card	Version 0.3
A3.1	Lost and Stolen Telephony	Version 0.4
A3.2	Advanced Search	Version 0.3
A3.4	Incorrect Name	Version 0.2
A3.5	Proof of Purchase	Version 0.1
A3.6	Interim Refunds	Version 0.1
A4.1	New Card	Version 0.2
A4.2	Existing Card	Version 0.2
A4.3	Cancel / Amend Orders	Version 0.1
A4.4	Order Not Delivered	Version 0.3
A4.5	Card Delivered Different to Order	Version 0.2
A5.1	Bulk (Corporate) Oyster Card orders	Version 0.3
A6.1	ID&V Process	Version 0.2
B1.1	Entry / Exit	Version 0.3
B1.2	Season Ticket Left at Home	Version 0.1
B1.3	Cancel / Surrender	Version 0.2
B1.4	Overlapping Ticket	Version 0.2
B1.5	Product Added to Hotlisted Card	Version 0.3
B1.6	Fares Additional Refund Application	Version 0.3
B1.7	Failed ATU Follow Up	Version 0.2
B1.8	Statement Requests	Version 0.3
B1.9	Website: Logging In Issues	Version 0.1
B1.10	Website: Cancel Online Order	Version 0.2
B1.11	Website: Failed Online Order	Version 0.1
B1.12	Trade Up	Version 1.1
B1.13	Trade Down	Version 0.3
B1.14	Failed Cards	Version 0.3
B1.15	Failed Card Interim	Version 0.2
B2.1	ID&V and Logging CPC Calls	Version 1.1
B2.2	Resolve CPC Issues	Version 1.1
B2.3	Incomplete Journeys	Version 1.1
B2.4	Accidental Taps	Version 1.1
B2.5	Mixed Card Journeys	Version 1.1
B2.6	CPC Revenue Inspection Appeals	Version 1.1