

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract,

# **Specification of Requirements for Government Banking's 2021 Merchant Acquiring Services Tender**

## **Contents**

1	INTRODUCTION .....	2
2	MERCHANT CARD ACQUIRING SERVICES.....	3
3	PAYMENT GATEWAY and ALTERNATIVE PAYMENT METHOD (APM) SERVICES.....	13
4	MERCHANT CARD ACQUIRING EQUIPMENT.....	31
5	FRAUD AVOIDANCE.....	38
6	ADDITIONAL MANDATORY AND GOVERNMENT BANKING SPECIFIC REQUIREMENTS.....	44
	Annex A – Minimum Service Level Performance Criteria .....	58
	Annex B – Transaction, Settlement and Potential DCC Currencies.....	60
	Annex C – Descriptions of Terms.....	63
	Annex D – Management Information Headings .....	66

## 1 INTRODUCTION

- A. Government Banking is the money transmission conduit for government departments and the wider public sector and as such represents a vital function for government.
- B. In accordance with the terms and conditions of Crown Commercial Services (CCS) RM6118 - Face to face and Card Not Present (CNP) card acquiring, Gateway and APM Services (Lot 1), Government Banking- is seeking to establish a single Supplier Call Off for the provision of Merchant Acquiring Services for the Government Banking Customers (also defined as Customers) identified as Cluster Members in Call-Off Schedule 12.
- C. The Supplier is required to provide Merchant Acquiring services to all Government Banking Customers included in the contract to facilitate the flow of funds from the cardholder to the Government Banking Customer.
- D. Government Banking Customers have a mix of requirements. For some Government Banking Customers, the Supplier is required to provide functionality as a Payment Service Provider (PSP) to collect and process card data for transmission to the Merchant Acquirer service. This includes provision of a customisable user defined payment page, Point of Sale (POS) terminals, Payment Gateways and so on.
- E. References to the Buyer below shall be deemed to cover both Government Banking and the Government Banking Customers.
- F. This Call Off Contract Term shall be for a period of eighty-four (84) months with the option to extend for a further two (2), twelve (12) month periods (84 months + 12 months + 12 months).
- G. These requirements build directly off the Crown Commercial Services Payment Acceptance framework, namely:
- Attachment 10 – Framework Schedule 1 (Specification) 2.0
  - Attachment 10a - Framework Schedule 1 (Specification Appendix A) Lots 1 - 6 Technical Requirements V 1.0
- H. In addition to laying out the foundation for the requirements, this specification will:
- Cover requirements which are unique to Government Banking and not covered at framework level.
  - Confirm elements identified as Optional at framework level; and
  - Strengthen the position on an existing requirement by the inclusion of more detail.
- I. Any requirement indicated by “M” is a mandatory requirement
- J. Requirements indicated by “O” are optional requirements that Government Banking or Government Banking Customers may require during the Call Off Contract.

## 2 MERCHANT CARD ACQUIRING SERVICES

	Framework Level	Government Banking Level
<b>CORE SERVICES</b>		
2.1. The Supplier is required to provide Merchant Card Acquiring Services, to facilitate the receipt, transfer and accounting of incoming domestic and foreign payment streams where current UK sanctions permit, from the Payer, from traditional, new and existing payment cards, to Buyers to facilitate Cardholder Present and Cardholder Not Present Transactions at locations in the UK and globally e.g. UK Military bases abroad, in particular transaction Authorisation, Clearing and, where possible, Settlement.	M	M
2.2. The Supplier shall ensure that all payments are processed, and any issues are resolved in accordance with the Crown Commercial Service's KPI's and the Buyers required Service Level found in Annex A – Minimum Service Level Performance Criteria.	M	M
2.3. Supplier shall state any known Payment Gateways they currently support (interface to) in addition to the Supplier's Payment Gateway and to which they are prepared to interface on a reasonable and non-discriminatory basis	M	M
2.4. The Supplier shall ensure that the following payment cards can be accepted (but Buyers will not be obliged to use) according to <b>ALL CURRENT AND FUTURE MANDATED CARD SCHEME RULES</b> for the Merchant Card Acquiring Services for all card types (e.g. credit, debit, prepaid, commercial, consumer, domestic and cross border) for the following schemes:	M	M
2.4.1. Visa (including Electron, VPay etc.)	M	M
2.4.2. MasterCard (including Maestro etc.)	M	M
2.4.3. American Express	O	M
2.4.4. Diners Club/Discover	O	M
2.4.5. JCB	O	M
2.4.6. China Union Pay, Union Pay International/UPOP.	O	M
2.5. The Supplier shall ensure that the Buyers receive uninterrupted Merchant Card Acquiring Services including authorisations and non-authorisations subject to agreed service levels which include maximum transactions per second, authorisation times and guaranteed availability.	M	M
2.6. The Supplier shall operate from dual centres geographically separated and these locations shall be specified	M	M

2.7. The Supplier's dual centres shall operate in active-active mode and support load balancing and automatic failover routing	O	O
2.8. Supplier's Payment Gateway (if provided by this Merchant Card Acquiring Supplier) will be dual centre and each will require secured, active communications access from and to each of Supplier's Merchant Card Acquiring dual centres.	M	M
2.9. Buyers additional Payment Gateways (as allowed under 2.3 above) will be dual centre and each will require secured, active communications access from and to each of Supplier's Merchant Card Acquiring dual centres.	O	O
2.10. The Supplier shall work with the Buyers and Buyers existing Payment Gateways and Buyers existing Merchant Card Acquiring Services to agree an implementation plan or plans if appropriate to transition to the Merchant Card Acquiring Services as required by the Buyers including providing support for migrating any existing recurring payments received by the Buyers' existing Payment Gateways and existing Merchant Card Acquiring Services but transition is not mandated.	M	M
2.11. The Supplier shall have sufficient capacity to ensure that the Buyers' transaction volumes are catered for without any adverse impact to the Merchant Card Acquiring Services provided to the Buyers and their Payers and transaction volumes and other volumetrics (e.g. number of concurrent web-based users) as set out in the Call Off.	M	M
2.12. The Supplier shall be capable of securely storing, for 7 years, and Supplier shall state whether such storage is available in real-time, near real time or on a batch basis, and in accordance with PCI-DSS, all payment and transaction data processed for and on behalf of the Buyers and the Supplier shall provide a mechanism for deletion of specified data according to GDPR legislation as updated from time to time.	M	M

2.13. The Supplier shall inform the Buyers in accordance with their Service Levels, of any issues or incidents affecting their Merchant Card Acquiring Services and shall maintain a public web status page and the issue response standard is given in Annex A – Minimum Service Level Performance Criteria. or level 1 issues (Buyer unable to transact) and Supplier shall state their expected resolution times for level 1 issues and shall state their other issue levels with expected response and resolution times	M	M
2.14. The Supplier shall inform the Buyers of new payment innovations and methods that become available within the remit of Merchant Card Acquiring as soon as they become available or are firmly committed for implementation by the Supplier in order that they can be implemented by the Buyers if required, including but not necessarily limited to:	M	M
2.14.1. Migration from Dual message to Single message transactions	O	M
2.14.2. Emerging significant card schemes and type	O	M
2.14.3. Tokenisation	O	M
2.14.4. Biometrics	O	M
2.14.5. Digital currencies	O	O
2.14.6. Other.	O	O
2.15. The Supplier shall ensure the Buyers can decide which payment cards in 2.4 above can be accepted and processed at any time, to ensure that the Buyers adhere to their policies regarding the type of payments that can be accepted and processed within card scheme rules and legislation.	M	M
2.16. The Supplier shall provide, by some mechanism, the Buyers and the Buyers Payment Gateways including the Supplier's and those as allowed under 2.3 above with details of new card IIN (BIN) ranges, and the IIN (BIN)s of Card Schemes in use, as and when they are provided by the Card Schemes, and shall ensure that there is no constraint imposed by the Supplier on the Buyers acceptance of the new IIN (BIN)s and IIN (BIN) ranges from the date they are available in the market.	M	M
2.17. The Supplier shall ensure a PCI-DSS secure connection (TLS 1.2 standard and as amended and upgraded from time to time, for example, TLS 1.3 as now defined in IETF RFC 8446, August 2018 or other approved secure industry standard) is used between a Buyer existing Payment Gateway (as allowed under 2.3 above) and the Supplier's Merchant Card Acquiring Services.	M	M

2.18. The Supplier shall ensure there is a segregation of each Buyer's data and that of any other merchants to avoid exposing each Buyer's data to unauthorised parties.	M	M
<b>MERCHANT CARD ACQUIRING SET-UP</b>		
2.19. The Supplier shall assign a unique Buyer identifier (CID) to each Buyer. The unique Buyer identifier used shall be agreed by the Supplier and each Buyer.	M	M
2.20. The Supplier shall engage and work with Buyers and Supplier's Payment Gateway and Buyers other Payment Gateways as allowed under 2.3 above in order to set-up and assign merchant IDs (MIDs), Terminal IDs (TIDs), and groups of MIDs and TIDs, and shall ensure that the set-up reflects the structure required by each Buyer.	M	M
2.21. The Supplier shall link Buyers' MIDs, TIDs and groups of MIDs and TIDs to specific Buyer bank accounts and facilitate separation by, but not necessarily limited to:	M	M
2.21.1. Lines of business	M	M
2.21.2. Different teams	M	M
2.21.3. Work streams	M	M
2.21.4. Currencies	M	M
2.21.5. Channels	M	M
2.21.6. Other.	O	O
2.22. The Supplier shall verify the accuracy of Buyers' MIDs and TIDs, and the required separation to ensure that the implementation is completed correctly.	M	M
2.23. The Supplier shall ensure that the Buyers can accept and settle transactions in GBP and where required into multiple MIDs and TIDs.	M	M
2.23.1. The Supplier shall ensure that the Buyers can accept, in addition to GBP, various currencies by MIDs and TIDs, including, but not limited to Acceptance and Settlement Currencies are listed in Annex B – Transaction, Settlement and Potential DCC Currencies.	O	M
2.24. The Supplier shall ensure Buyers can assign each Transaction a unique, custom identifier that shall be agreed by the Supplier and the Buyers and shall be included in all dataflows and reports.	M	M

2.25. Buyers shall be able to select a floor limit (in consultation with the Supplier), and the Buyers Payment Gateways including the Supplier's and those (as allowed under 2.3 above) including a zero limit that requires all transactions to be authorised to confirm sufficient funds are in the Payer's account prior to the transaction being processed and an offline floor limit for use when the Merchant Card Acquiring equipment fails to communicate with the Supplier.	M	M
<b>TAKING &amp; PROCESSING PAYMENTS &amp; SETTLEMENT</b>		
2.26. If required by the Buyers, and in accordance with Card Scheme rules, the Supplier shall provide the Buyers with a facility to collect and transfer payment processing charges if any from a Payer in a stream separate from the Gross revenue collected to enable the Buyers to reconcile the recovery of payment processing charges within internal accounting ledgers, that is, an option for Gross Settlement as well as Net Settlement except where card scheme rules or legislation make this impossible.	M	M
2.27. When each Transaction is processed, the Merchant Card Acquiring Services shall facilitate authorisation of Transactions to provide Buyers with a response indicating the status of each Transaction submitted, including, all details on the decline codes used by issuers as allowed under Card Scheme rules, including, but not necessarily limited to;	M	M
2.27.1. Approve	M	M
2.27.2. Decline	M	M
2.27.3. Refer (for Issuer contact during transaction)	O	M
2.27.4. Decline and pick up card	O	M
2.27.5. Other.	O	O
2.28. The Supplier shall ensure that for each unique Transaction reference, payment is only taken once enabling Buyers to notify the Payer accordingly with a customisable message written by the Buyer.	M	M
<b>SETTLEMENT</b>		
2.29. The Supplier will assist as necessary all Buyers Payment Gateway Service providers (whether Supplier's or otherwise as allowed under 2.3 above) with configuring equipment to initiate end of day procedures or single message transaction submission when this becomes an industry standard.	M	M

2.30. The Supplier shall enable Buyers in conjunction with Buyers Payment Gateways (whether Supplier's or otherwise (as allowed under 2.3 above) to choose and put in place an agreed settlement process, including times, for the Buyers' end of day procedures and receipt of funds and this shall be flexible by MID and TID.	M	M
2.31. Buyers may require some payment cards owned by some card schemes to be settled directly to Buyers by those card schemes or as dictated by card scheme rules, for example Amex	M	M
2.32. Buyers may require Supplier to settle certain currencies to an institution that is providing Dynamic Currency Conversion services or other currency services to Buyers.	O	M
2.33. The Supplier shall support day 0 (intraday) settlement, where day 0 is the date payment is taken before the agreed end of day and shall state any variation between card schemes and shall state any constraints imposed on Buyers in order to achieve intraday settlement, for example, transaction submission by a particular time of that day.	O	O
2.34. The Supplier shall support day 1 settlement, where day 1 is the date after payment is taken and shall state any constraints imposed on Buyers in order to achieve day 1 settlement, for example, transaction submission by a particular time on day 0.	M	M
2.35. The Supplier shall not retain any settlement funds as deposit unless explicitly agreed with the Buyers	M	M
2.36. The Supplier shall provide Buyers with standard terms of 30 days for payments of fees and charges, with the Supplier offering prompt payment discounts for earlier settlement	O	O
2.37. The Supplier shall provide a mechanism to ensure that there is no Netting Off of monies to or from a Buyer's bank account(s), to enable Buyers to see all receipts coming in and all Refunds going out as distinct Transactions and not a composite figure except where card scheme rules or legislation or operational requirements make this impossible.	M	M
2.38. The Supplier shall provide a mechanism to ensure that there is a net settlement option where there is netting off of monies to or from a Buyer's bank accounts except where card scheme rules or legislation or operational requirements make this impossible.	M	M

<b>FOREIGN CURRENCY TRANSACTIONS</b>		
2.39. Where required, the Supplier shall provide the Buyers with Dynamic Currency Conversion or equivalent.	O	M
2.40. Buyers may require Supplier to interface with another institution that provides Dynamic Currency Conversion services.	O	O
2.41. The Supplier shall ensure that the Buyers can accept and settle transactions in GBP and where required into multiple MIDs and TIDs.	M	M
2.41.1. The Supplier shall ensure that the Buyers can accept, in addition to GBP, various currencies by MIDs and TIDs, including, but not limited to Acceptance and Settlement Currencies are listed in Annex B – Transaction, Settlement and Potential DCC Currencies	O	M
<b>REFUNDS, REVERSALS and CHARGEBACKS</b>		
2.42. Where a Chargeback or Refund (credit to cardholder) is applied, the Supplier shall ensure that the Buyer is not charged more than an amount that Supplier shall specify in the provided agreed rate card, and which may be banded by volume, plus the cost to process the original payment	M	M
2.43. The Supplier shall provide Buyers with a secure Chargeback and Request for Information electronic management system accessible by authorised Buyer users to provide information required to manage Chargeback and Request for Information occurrences and regulatory fraud reporting, including, but not necessarily limited to:	M	M
2.43.1. Cardholder Present: POS terminals	M	M
2.43.2. Cardholder Not Present, including any telephone payments	M	M
2.43.3. Online transactions	M	M
2.43.4. Fraudulent transactions	M	M
2.43.5. Other.	O	O
2.44. Supplier's Chargeback management system shall automatically reject (represent debits) Chargebacks where the Supplier's system holds relevant and sufficient rejection information, for example (only), 'out of time' and Supplier shall disclose to Buyer if required the reasons for automatic rejection	M	M

2.45. The Supplier shall provide a complete audit trail, including electronic tie-back to the original Supplier transaction records, enabling Buyers the ability to identify individual payments so all Chargebacks and Refunds can be returned to the original payment card.	M	M
2.46. When a Chargeback is authorised/not authorised the Supplier shall apply the debit/credit to the next Gross settlement and include this debit/credit in the daily report referencing the original transaction reference but this does not include any chargeback fee.	M	M
2.47. The Supplier shall provide Buyers with any information that is required by the Buyers to respond to requests for information (RFIs), for Chargebacks and dispute resolution and the Supplier shall work with the Buyers as required to resolve any issues or queries satisfactorily in accordance with the various Card Scheme rules and the Buyers' Service Levels.	M	M
2.48. Buyers shall have a minimum of 14 working days, or such lesser time as required by Card Scheme rules, and a maximum as set by Card Scheme rules, from the time of receipt of an enquiry, to investigate and respond to enquiries and the Supplier shall work with the Buyers as required to ensure a satisfactory resolution to enquiries relating to, but not necessarily limited to:	M	M
	M	M
2.48.1. Referrals	M	M
2.48.2. Refunds	M	M
2.48.3. Errors	M	M
2.48.4. Fraud	M	M
2.48.5. Other.	O	O
<b>CUSTOMER SERVICE AND SUPPORT</b>		
2.49. The Supplier shall provide support, as required, to the Buyers and where applicable all Buyers Payment Gateways within an agreed timetable and during specific periods of each day, week and year as specified in Annex A – Minimum Service Level Performance Criteria., but not necessarily limited to:	M	M
2.49.1. Set-up of MIDs	M	M
2.49.2. Set-up of TIDS	M	M
2.49.3. Adding to existing MIDs and TIDS, as required	M	M
2.49.4. Interfacing with varying front and back end technology	M	M
2.49.5. Alternative card charging mechanisms	M	M
2.49.6. Fraud minimisation	M	M
2.49.7. Risk management systems	M	M
2.49.8. Incident management	M	M

2.49.9. Reporting files and systems	M	M
2.49.10. Changes in card interchange rates and scheme fees	M	M
2.49.11. Chargebacks and other dispute procedures	M	M
2.49.12. Information on changes in legislation affecting the Merchant Card Acquiring Services	M	M
2.49.13. Technical support and incident management	M	M
2.49.14. Interaction and support with third party suppliers	M	M
2.49.15. Help prevent identified individual Payers from making payments	M	M
2.49.16. Help to find details of payments made by individual Payers	M	M
2.49.17. A dedicated Buyer and technical helpdesk for in and out-of-hours telephone or email queries/issues	M	M
2.49.18. System availability	M	M
2.49.19. Declines optimisation	M	M
2.49.20. Interchange optimisation	M	M
2.49.21. Card scheme fee optimisation	M	M
2.49.22. Representing Authority and Buyer interests with schemes and issuers	M	M
2.49.23. Other.	O	O
<b>PRICING</b>		
2.50. Supplier shall provide and offer easy to reconcile simple blended pricing and Interchange ++ pricing, specifically including interchange and fees and charges either of which may be chosen by the Buyer and shall state which other pricing mechanisms are available.	M	M
2.51. Blended pricing is intended to be fixed for the duration of the contractual term and any variation shall be justified to Crown Commercial Services and mutually agreed between the Supplier and Crown Commercial Services.	M	M
2.52. For Interchange ++ pricing the Supplier fee element may not be altered for the duration of the contractual term.	M	M
2.53. For Interchange ++ pricing the Supplier shall pass Scheme fees and Interchange fees at cost i.e. with no Supplier mark up.	M	M
2.54. For Interchange ++ pricing any fees not in sterling (GBP) will be converted by a foreign exchange rate mechanism to be agreed at the start of the contractual agreement concluded by Crown Commercial Services with the Supplier.	M	M

2.55. All components of Interchange ++ charges and all other fees and charges will be subject to audit on demand by Crown Commercial Services provided that the Crown Commercial Services can demonstrate that there are reasonable grounds to believe that fees and charges are being applied incorrectly.	M	M
2.56. Supplier shall provide an annual financial audit by a qualified external audit institution to Crown Commercial Services to demonstrate that Interchange ++ charges and all other fees and charges are being applied correctly	M	M

### 3 PAYMENT GATEWAY and ALTERNATIVE PAYMENT METHOD (APM) SERVICES

This section sets out the Services Requirements that the Supplier shall be required to fulfil when providing Payment Gateway Services.

	Framework Level	Government Banking Level
<b>CORE SERVICES</b>		
3.1. The Supplier is required to provide Payment Gateway Services, to facilitate the receipt, transfer and accounting of incoming domestic and foreign payment streams, including e-Comm online payments where current UK sanctions permit, from the Payer, from traditional, new and existing payment cards and from new and existing Alternative Payment Methods (APMs), to Buyers at locations in the UK. Present and Cardholder Not Present Transactions, in particular transaction Authorisation, Clearing and, where possible, Settlement.	M	M
3.2. The Supplier is required to provide Payment Gateway Services, to facilitate the receipt, transfer and accounting of incoming domestic and foreign payment streams, including e-Comm online payments where current UK sanctions permit, from the Payer, from traditional, new and existing payment cards and from new and existing Alternative Payment Methods (APMs), to Buyers at locations globally e.g. UK Military bases abroad, to facilitate Cardholder Present and Cardholder Not Present Transactions, in particular transaction Authorisation, Clearing and, where possible, Settlement.	O	M
3.3. The Supplier shall work with the Buyers and the Supplier's Merchant Card Acquiring Service and APM provider or providers to collect and process payment data in compliance with PCI-DSS standards for transmission to the Supplier's Merchant Card Acquiring Service and applicable APM provider and ensure that all payments are processed and any issues are resolved in accordance with the Authority's KPI's and the Buyers Service Levels.	M	M
3.4. Supplier shall state which Merchant Card Acquiring Service providers their Payment Gateway supports (interfaces to) and to which their Payment Gateway will interface to on a reasonable and non-discriminatory basis and at least one is required where this requirement is included in a mandatory Lot.	O	O
3.5. Supplier shall state which aggregating Alternative Payment Method APM providers they currently support (interface to) or provide on their own behalf	M	M

3.6. Supplier shall state which integrated third party solutions they currently support (interface to) e g intershop, shopify	M	M
3.7. The Supplier shall ensure that the following payment cards can be accepted (but Buyers will not be obliged to use) according to <b>ALL CURRENT AND FUTURE MANDATED CARD SCHEME RULES</b> for the Merchant Card Acquiring Services for all card types (e.g. credit, debit, prepaid, commercial, corporate, consumer, domestic and cross border) for the following schemes:	M	M
3.7.1. Visa (including Electron, VPay etc.)	M	M
3.7.2. MasterCard (including Maestro etc.)	M	M
3.7.3. American Express	M	M
3.7.4. Diners Club/ Discover	O	M
3.7.5. JCB	O	M
3.7.6. China Union Pay, Union Pay International/UPOP.	O	M
3.8. The Supplier shall ensure that expedited branded checkout payment methods can be accepted (but Buyers will not be obliged to use) but not necessarily limited to:	M	M
3.8.1. ApplePay	M	M
3.8.2. G Pay	M	M
3.8.3. Masterpass	O	O
3.8.4. Visa Checkout	O	O
3.8.5. Samsung Pay.	O	M
3.8.6. Amazon Pay.	O	M
3.8.7. Other.	O	O
3.9. The Supplier shall specify which APMs they can, route to and process or route to, either collect model or otherwise, (but Buyers will not be obliged to use) according to <b>ALL CURRENT AND FUTURE APM SCHEME RULES</b> . This includes, but is not necessarily limited to:	M	M
3.9.1. Paypal	M	M
3.9.2. UK DD and other UK credit transfer mechanisms	O	O
3.9.3. Alipay	O	M
3.9.4. WeChat	O	M
3.9.5. Paysafecard	O	O
3.9.6. iDeal	O	M
3.9.7. Sofort	O	M
3.9.8. Klarna	O	O
3.9.9. Trustly	O	M
3.9.10. UK Open Banking (single, deferred, regular payments)	O	M
3.9.11. Other.	O	O

3.10. The Supplier shall allow Buyers as required to connect or contract directly or indirectly to any or all APMs without using the Supplier services.	M	M
3.11. The Supplier shall ensure that the Buyers receive uninterrupted Payment Gateway Services including authorisations and non-authorisations subject to agreed service levels Volumetrics (as set out in the Buyer Call Off) which include maximum transactions per second, authorisation times and guaranteed availability.	M	M
3.12. The Supplier shall operate from dual centres geographically separated and these locations shall be specified	M	M
3.13. The Supplier's dual centres shall operate in active-active mode and shall support load balancing and automatic failover routing	M	M
3.14. Supplier's Merchant Card Acquiring Services (if provided by this Payment Gateway Supplier) will be dual centre and each will require secured, active communications access from and to each of Supplier's Payment Gateway dual centres.	M	M
3.15. Buyers additional Merchant Card Acquiring Services (as allowed under 3.4 above) will be dual centre and each will require secured, active communications access from and to each of Supplier's Payment Gateway dual centres.	O	O
3.16. The Supplier shall work with the Buyers and Buyers existing Merchant Card Acquiring Services and Payment Gateway Services to agree their implementation plan or plans if appropriate to transition to the Payment Gateway Services as required by the Buyers including, if required, providing support for migrating any existing recurring payments received by the Buyers' existing Payment Gateway Services and existing Merchant Card Acquiring Services but transition is not mandated.	M	M
3.17. The Supplier shall have sufficient capacity to ensure that the Buyers' transaction volumes are catered for without any adverse impact to the Payment Gateway Services provided to the Buyers and their Payers and transaction and other volumetrics (e.g. number of concurrent web-based users) are given in Annex A – Minimum Service Level Performance Criteria.	M	M

3.18. The Supplier shall be capable of securely storing, for 7 years, and Supplier shall state whether such storage is available in real-time or near real-time or on a batch basis, and in accordance with PCI-DSS, all payment and transaction data processed for and on behalf of the Buyers and the Supplier shall provide a mechanism for deletion of specified data according to GDPR legislation as updated from time to time.	M	M
3.19. The Supplier shall inform the Buyers in accordance with their Service Levels, of any issues or incidents affecting their Payment Gateway Services and shall maintain a public web status page and the issue response standard is given in Annex A – Minimum Service Level Performance Criteria. or level 1 issues (Buyer unable to transact) and Supplier shall state their expected resolution times for level 1 issues and shall state their other issue levels with expected response and resolution times.	M	M
3.20. The Supplier shall inform the Buyers of new payment innovations and methods that become available and make such innovations and methods available to the Buyers in order that they can be implemented by the Buyers if required, including, but not necessarily limited to:	M	M
3.20.1. Migration from Dual message to Single message transactions	M	M
3.20.2. Emerging significant APMs	M	M
3.20.3. Biometrics	O	O
3.20.4. Digital currencies example Bitcoin	O	O
3.20.5. Other.	O	O
3.21. The Supplier shall ensure the Buyers can decide which payment cards and branded payment methods and APMs (in 3.7 above, 3.8 above and 3.9 above) can be accepted and processed at any time, to ensure that the Buyers adhere to their policies regarding the type of payments that can be accepted and processed.	M	M
3.22. The Supplier shall support a request to provide the Buyers with details of new card IIN (BIN) ranges, and the IIN (BIN)s of Card Schemes in use, as and when they are provided by the Card Schemes and Supplier's Merchant Card Acquiring Service providers, and shall ensure that there is no constraint imposed by the Supplier on the Buyers acceptance of the new IIN (BIN)s and IIN (BIN) ranges from the date they are available in the market and Supplier shall state the mechanisms for provision including by file transfer and by API .	M	M

3.23. The Supplier shall ensure a PCI-DSS secure connection (TLS 1.2 standard and as amended and upgraded from time to time, for example, TLS 1.3 as now defined in IETF RFC 8446, August 2018 or other approved secure industry standard) is used between a Buyer, Buyer point of presence, including directly from Payer where applicable and the Supplier's Payment Gateway Service.	M	M
3.24. The Supplier shall ensure a PCI-DSS secure connection (TLS 1.2 standard and as amended and upgraded from time to time, for example, TLS 1.3 as now defined in IETF RFC 8446, August 2018 or other approved secure industry standard) is used between the Supplier's Payment Gateway Service and any additional Merchant Card Acquiring service as allowed under 3.4 above.	M	M
3.25. The Supplier shall ensure there is a separation of each Buyer's data and that of any other merchants to avoid exposing each Buyer's data to unauthorised parties.	M	M
<b>PAYMENT GATEWAY SERVICES</b>		
3.26. The Supplier shall provide Payment Gateway Services for Buyers at designated locations in the UK and globally, e.g. UK Military bases abroad, including third party locations.	M	M
3.27. The Payment Gateway Services shall have the functionality to connect to the Supplier's Merchant Card Acquiring Service and only any additional Merchant Card Acquiring service as allowed under 3.4 above so that the Buyers are not required to invest in a bespoke network or new infrastructure to facilitate the Merchant Card Acquiring Service. Supplier's Payment Gateway Services connectivity to Supplier's Merchant Card Acquiring Service and any additional Merchant Card Acquiring service as allowed under 3.4 above shall be secure and high capacity and shall cover, but shall not necessarily be limited to:	M	M
3.27.1. Internet connection	M	M
3.27.2. Any connectivity of sufficient security and capacity	M	M
3.27.3. Broadband	O	O
3.27.4. MPLS	O	O
3.27.5. Other.	O	O

3.28. The Supplier shall support a mechanism to enable Buyer to take Cardholder Not Present transactions in a call centre environment including IVR (which may be run by a 3 <sup>rd</sup> party), usually referred to as Mail Order/Telephone Order and Supplier shall state how they support this mechanism being PCI-DSS compliant.	M	M
3.28.1. As a minimum a simple screen-based mechanism shall be available.	M	M
3.29. The Supplier shall provide Buyers with Payment Gateway Services and connect to the Supplier's Merchant Card Acquiring Services and any additional Merchant Card Acquiring service as allowed under 3.4 above to facilitate Cardholder Present transactions at point of presence to enable the Buyers' Payers to make payments.	M	O
3.30. Buyers points of presence shall include a wide range of Merchant Card Acquiring Equipment including, but not necessarily limited to,	M	O
3.30.1. EMV Compliant PIN Entry Devices (including contactless), terminal, smart MPOS providers e.g. Verifone, Ingenico, PAX, Spire, Worldline	M	O
3.30.2. EPOS/ECR solution providers e.g. Oracle/Micros	O	O
3.30.3. Other.	O	O
3.31. The Supplier shall provide details of all other encrypted (TLS 1.2 and subsequent as amended from time to time, for example, TLS 1.3 as now defined in IETF RFC 8446, August 2018 or other approved secure industry standard). integration mechanisms for use by the Buyer.	M	M
3.31.1. frame	M	M
3.31.2. Hosted payment page	M	M
3.31.3. Mobile SDKs	O	O
3.31.4. Silent order POST	O	O
3.31.5. Other.	O	O
3.32. The Supplier shall provide details of secure, encrypted (see 3.31 above) API integration connections from other PCI compliant Level 1 Service providers including, but not necessarily limited to,	M	M
3.32.1. GOV.UK Pay	M	M
3.32.2. Other.	O	O
3.33. Other PCI compliant Level 1 Service providers may be dual centre and each (where dual) will require secured, active communications access from and to each of the Supplier's Payment Gateway dual centres.	M	M

3.34. The Supplier shall ensure that the Payment Gateway Services can process Refunds and all other card scheme and APM provider mandated transaction types.	M	M
3.35. The Supplier shall ensure a secure connection (TLS 1.2 standard and as amended and upgraded from time to time, for example, TLS 1.3 as now defined in IETF RFC 8446, August 2018 or other approved secure industry standard) is used between the Buyer's website, the Buyers' points of presence, and the Supplier's Payment Gateway Services at all times. This connectivity shall be of sufficient capacity and shall cover, but shall not necessarily be limited to:	M	M
3.35.1. Internet connection	M	M
3.35.2. Any emerging connectivity of sufficient security and capacity	M	M
3.35.3. Broadband	O	O
3.35.4. MPLS	O	O
3.35.5. Other.	O	O
3.36. The Supplier shall ensure that Payment Gateway Services and systems provided to Buyers to take payments are in line with current industry standards in order that the Payment Gateway Services will reliably process each transaction within defined service levels (see Annex A – Minimum Service Level Performance Criteria), excluding time outboard of the Payment Gateway Service to Supplier's Merchant Card Acquiring Service providers, card scheme networks and APM providers.	M	M
3.37. The Supplier shall ensure that all web-based interfaces use by Buyers or Payers meet, as a minimum, Level AA of the Web Content Accessibility Guidelines (WCAG) 2.0 and UK Equality Act (2010) legislation as updated from time to time.	M	M
3.38. The Supplier shall maintain, as a minimum, the equivalent level of browser support as GOV.UK.	M	M
3.39. The Supplier shall ensure that the Payment Gateway pages are rendered correctly for compatibility with devices with variable screen sizes, including, but not necessarily limited to:	M	M
3.39.1. Desktops	M	M
3.39.2. Laptops	M	M
3.39.3. Smart phones	M	M
3.39.4. Tablet devices	M	M
3.39.5. Other software only devices as standards allow now and, in the future,	M	M
3.39.6. Other.	O	O

3.40. The Supplier shall ensure that the Payment Gateway pages for Payers can be customised, by the Supplier and/or the Buyer, including, but not necessarily limited to, the customisation of and the Supplier shall state which mechanisms are available:	M	M
3.40.1. Card type acceptance including ordering of card types	M	M
3.40.2. APMs	M	M
3.40.3. Copy	O	O
3.40.4. Branding	O	O
3.40.5. Logos	O	O
3.40.6. Colour schemes	O	O
3.40.7. Fonts	O	O
3.40.8. Phrases	O	O
3.40.9. Wording	O	O
3.40.10. Contact details	O	O
3.40.11. Currencies	O	O
3.40.12. Other.	O	O
3.41. Any changes requested by Buyers to the Payment Gateway pages shall be supported, and the methods stated	M	M
3.41.1. Card type acceptance	M	M
3.41.2. APMs	M	M
3.41.3. Copy	O	O
3.41.4. Branding	O	O
3.41.5. Logos	O	O
3.41.6. Colour schemes	O	O
3.41.7. Fonts	O	O
3.41.8. Phrases	O	O
3.41.9. Wording	O	O
3.41.10. Contact details	O	O
3.41.11. Currencies	O	O
3.41.12. Other.	O	O
3.42. If required by Buyers, the Supplier shall provide the Buyers with auto populated or manual entry payment page(s) in order to capture the data required to process payments and provide the Buyers with the relevant reporting information, but not necessarily limited to, the following fields:	M	M
3.42.1. PAN (15 to 19 digits)	M	M
3.42.2. CSC (3 & 4 digits)	M	M
3.42.3. Amount	M	M
3.42.4. Expiry end date	M	M
3.42.5. Individual Payer name	M	M
3.42.6. Buyer identifier (Company ID (CID))	M	M
3.42.7. Buyer Transaction description reference	M	M
3.42.8. Start date (where required)	M	M

3.42.9. Secure link to APM providers as required by those providers or any other regulatory standards	M	M
3.42.10. Buyer Payer identifier	M	M
3.42.11. Items/services purchased	O	O
3.42.12. Email address	O	O
3.42.13. Other	O	O
3.42.14. Individual Payer billing address including post code.	O	O
3.43. The Payment Gateway Services provided to the Buyers shall have Payment Gateway pages with a selection of languages for multi-lingual Payers to use the Payment Gateway Services in their own language. The selection of languages shall include, but shall not necessarily be limited to:	M	M
3.43.1. English	M	M
3.43.2. Welsh	M	M
3.43.3. Other.	O	O
3.44. The Supplier shall provide Buyers with a well-documented real time HyperText Transfer Protocol Secure (HTTPS) Application Programme Interface (API) to capture payment details through their own payment pages or equivalent, before the Transaction is processed.	M	M
3.44.1. The API shall be RESTful	O	O
3.45. Supplier shall provide a mechanism so that cardholder data and sensitive authentication data does not necessarily need to pass through Buyers main computers	M	M
3.46. Supplier shall provide a mechanism where Cardholder data shall be returned to the Buyer as a one-to-one mapped token which can be stored by the Buyers main computers and a masked PAN showing only the first 6 and last 4 digits, or optionally only the last 4	M	M
3.47. Supplier is responsible for converting token on reuse to a PAN to enable subsequent payments without Payer needing to enter PAN details and so facilitating one-click payment	M	M
3.48. Supplier cannot retain PCI-DSS defined sensitive authentication data except for a strictly limited period, example 15 minutes as allowed by PCI standards.	M	M
3.49. Supplier shall provide a mechanism to tokenise cardholder data out with a payment	M	M

3.50. Supplier shall provide a mechanism to bulk tokenise Buyers existing cardholder data, with PCI compliance, to assist in any necessary transition from an existing Supplier to the new Supplier	M	M
3.51. Supplier shall, on contract termination (expiry), provide a bulk file of detokenised cardholder data, free of charge and with an agreed service level as specified in Annex A – Minimum Service Level Performance Criteria. and in a PCI compliant manner	M	M
3.52. Supplier shall provide for secure communication from Buyer point of presence equipment and will generate a token and masked PAN as for payment pages. Identical PANs will generate the same token across payment pages and point of presence (all channels) to allow true omni channel operation and post purchase MI	M	M
3.53. Supplier shall provide a mechanism that exposes card scheme Payment Account Reference (PAR) values where card have been stored in ApplePay or G Pay devices, as these stored PANs do not equal original cardholder data	O	O
3.54. Supplier shall state whether they use a 3 <sup>rd</sup> party external tokeniser or a 3 <sup>rd</sup> party in-house tokeniser or a Supplier developed own tokeniser	M	M
3.55. Supplier shall state whether they would consider providing token services to other gateways	O	O
3.56. Supplier's tokenisation services shall be optional for Buyers.	M	M
3.57. The Supplier shall state what mechanism and 3 <sup>rd</sup> party systems they support to enable PCI-DSS compliance in a Buyer's call centre environment, for example, DTMF masking, IVR.	M	M
3.58. The Supplier shall, where requested by a Buyer in the Call Off, allow for encrypted API connection, with full transaction data including sensitive payment card or APM details from another PCI compliant Level 1 Service provider including, but not limited to, <b>GOV.UK Pay</b> .	M	M
3.59. The Supplier shall provide Buyers with one or more seamless mechanisms for transition from the Buyer's website to the Payment Gateway Services so it appears to the Payer that they are still on the Buyer's website and these mechanisms shall be specified e.g. hosted payment page. The transition shall include ensuring that the Payer is aware that they are entering a secure environment.	M	M

3.60. The Supplier shall ensure that there is a segregation of the Buyer's data and that of any other merchants to avoid exposing the Buyer's data to unauthorised third parties.	M	M
3.61. The Supplier shall provide Buyers with the facility to accept and securely process recurring and repeat payments through the Payment Gateway Services as required.	M	M
3.62. The Supplier shall provide Buyers with details and information of new APMs as and when they become available within their offering and shall ensure that if required by the Buyers, that their Payment Gateway Services can accept them	M	M
3.63. The Supplier shall state what services they supply to hold Payer's details including payment methods previously used and stored to enable new payment to be made without re-entering previous details – a process known as one-click but this does not preclude Buyer from managing this process externally to the Supplier.	M	M
3.64. The Payment Gateway Services shall provide the Buyer with 3D Secure 1.0 and EMVCO 3-D Secure 2.2 as amended or replaced from time to time or equivalent for all card payments made by a Payer to the Buyer using the Payment Gateway Services. Buyer shall not be required to use this service and shall be able to use or not use on any individual payment transaction within the constraints of PSD2 regulations as amended or replaced from time to time.	M	M
3.65. The Supplier shall apply all SCA exemptions, where allowed, on transactions and shall specify to the Authority how they take advantage of the SCA exemptions allowed under PSD2	M	M
3.66. The Payment Gateway Services will provide a mechanism to alert the Buyers by secure API or alternative secure mechanism if the status of a transaction changes after authorisation or settlement and the Buyers will not be obliged to use any or all of these mechanisms.	O	O
<b>MERCHANT CARD ACQUIRING AND APM SET-UP</b>		
3.67. The Supplier shall assign a unique Identifier to each Buyer. The unique Identifier used shall be agreed by the Supplier and each Buyer and will map to the Merchant Card Acquiring Service CID where appropriate.	M	M

3.68. The Supplier shall engage and work with Buyers and Buyers Merchant Card Acquiring Service providers and APM providers as required in order to set-up and assign merchant IDs (MIDs), Terminal IDs (TIDs), and groups of MIDs and TIDs, and other identifiers for APM providers and shall ensure that the set-up reflects the structure required by each Buyer.	M	M
3.69. The Supplier shall link Buyers' APM identifiers to specific Buyer bank accounts where Supplier is operating a Collect model, where more than one APM settlement is aggregated by the Supplier for Buyers, and facilitate separation by, but not necessarily limited to:	M	M
3.69.1. Lines of business	M	M
3.69.2. Different teams	M	M
3.69.3. Work streams	M	M
3.69.4. Currencies	M	M
3.69.5. Other.	O	O
3.70. The Supplier shall verify the accuracy of Buyers' MIDs and TIDs, and the required separation to ensure that the implementation is completed correctly.	M	M
3.71. The Supplier shall not delete/purge any inactive MIDs or TIDs without express permission of the Buyer.	M	M
3.72. The Supplier shall ensure that the Buyers can accept and settle transactions in GBP and where required into multiple MIDs and TIDs.	M	M
3.72.1. The Supplier shall ensure that the Buyers can accept, in addition to GBP, various currencies by MIDs and TIDs, including, but not limited to Acceptance and Settlement Currencies are listed in Annex B – Transaction, Settlement and Potential DCC Currencies	O	M
3.73. The Supplier shall ensure Buyers can assign each Transaction a unique, custom identifier that shall be agreed by the Supplier and the Buyers and shall be included in all dataflows and reports.	M	M
3.74. Buyers shall be able to select a floor limit, in consultation with the Supplier and the Buyers Merchant Card Acquiring providers including the Supplier's and those as allowed under 3.4 above, including a zero limit that requires all transactions to be authorised to confirm sufficient funds are in the Payer's account prior to the transaction being processed and an offline floor limit for use when the Merchant Card Acquiring equipment fails to communicate with the Supplier.	M	M

3.75. The Supplier shall agree a process and other mechanisms with each Buyer that shall allow only designated Buyer personnel or their authorised representatives acting as agents to issue Refunds by manual intervention.	M	M
3.76. Where Buyers own or rent Merchant Card Acquiring equipment that is used to accept payments under separate contracts, on a Buyer's authorisation, the Supplier shall work with the Buyer's third party suppliers, as if they are the Buyer, to connect the Merchant Card Acquiring equipment to the Payment Gateway Services at a reasonable and non-discriminatory charge to be agreed by the parties, to ensure all payments are processed and to any issues are resolved in accordance with the Authority's KPI's and the Buyer's Service Levels	M	M
<b>TAKING &amp; PROCESSING PAYMENTS &amp; SETTLEMENT</b>		
3.77. The Supplier will assist as required Buyers additional Merchant Card Acquiring (as allowed under 3.4 above) and Supplier's Merchant Card Acquiring Service and additional Merchant Card Acquiring Equipment Service providers under 4.3 below and Supplier's Merchant Equipment Service provider with configuring equipment to initiate end of day procedures or single message transaction submission when this becomes an industry standard	M	M
3.78. When each Transaction is processed, the Payment Gateway Services shall facilitate authorisation of Transactions to provide Buyers with a response, including all codes allowed by card scheme and APM rules, indicating the status of each Transaction submitted, including, but not necessarily limited to	M	M
3.78.1. Approve	M	M
3.78.2. Decline	M	M
3.78.3. Other APM responses as defined by the APM provider	M	M
3.78.4. Refer	O	O
3.78.5. Decline and pick up	O	O
3.78.6. Other.	O	O
3.79. The Supplier shall ensure that for each unique Transaction reference, payment is only taken once enabling Buyers to notify the Payer accordingly with a customisable message written by the Buyer in agreement with the Supplier.	M	M

3.80. Where required, the Supplier shall allow Buyers to register a callback Uniform Resource Locator (URL) to receive real time updates when the status of a Transaction changes.	O	O
3.81. The Supplier shall ensure that any callback URL comes from a specified range of Internet Protocol (IP) addresses, which shall be communicated to the Buyers, to enable the callback URL to be permitted through the Buyers' firewalls and validated within applications as an extra security measure.	O	O
3.82. The Supplier shall allow Buyers to register different Uniform Resource Locators (URL) relating to receiving notification of either authorisation approval or decline.	M	M
3.83. The Supplier shall provide Buyers with the option to automatically confirm payment with the Payer via email and where required manage all communication with the Payer.	O	O
3.84. Where required, the Supplier shall provide Buyers with the functionality to customise receipt emails. Buyers shall be able to customise the following as a minimum, but not necessarily limited to:	O	M
3.84.1. Branding	O	O
3.84.2. Text	O	O
3.84.3. Contact details	O	O
3.84.4. Website details	O	O
3.84.5. Web links to enquiry forms.	O	O
3.84.6. Web links to enquiry forms.	O	O
<b>APM SETTLEMENT</b>		
3.85. The Supplier shall allow the Buyer to sign contracts with APMs directly or to allow Supplier's Payment Gateway to take settlement of the APM funds on its behalf (known as the Collect Model) and manage associated settlement risk, refunds etc. as if they were Card Payments	M	M
3.86. The Supplier shall enable Buyers in conjunction with Buyers APM providers to choose and put in place an agreed settlement process, including times, for the Buyers' end of day procedures and receipt of funds.	M	M
3.87. The Supplier shall agree with the Buyers in conjunction with Buyers APM providers the settlement cut off time. A Buyer shall have the flexibility to set this by MID or TID to facilitate alignment of its system cut offs with the Payment Gateway Services cut offs.	M	M

3.88. The Supplier shall provide a mechanism to ensure each Buyer receives value for all APM payments, except where APM providers settle directly with Buyers in its specified bank account(s) and in accordance with its chosen agreed day and time which may be day 0 (intraday) or on day 1 or on such day as shall be agreed between the Supplier and the Buyer which will be no later than that provided by the APM supplier plus 1 day, where day 0 is the date payment is taken before the agreed end of day. This ensure that revenue is paid over in accordance with each Buyer's agreed settlement date and time and mechanism. Supplier shall not retain any settlement funds as deposit.	M	M
3.89. The Supplier shall provide Buyers with standard terms of 30 days for payments of fees and charges, with the Supplier offering prompt payment discounts for earlier settlement	O	O
3.90. The Supplier shall provide a mechanism to ensure that there is no Netting Off of monies to or from a Buyer's bank account(s), to enable Buyers to see all receipts coming in and all Refunds going out as distinct Transactions and this will include chargebacks and not a composite figure except where card scheme rules or legislation or operational requirements make this impossible.	M	M
3.91. The Supplier shall provide a mechanism to ensure that there is a net settlement option where there is netting off of monies to or from a Buyer's bank accounts except where card scheme or APM rules or legislation or operational requirements make this impossible	M	M
<b>FOREIGN CURRENCY TRANSACTIONS</b>		
3.92. The Supplier shall ensure that the Buyers can accept and settle transactions in GBP and where required into multiple MIDs and TIDs.	M	M
3.92.1. The Supplier shall ensure that the Buyers can accept, in addition to GBP, various currencies by MIDs and TIDs, including, but not limited to Acceptance and Settlement Currencies are listed in Annex B – Transaction, Settlement and Potential DCC Currencies	O	M
3.93. Where required, the Supplier shall provide the Buyers with Dynamic Currency Conversion or equivalent.	O	M
3.94. Buyers may require Supplier to interface with another institution that provides Dynamic Currency Conversion services.	O	O

3.95. The Supplier shall ensure that the Buyers can accept and settle transactions in GBP and where required into multiple MIDs and TIDs.	M	M
3.95.1. The Supplier shall ensure that the Buyers can accept, in addition to GBP, various currencies by MIDs and TIDs, including, but not limited to Acceptance and Settlement Currencies are listed in Annex B – Transaction, Settlement and Potential DCC Currencies	O	M
<b>REFUNDS (full and partial), REVERSALS and CHARGEBACKS</b>		
3.96. Where required, the Supplier shall provide Buyers with the capability to process bulk Refunds using an electronic file upload.	M	M
3.97. The Supplier shall provide Buyers with a well-documented real time secure API to initiate Refunds for any given Transaction to provide a smooth integration with a Buyer's case management system.	M	M
3.97.1. APIs shall be RESTful	O	O
3.98. The Supplier shall provide Buyers with a web-based portal to initiate Refunds for any given Transaction.	M	M
3.99. The Supplier shall provide Buyers with a Refund report including any information required by Buyers to execute a full or partial Reversal or Refund (credit to cardholder) of a Transaction easily, promptly and to the original payment method.	M	M
3.100. The Supplier shall provide a complete audit trail enabling Buyers the ability to identify individual payments so all Refunds can be returned to the original payment mechanism.	M	M
<b>CUSTOMER SERVICE AND SUPPORT</b>		
3.101. The Supplier shall provide support to the Buyers and where applicable Buyers other providers within an agreed timetable as specified in Annex A – Minimum Service Level Performance Criteria. and including, but not necessarily limited to:	M	M
3.101.1.Set-up of MIDs	M	M
3.101.2.Set-up of TIDs	M	M
3.101.3.Adding to existing MIDs and TIDS, as required	M	M
3.101.4.Supply and interfacing to of hardwired PDQ Terminals (including Contactless)	M	O
3.101.5.Supply and interfacing to of wireless PDQ Terminals (including Contactless)	M	O

3.101.6. Supply and interfacing to of Bluetooth PDQ Terminals (including Contactless)	M	O
3.101.7. Electronic PDQ card payment terminals (including Contactless)	M	O
3.101.8. MPOS equipment	M	O
3.101.9. Data transmission to the supplier	M	O
3.101.10. Interfacing with car parking payment machines	M	O
3.101.11. Interfacing with varying front and back end technology	M	O
3.101.12. Interfacing with contactless alternatives	M	O
3.101.13. Alternative card charging mechanisms	M	M
3.101.14. Fraud minimisation	M	M
3.101.15. Risk management systems	M	M
3.101.16. Incident management	M	M
3.101.17. Reporting files and systems	M	M
3.101.18. Changes in card interchange rates and scheme fees	M	M
3.101.19. Chargebacks	M	M
3.101.20. Information on changes in legislation affecting the Payment Gateway Services	M	M
3.101.21. Technical support and incident management	M	M
3.101.22. Interaction and support with third party suppliers	M	M
3.101.23. Connectivity to Merchant Card Acquiring Services	M	M
3.101.24. Help prevent identified individual Payers from making payments	M	M
3.101.25. Help to find details of payments made by individual Payers	M	M
A dedicated technical helpdesk for in and out-of-hours telephone or email queries/issues	M	M
3.101.27. System availability	M	M
3.101.28. Declines optimisation	M	M
Marketplace regulatory support to manage flow of funds through relevant FCA licenses and contracts with sub-entities	M	M
3.101.30. Items/services purchased.	O	O
3.101.31. Helping a Payer make and complete a payment	O	O
3.101.32. Other.	O	O
OTHER		
3.102. The Supplier shall state whether they support any mechanisms to share their data. including tokens and fraud data with other Payment Gateways	O	O
OPTIONAL CAPABILITY		

3.103. Buyers may have a requirement to provide over the counter banking services including but not necessarily limited to	O	O
3.103.1.Withdrawals	O	O
3.103.2.Deposits	O	O
3.103.3.Mini-statements	O	O
3.103.4.PIN services	O	O
3.103.5.Other.	O	O
3.104. Supplier shall state whether they have the capability to support such services.	O	O
3.105. Supplier shall state the mechanisms for supporting such services.	O	O
3.106. Supplier shall state whether they support services additional to those in 3.103 above.	O	O
3.107. Supplier shall state what Value Added Services they can provide to the services in 3.103 above.	O	O
3.108. The Supplier shall state which PISPs they use and which PISPs they support, even if not in live operation, in order to offer an alternative to direct connection to a PISP by the Buyers.	M	M

## 4 MERCHANT CARD ACQUIRING EQUIPMENT

This section sets out the Services Requirements that the Supplier shall be required to fulfil when providing Merchant Card Acquiring Equipment.

	Framework Level	Government Banking Level
<b>CORE SERVICES</b>		
4.1. The Supplier is required to provide Merchant Card Acquiring Equipment, to facilitate the receipt, transfer and accounting of incoming domestic and foreign payment streams where current UK sanctions permit, from the Payer, from traditional, new and existing payment cards, to Buyers (and via Supplier's Payment Gateway Service and the relevant Merchant Card Acquiring service) to facilitate Cardholder Present and Cardholder Not Present Transactions at locations in the UK and globally e.g. UK Military bases abroad.	M	M
4.2. The Supplier shall work with the Buyers and the Supplier's Payment Gateway Service to collect and process payment data for transmission to the relevant Merchant Card Acquiring Services and ensure that all payments are processed and any issues are resolved in accordance with the Authority's KPI's and the Buyers Service Levels	M	M
4.3. Supplier shall state which Payment Gateways they currently support (interface to) in addition to the Supplier's Payment Gateway and which terminal protocols they support and whether they will allow interface to those Payment Gateways on a reasonable and non-discriminatory basis.	M	M
4.4. The Supplier shall ensure that the following payment cards can be accepted (but will not be obliged to use) according to <b>ALL CURRENT AND FUTURE MANDATED CARD SCHEME RULES</b> for the Merchant Card Acquiring Services for all card types (e.g. credit, debit, prepaid, commercial, consumer, domestic and cross border) for the following schemes:	M	M
4.4.1. Visa (including Electron, VPay etc.)	M	M
4.4.2. MasterCard (including Maestro etc.)	M	M
4.4.3. American Express	M	M
4.4.4. Diners Club/ Discover	M	M
4.4.5. JCB	O	M
4.4.6. China Union Pay, Union Pay International/UPOP.	O	M

4.5. The Supplier shall work with the Buyers as required by the Buyer and Supplier's Payment Gateway to agree their implementation plan or plans if appropriate to transition any existing Merchant Card Acquiring Equipment to connect to Supplier's Payment Gateways or other Payment Gateway as allowed under 4.3 above.	M	M
4.6. The Supplier shall provide, maintain and update all of the hardware and software required to facilitate the acceptance of payments through the Merchant Card Acquiring Equipment required by the Buyers.	M	M
4.7. The Supplier shall provide replacements for faulty Merchant Card Acquiring Equipment within service levels specified in Annex A – Minimum Service Level Performance Criteria.	M	M
4.8. Supplier shall state whether they use 3 <sup>rd</sup> party maintainers and if so which.	M	M
4.9. The Supplier shall be capable of securely storing, for 7 years, and Supplier shall state whether such storage is available in real time or near real-time or on a batch basis, and in accordance with PCI-DSS, all Equipment data such as logs of maintenance and encryption key data processed for and on behalf of the Buyers and the Supplier shall provide a mechanism for deletion of specified data according to GDPR legislation as updated from time to time.	M	M
4.10. The Supplier shall inform the Buyers in accordance with their Service Levels, of any issues or incidents affecting their Merchant Card Acquiring Equipment and the issue response standard is given in Annex A – Minimum Service Level Performance Criteria or level 1 issues (Buyer unable to transact) and Supplier shall state their expected resolution times for level 1 issues and shall state their other issue levels with expected response and resolution times.	M	M
4.11. The Supplier shall inform the Buyers of new payment innovations and methods that become available and make such innovations and methods available to the Buyers in order that they can be implemented by the Buyers if required, including, but not necessarily limited to:	M	M
4.11.1. New terminal types and capabilities	M	M
4.11.2. Tokenisation	O	M
4.11.3. Software only acceptance solutions	O	M
4.11.4. Referral	O	M
4.11.5. Digital currencies	O	O
4.11.6. Other	O	O

4.12. The Supplier shall ensure the Buyers can decide which payment cards in 4.4 above can be accepted and processed at any time, to ensure that the Buyers adhere to their policies regarding the type of payments that can be accepted and processed.	M	M
4.13. The Supplier shall ensure there is a separation of each Buyer's equipment data and that of any other merchants to avoid exposing each Buyer's data to unauthorised parties.	M	M
<b>MERCHANT CARD ACQUIRING EQUIPMENT</b>		
4.14. Where required, the Supplier shall provide the Buyers with POS and MPOS equipment, or equivalent, and connect to the Supplier's Payment Gateway Services providers or Payment Gateways as allowed under 4.3 above to facilitate Cardholder Present and Cardholder Not Present Transactions, including Refunds and other standard card scheme transactions types, using Chip and PIN and Contactless technology at designated locations in the UK and globally e.g. UK Military bases abroad, including third party locations and mobile teams The choice of equipment shall include, but shall not necessarily be limited to :	M	M
4.1. Fixed Terminals	M	M
4.2. Mobile Terminals (GSM connectivity)	M	M
4.3. PDQ Terminals	O	O
4.4. Bluetooth Terminals	O	O
4.5. Customer Activated Terminals	O	O
4.6. Wireless Terminals	O	O
4.7. Remote Wireless Terminals	O	M
4.8. Unattended or semi-attended Terminals	O	M
4.9. Portable Terminals (WiFi connectivity)	O	O
4.10. MPOS equipment.	O	O
4.11. Smarts (with cashdrawer, scanner, printer etc.)	O	O
4.12. Software only terminals (when standards from certification bodies allow such as EMVCo, and PA/PCI DSS allow)	O	O
4.13. Other.	O	O
4.14. Point-to-point accredited terminal solutions.	O	O
4.15. Electronic equipment shall be tamper proof, tamper evident and encryption keys shall be invalidated on tampering.	M	M
4.16. Support for a variety of integration types including but not necessarily limited to, with appropriate security including Point to Point Encryption where appropriate:	M	M
4.16.1. Standalone	M	M
4.16.2. Integrated	O	M
4.16.3. Semi-integrated	O	M

4.16.4. Other.	O	M
4.17. The Merchant Card Acquiring Equipment shall have the functionality, where required, to connect to the Supplier's Payment Gateway Service providers or Payment Gateways as allowed under 4.3 above so Buyers are not necessarily required to invest in a bespoke network or new infrastructure to facilitate the Supplier's Merchant Card Acquiring Services or Merchant Card Acquiring provider as allowed under 3.4 above via Supplier's Payment Gateway Services. or Payment Gateways as allowed under 4.3 above and Merchant Card Acquiring Equipment connectivity shall cover, but shall not necessarily be limited to:	M	M
4.17.1. Internet connection	M	M
4.17.2. Any emerging connectivity of sufficient security and capacity	M	M
4.17.3. Broadband	O	O
4.17.4. GPRS	O	O
4.17.5. Wireless	O	O
4.17.6. Satellite communication facilities	O	O
4.17.7. Other.	O	O
4.18. Where required, the Supplier shall provide Buyers with POS and MPOS equipment, or equivalent, at the Buyers' UK and global sites, including at permanent UK bases globally and potentially on-board UK ships.	O	M
4.19. The Supplier shall ensure with Supplier's Payment Gateway Service or Payment Gateways as allowed under 4.3 above that any industry changes to contactless threshold values are applied to all Buyer Merchant Card Acquiring Equipment free of charge and are available with immediate effect in line with the industry launch and go-live date.	M	M
4.20. If the Supplier and a Buyer agree the need for manual imprinter terminals, the Supplier shall ensure that all data on its Till Rolls, Sales Vouchers and copy Sales Vouchers are consistently clear and easily readable.	M	M
4.21. The Supplier shall enable the Buyers to use their own banking industry approved Till Rolls and Sales Vouchers.	M	M
4.22. The Supplier shall be able to supply and manage the supply of standard Till Rolls and Sales Vouchers.	M	M
<b>PAYMENT GATEWAY SET-UP</b>		

4.23. Supplier will assist with acquirer certification, configuring relevant terminal identifiers encryption key loading and connectivity to Supplier's Payment Gateway Service providers or Payment Gateways as allowed under 4.3 above as required by Supplier's Merchant Card Acquiring Service or Merchant Card Acquiring Service as allowed under 3.4 above.	M	M
<b>TAKING &amp; PROCESSING PAYMENTS &amp; SETTLEMENT</b>		
4.24. When each Transaction is processed, the Merchant Card Acquiring Equipment shall facilitate authorisation of Transactions to provide Buyers with a response indicating the status of each Transaction submitted, including all details on the codes as allowed under card scheme rules, including, but not necessarily limited to;	M	M
4.24.1. Approve	M	M
4.24.2. Decline	M	M
4.24.3. Refer	O	M
4.24.4. Decline and pick up	O	M
4.24.5. Other.	O	O
4.25. The Supplier shall ensure that for each unique Transaction reference, payment is only taken once enabling Buyers to notify the Payer accordingly with a customisable message written by the Buyer in agreement with the Supplier.	M	M
<b>SETTLEMENT</b>		
4.26. The Supplier will assist as required Supplier's Payment Gateway Service and any Payment Gateways as allowed under 4.3 above with configuring equipment to initiate end of day procedures or single message transaction submission when this becomes an industry standard.	M	M
4.27. The Supplier shall provide Buyers with standard terms of 30 days for payments of fees and charges, with the Supplier offering prompt payment discounts for earlier settlement	O	O
<b>FOREIGN CURRENCY TRANSACTIONS</b>		
4.28. The Supplier shall provide the Buyers with equipment which does not inhibit multiple Acceptance currencies.	M	M
4.29. The Supplier shall provide the Buyers with equipment that does not inhibit special processing as required for Dynamic Currency Conversion or equivalent particularly as regards to special receipt printing.	M	M

REPORTING and INVOICING (ADDITIONAL)		
4.30. Additional Supplier reporting will relate to locations of equipment, age, maintenance due dates, hot stock held at locations, stock held at Supplier locations, fault reporting analysis, tamper evidence and other details to be determined.	M	M
4.31. The Supplier shall provide an accurate invoice in Gross GBP Sterling to the Buyer in their choice of paper or electronic format including line item detail for, but not necessarily limited to:	M	M
4.31.1. Standard maintenance charges	M	M
4.31.2. Supplies e.g. till rolls	M	M
4.31.3. Out of hours call outs	M	M
4.31.4. Other.	O	O
CUSTOMER SERVICE AND SUPPORT		
4.32. The Supplier shall provide maintenance, installation and swap services for the equipment provided to Buyers, considerations are, but not necessarily limited to:	M	M
4.32.1. UK and overseas including on-board ship	M	M
4.32.2. PCI-DSS requirements including key management	M	M
4.32.3. Same day response	M	M
4.32.4. Non-same day response	M	M
4.32.5. Hot swap stock kept at Supplier locations	M	M
32.6. Spare stock kept at Merchant Card Acquiring Equipment providers premises – single or multiple locations	M	M
4.32.7. Procedures and processes for swapping equipment – PCI-DSS considerations	M	M
4.32.8. Other.	O	O
4.33. The Supplier shall provide <b>support</b> to the Buyers and where applicable Supplier's Payment Gateways or Payment Gateways as allowed under 4.3 above within an agreed timetable and specific times of each day, month and year as specified in Annex A – Minimum Service Level Performance Criteria and including, but not necessarily limited to:	M	M
3.1. Supply of hardwired Payment Acceptance Terminals (including Contactless)	M	M
3.2. Supply of wireless Payment Acceptance Terminals (including Contactless)	M	M
3.3. Supply of Bluetooth Payment Acceptance Terminals (including Contactless)	O	O
3.4. Incident management	M	M
3.5. Reporting files and systems	M	M
3.6. Technical support and incident management	M	M
3.7. Interaction and support with third party suppliers	M	M

3.8. A dedicated business and technical helpdesk for in and out-of-hours telephone or email queries/issues	M	M
3.9. System availability	O	O
3.10. Other.	O	O
4.34. The Supplier shall provide Buyers with a dedicated customer service team for queries in order to ensure effective running of the Merchant Card Acquiring Equipment service.	M	M

## 5 FRAUD AVOIDANCE

This section sets out the Services Requirements that the Supplier shall be required to fulfil when providing Fraud Avoidance Services.

	Framework Level	Government Banking Level
<b>FRAUD AND RISK MANAGEMENT CORE</b>		
5.1. The Supplier shall provide the Authority with detailed information and standards on how fraud and risk assessment and management is and shall be managed by the Supplier for Buyers within the context of the requirements below.	M	M
5.2. The Supplier shall work with the Buyers to reduce fraud and ensure they take steps to reduce the incidents of fraud and/or money laundering via their service.	M	M
5.3. Where required by Buyer an assessment of Fraud rates will be made at the beginning of the contractual arrangement with the Supplier and fraud reduction targets will be agreed – thereafter Fraud rates will be assessed at regular Supplier and Buyer reviews and Action plans developed to further reduce Fraud rates.	O	O
5.4. The Supplier shall provide Buyers with transaction risk assessment services that will enable Buyers to monitor and assess the associated risk of each transaction as requested by Buyers on a transaction by transaction <b>optional</b> basis.	M	M
5.5. Risk assessment shall be provided by Supplier either pre-authorisation or post-authorisation or not at all at Buyers option, by Merchant Card Acquiring Service providers or Payment Gateway Service providers, as requested by Buyers on a transaction by transaction optional basis.	M	M
5.6. Buyers may require Merchant Card Acquiring Service providers or Payment Gateway Service providers to interface to an independent third-party fraud mitigation tool and interface to the third-party tool shall be either pre-authorisation or post-authorisation or not at all as requested by Buyers on a transaction by transaction optional basis.	O	O
5.7. Buyers may additionally use a third-party fraud mitigation tool independent of Supplier, instead of Supplier risk assessment services. Suppliers shall ensure Buyers are able to <b>use a third-party fraud mitigation tool independent of Supplier.</b>	M	M

	Framework Level	Government Banking Level
5.8. The Supplier's fraud management tools shall apply to all payment card types accepted by the Buyer and across all channels used by the Buyer.	M	M
5.9. The Supplier shall state whether their fraud management tools are able to be applied to Alternative Payment Methods (APMs as in 3.9 above), DDs, FPS etc. accepted by the Buyer and across all channels used by the Buyer.	M	M
<b>TELEPHONE COMMUNICATION.</b>		
5.10. The Supplier shall agree a process with Buyers and Buyer Payment Gateways for communicating via telephone, with an agreed telephone authentication process to ensure that all calls made are from genuine employees of the Buyer and Supplier, who have been approved to speak with the other party.	M	M
<b>STANDARD ONLINE and MOBILE CARD SECURITY SERVICES.</b>		
5.11. 3D Secure. The Supplier shall provide for access to merchant 3D Secure 1.0 and EMVCO 3-D Secure 2.2 as amended or replaced from time to time or equivalent on a card-based transaction by transaction optional basis as requested by the Buyer.	M	M
5.12. The Supplier shall apply all SCA exemptions, where allowed, on transactions and shall specify to the Authority how they take advantage of the SCA exemptions allowed under PSD2	M	M
5.13. CSC (Card Security Code) validation on a card-based transaction by transaction optional basis as requested by the Buyer.	M	M
5.14. AVS (Address Verification Service) validation on a card-based transaction by transaction optional, and where relevant to territory, basis as requested by the Buyer.	M	M
<b>TRANSACTIONAL PAYMENT RISK MANAGEMENT.</b>		
5.15. Supplier and/or third-party risk assessment services will have access to complete transaction and Payer data and Payer device signature as known to the Buyers at the time of the transaction.	M	M
5.16. Risk assessment will make use of industry standard sources but not necessarily limited to:	M	M

	Framework Level	Government Banking Level
5.16.1. Current lists of fraudulent and stolen cards (updated by Issuer fraud alerts).	M	M
5.16.2. Card issuers sourced data	O	O
5.16.3. BT OSIS	O	O
5.16.4. CIFAS	O	O
5.16.5. Electoral roll	O	O
5.16.6. Death records	O	O
5.16.7. Sanctions	O	O
5.16.8. PEP	O	O
5.16.9. Issuing country	O	O
5.16.10. Credit activity	O	O
5.16.11. IP address details	O	O
5.16.12. email validation	O	O
5.16.13. Other.	O	O
5.17. Supplier risk assessment shall make use of third-party value added services as required by the Buyer, such as those provided by but not necessarily limited to	O	O
5.17.1. Telesign	O	O
5.17.2. Ethoca	O	O
5.17.3. GBGroup	O	O
5.17.4. Threatmetrix	O	O
5.17.5. 192	O	O
5.17.6. Other.	O	O
5.17.7. Comprehensive Rule based processing will be included, but will not necessarily be limited to	M	M
5.17.8. Score against velocity (volume and value), block list, white list, pattern analysis, computed values	M	M
5.17.9. Applied to all transaction data and Payer data and Payer device signature (device used to attempt payment) such as, but not limited to, field values, grouped values, concatenated values, wild carded values and historical data relating to that data	O	O
5.17.10. Capable of rules being applied to groups of transaction data, Payer characteristics and Payer device signature e.g. domestic vs international, and operate hierarchically	O	O
5.17.11. Capable of champion/challenger strategies	O	O
5.17.12. Capable of being scheduled for activation or deactivation.	O	O
5.17.13. Other.	O	O
5.18. Supplier's rule outcome shall yield a weighted risk score to which will be used to provide an indicator to the Buyer see 5.20 below).	M	M

	Framework Level	Government Banking Level
5.19. Supplier shall state whether they can utilise inference engines and or machine learning to contribute to risk score.	O	O
5.20. Supplier shall return the risk score to the Buyer with an indicator – Approve, Decline, Challenge based on score banding set by the Buyer.	M	M
5.21. Challenge transactions shall be added to a case management system which can be accessed by Buyers via a web-based interface or by secure, API to manually review the transaction and the reason behind the challenge and change the Challenge to Approve (with Buyer assuming the risk) or Decline.	M	M
5.21.1. APIs shall be RESTful	O	O
5.22. Buyer will be able to require Supplier to rescore transactions e.g. if shipping address changes.	O	O
5.23. Buyer will be able to require Supplier to force Approve (with Buyer assuming the risk) a transaction.	M	M
5.24. Buyer will be able to set silent rules which are non-operational but will functionally test an alternative outcome.	M	M
5.25. Buyer will be able to run transactions in test mode against alternative rules to determine alternative outcomes.	M	M
<b>MANAGEMENT</b>		
5.26. The Supplier shall provide a web-based interface and a well-documented synchronous secure API to enable Buyers to query the current fraud status of any Transaction based on a Buyer's unique or custom identifiers for that Transaction, in order that the Buyer can retrieve up to date details of Transactions whose status may have changed.	M	M
5.26.1. APIs shall be RESTful	O	O
5.27. Rules shall be capable of amendment by Buyer via a web-based interface and/or secure API and/or batch upload.	M	M
5.27.1. APIs shall RESTful	O	O

	Framework Level	Government Banking Level
5.28. The Supplier shall provide Buyers with the functionality to update rules values and weighting from locally held automated risk assessment and monitoring systems and/or dynamically update risk scores via a web-based interface and/or secure API and/or batch upload.	M	M
5.28.1. APIs shall be RESTful	O	O
5.29. The Supplier shall provide the capability to update and manage the Buyers' Watch, Block and White Lists with shared fraud data derived from third parties, via a web-based interface and/or secure API and/or batch upload, including, but not necessarily limited to;	M	M
5.29.1. Shared financial intelligence sources	M	M
5.29.2. Other merchant acquiring services	O	O
5.29.3. Other Government Departments	O	O
5.29.4. Other.	O	O
5.30. Where Watch, Block Lists and shared fraud data updates are provided, the Supplier shall provide the Buyers with contextual information indicating the source of the intelligence and reason for inclusion.	M	M
5.31. Where the Supplier detects unusual patterns of activity that might indicate malicious activities, for example a spike in numbers of potentially fraudulent Transactions the Supplier shall inform the Buyer's designated security contact immediately by alerting via email and SMS.	M	M
5.32. The Supplier shall provide the Buyers with incident reporting and enable investigation with real-time lookup, research and export of selected data sets relevant to a specific event or events across one, many or all of a Buyer's accounts for any reason including to answer any Freedom of Information Act (FOIA) or GDPR request and these reports shall be accessible via secure website and downloadable in an agreed format by SFTP and other agreed mechanisms.	M	M
5.33. The Supplier shall provide the Buyer with access to a comprehensive range of management information about the performance and efficacy of the fraud and risk management system.	M	M
5.34. Fraud data transaction history shall be retained for seven years, and the Supplier shall state whether such storage is available in real-time, near real-time or on a batch basis, and the Supplier shall provide a mechanism for deletion of specified data according to GDPR legislation as updated from time to time.	M	M

	Framework Level	Government Banking Level

## 6 ADDITIONAL MANDATORY AND GOVERNMENT BANKING SPECIFIC REQUIREMENTS

This section sets out the Mandatory Requirements that the Supplier shall be required to fulfil when providing Services.

These requirements (e.g. reporting, compliance, set-up) which are applicable to all other sections and SHALL be included with any previous sections.

	Framework Level	Government Banking Level
<b>BUSINESS CONTINUITY</b>		
6.1 The Supplier shall ensure that in the event of failure, the Supplier shall maintain failover capacity and data storage processes and Help desk support to effect a failover or disaster recovery operation.	M	M
6.2 The Supplier shall ensure a robust business continuity and disaster recovery plan is in place for all Services and shall be able to demonstrate disaster recovery to ensure continuity of the Services APMs without loss, as and when required by the Authority or a Buyer.	M	M
6.3 The Supplier shall provide the business continuity and disaster recovery plan to the Authority as part of the initial assessment process and this will be reviewed between the Supplier and the Authority. on a yearly basis or the business continuity and disaster recovery plan shall be certified by Supplier's External Auditors as part of the initial assessment process and on a yearly basis as fit for purpose to enable Supplier to meet its obligations to Buyer	M	M
6.4 The Supplier shall ensure that in the event of disaster recovery, connectivity between the Buyers and the Services is maintained.	M	M
6.5 Any further Service Levels for failover are contained in Annex A – Minimum Service Level Performance Criteria	M	M
<b>AUTHORITY REQUIREMENTS</b>		

	Framework Level	Government Banking Level
6.6 The Supplier shall contractually provide dedicated expert technical consultancy, to work with the Authority and the Buyers to support the government's strategy to improve its capabilities in the area of electronic purchasing and payment, and to encourage and assist Buyers to move away from traditional payment acceptance methods (cash/cheque) where appropriate, and move towards greater use of new technology that can be utilised to increase electronic receipt of payments through Card and APM payments.	M	M
6.7 The Supplier shall make transparent any process by which volume based pricing tiers are reset e.g. monthly/yearly	M	M
<b>TRAINING</b>		
6.8 The Supplier shall provide, within agreed limits, initial and on-going training free of charge to the Authority and Buyers on how to use the Services including any management tools and shall provide updated guidance documents as and when required, free of charge, to the Authority and the Buyers.	M	M
6.9 As and when required, the Supplier shall provide the Buyers, within agreed limits, free training on the use of any of the Services implemented by the Buyers, including e-training for the Buyers and Supplier shall state any constraints on such provision.	M	M
<b>TESTING and CERTIFICATION</b>		
6.10 The Supplier shall provide where relevant to the Supplier's services and where integration is required between Buyers, Supplier's Services and Buyers other providers, a sandbox environment for the Buyers and the Buyers other providers to allow for production-like testing of integrations, including the use of any identifiers that are in use for the production environment and to allow for penetration testing to verify the end-to-end security of the integrated and test accounts shall be set up within timetables specified in Annex A – Minimum Service Level Performance Criteria	M	M

	Framework Level	Government Banking Level
6.11 The Supplier shall provide a facility, where relevant to the Supplier's services, whether in the normal testing sandbox environment or another replica environment for the Buyers to run where relevant to the Supplier's Services realistic end-to-end performance and capacity testing to allow the Buyers to prepare before launching a new service and/or before a period of peak demand of Services users in the UK and abroad.	M	M
6.12 Supplier shall provide Certification testing facilities, and assistance with Certification, where relevant to the Supplier's Services between Buyers and Buyers other providers.	M	M
<b>WEB BASED ACCESS</b>		
6.13 Supplier web-based interfaces provided to the Authority and Buyers shall require secure two factor authentication role and privilege-based access.	M	M
6.14 Supplier web-based interfaces provided to the Authority and Buyers shall conform to WCAG 2.0 Level AA guidelines and standards and conform to UK Equality Act (2010) legislation as updated from time to time.	M	M
<b>SUPPORT</b>		
6.15 The Supplier shall provide Buyers with a dedicated business and technical helpdesk with a Service Level as specified in Annex A – Minimum Service Level Performance Criteria here relevant to the Services, but not necessarily limited to, and Supplier shall state any constraints on such provision:	M	M
6.15.1 Incidents	M	M
6.15.2 Problems	M	M
6.15.3 Alerts	M	M
6.15.4 Account queries	O	M
6.15.5 Invoice queries	O	M
6.15.6 Payer queries	O	O
6.15.7 Software	O	O
6.15.8 Hardware	O	O
6.15.9 Other.	O	O

	Framework Level	Government Banking Level
6.16 The Supplier shall ensure that all invoices and account payment queries received from the Buyers are resolved in accordance with the Buyers' agreed Service Levels	M	M
6.17 The Supplier shall ensure that if Buyers change Payment Acceptance provider or providers they shall work with the Buyers in supporting, where relevant to the Supplier's Services, the new provider in order that operational change is efficient and payment Transactions can occur uninterrupted and are all reconciled and settled.	M	M
6.18 The Supplier shall provide a named account manager for all accounts processing 1 million Transactions per annum and above. Where the account is less than 1 million Transactions, account management shall be appropriate to the size of the Buyers' specific requirements and strategic nature of the Buyers.	M	M
6.19 The Supplier shall provide Buyers with a dedicated customer service team for queries in order to ensure effective running of the Services.	M	M
<b>COMPLIANCE – STANDARDS and REGULATIONS</b>		
6.20 The Supplier shall ensure the Services provided to the Buyers comply with the current version of the Payment Cards Industry Data Security Standard (PCI-DSS) and all Supplier, or partner, systems and facilities are certified as Level 1 compliant with a RoC by a Qualified Security Assessor.	M	M
6.21 The Supplier shall ensure the payment processing software delivered under the Services provided to the Buyers comply with the current version of PA-DSS.	M	M
6.22 The Supplier shall ensure the payment processing software delivered under the Services provided to the Buyers comply with any and all requirements under PSD2 – the 2nd Payment Services Directive.	M	M
6.23 Upon the commencement of the Framework Agreement, and on an annual basis (as a minimum), and following any major system change, the Supplier shall provide the following information assurance evidence to the Authority:	M	M

	Framework Level	Government Banking Level
6.23.1 Evidence, in the form of independent certification, that the Services provided conform to PCI-DSS, and evidence of any other claimed security measures, or equivalents, and security controls implemented	M	M
6.23.2 Evidence of an independent IT health check using a CESG approved check service provider.	O	O
6.24 The Supplier shall provide the same information assurance evidence specified at 6.23 above to Buyers at regular intervals and upon request.	M	M
6.25 The Supplier's information security management system (relevant to the Services) shall be accredited to ISO27001(2013) or demonstrably compliant with relevant measures therein contained:	M	M
6.26 If the Supplier's information security management system (relevant to the services) is accredited to the ISO27001(2013) Standard, or equivalent, or the Supplier can demonstrate compliance with the relevant ISO27001(2013) measures, the Supplier is required to provide evidence of this accreditation and compliance to the Authority and Buyers at regular intervals and upon request.	M	M
6.27 The Supplier shall ensure the Services provided are maintained to the current standards set by PCI-DSS, PA-DSS, Payment Services Regulations, UK Cards Association, EMVCO, operate within the current rules of the Card Schemes and APM providers, GDPR, The UK Equality Act (2010) and WCAG 2.0 level AA guidelines and conform to other relevant UK legislation that may be applicable in certain circumstances and as amended and updated and enhanced from time to time.	M	M
6.28 The Supplier shall provide the Buyers with current information detailing the Buyers' PCI-DSS responsibilities and shall work with the Buyers to ensure that the Buyer is fully compliant with the current PCI-DSS Standard.	M	M
6.29 Certification to either Cyber Essentials or Cyber Essentials Plus is mandatory and the Supplier shall state when they were awarded certification.	M	M
<b>MONITORING</b>		

	Framework Level	Government Banking Level
6.30 The Supplier shall provide the Buyers with the functionality to monitor Supplier's availability, transaction completion rates and Transaction timings.	O	O
6.31 The Supplier shall provide the Buyers with management reporting functionality which includes the ability to report on Transaction monitoring events across one, many and/or all of a Buyer's accounts.	M	M
6.32 The Supplier shall provide the Buyers with the option to manage the Transaction monitoring services via a secure web-based interface hosted by the Supplier and remotely accessible to the Buyers.	M	M
6.33 Where required the Supplier shall provide the Buyers with remote access to the functions of the transaction monitoring service for consumption within locally held transaction monitoring platforms including, but not necessarily limited to:	M	M
6.33.1 Report out in real time	M	M
6.33.2 Alerts	M	M
6.33.3 Associated contextual transaction meta data.	O	O
6.33.4 Other.	O	O
6.34 Where required, the Supplier shall allow Buyers to subscribe to an appropriately secured real-time feed of transaction status information to receive updates, including, but not necessarily limited to:	O	O
6.34.1 Transactions processed	O	O
6.34.2 Transactions scored for fraud.	O	O
6.34.3 Transactions not scored for fraud	O	O
6.34.4 Other	O	O
6.35 Where the Supplier detects unusual patterns of activity that might indicate malicious activities, for example a denial of service attack or distributed denial of service attack the Supplier shall inform the Buyer's designated security contact immediately by alerting via email and SMS.	M	M
<b>REPORTING and INVOICING</b>		
6.36 The Supplier shall provide a comprehensive range of standard reports which shall be clear and easy to understand, with Buyers able to specify the reporting hierarchy and a method of producing ad-hoc reports. Not all reports are required from each Supplier type (Merchant Card Acquiring, Payment Gateway, Merchant Card Acquiring Equipment).	M	M

	Framework Level	Government Banking Level
6.37 The Supplier shall ensure that an online system to manage Transaction data is provided to the Buyers, and that it has no limitations on the volumes of data and reports that can be downloaded, so the Buyers can download the information they require.	M	M
6.38 The Supplier shall ensure that Buyers can securely access any provided reports (which includes statements, electronic billing and invoices) by, but not necessarily limited to:	M	M
6.38.1 HTTPS API	M	M
6.38.2 Secure File Transfer Protocol (SFTP)	M	M
6.38.3 Secure email.	O	O
6.38.4 Other.	O	O
6.39 The Supplier shall provide the Buyers with the facility to produce, download and export reports so the Buyers can manage their payment processes in the following formats where appropriate, including, but not necessarily limited to:	M	M
6.39.1 Excel	M	M
6.39.2 Comma Separated Values (CSV)	O	M
6.39.3 Space delimited	O	O
6.39.4 Comma delimited	O	O
6.39.5 Text format (XML)	O	O
6.39.6 PDF	O	O
6.39.7 SWIFT	O	O
6.39.8 BAI.	O	O
6.39.9 Other.	O	O
6.40 The Supplier shall provide Buyers with payment data and the facility to produce, download and export statements and reports so that Buyers can manage their payment processes. The statements and reports shall contain, but are not necessarily limited to, the following fields (or a selection):	M	M

	Framework Level	Government Banking Level
6.40.1 CID	M	M
6.40.2 MID	M	M
6.40.3 TID	O	O
6.40.4 The Buyer Payer identifier	O	O
6.40.5 The Buyer Transaction description reference	O	O
6.40.6 Payer transaction description reference	O	O
6.40.7 Payer details	O	O
6.40.8 Payer device signature	O	O
6.40.9 Services purchased	O	O
6.40.10 Reason code	O	O
6.40.11 Auth code	O	O
6.40.12 CVM details	O	O
6.40.13 3DS response code and signature	O	O
6.40.14 AVS response code	O	O
6.40.15 Fraud score	O	O
6.40.16 Fraud indicator	O	O
6.40.17 Chargeback annotation and reason	O	O
6.40.18 Status (authorised/cleared/settled/chargeback)	O	O
6.40.19 Payment details (card details/APM details)	O	O
6.40.20 Gross amount of payment	O	O
6.40.21 Gross amount of refund or chargeback	O	O
6.40.22 Posting date	O	O
6.40.23 Transaction date	O	O
6.40.24 Interchange fee	O	O
6.40.25 Description of Transaction	O	O
6.40.26 Currencies	O	O
6.40.27 Time (hours:minutes:seconds:milliseconds)	O	O
6.40.28 Gross value	O	O
6.40.29 Value Added Tax (VAT)	O	O
6.40.30 Level 3 data supplied by Card Schemes for Corporate reconciliation e.g. from travel and entertainment sector	O	O
6.40.31 Other.	O	O
6.41 The Supplier shall provide Buyers with a report of processed Transactions to enable Buyers to update their accounting and cash management systems and to provide the capability to search for individual Transactions or groups of Transactions by, but not necessarily limited to, the following fields:	M	M
6.41.1 Transaction data see 6.40 above.	M	M
6.41.2 Summary at various levels including but not limited to, – CID, MID, TID, Payment types (card/APM types), Gross payments/Gross refunds	M	M
6.41.3 Other.	O	O

	Framework Level	Government Banking Level
6.42 The Supplier shall provide Buyers with the report in 6.41 above at various time intervals including but not limited to intraday (ad-hoc), end of day (by 07.00 on the next day), end of month, quarterly and annual.	M	M
6.43 The Supplier shall provide an accurate invoice in Gross GBP Sterling to the Buyer detailing card scheme interchange fees, scheme fees, APM fees and Supplier fees. Where an electronic invoice is provided, with a full breakdown of any fees and charges, including line item detail for, but not necessarily limited to the data in 6.40 above (or a selection).	M	M
6.44 Supplier shall validate interchange fees, for all card transactions, charged by card schemes.	M	M
6.45 The Supplier shall provide Buyers with access to an online system to provide real-time access to view all card/Alternative Payment Method Transactions, including, but not necessarily limited to the transaction data in 6.40 above.	M	M
6.46 The Supplier shall ensure that any online reporting system provided to Buyers does not limit the number and type of reports that can be generated and/or downloaded in any given period, or the number of times the Transaction status can be queried via a web interface or API.	M	M
6.47 The Supplier shall ensure Buyers are able to obtain, at any time, an accurate real-time view of their Merchant Card Acquiring Services and APM payments.	M	M
6.48 The Supplier shall provide Buyers with online access to a report, or provide a report in accordance with the Buyers' delivery methods and frequencies, with details including, but not necessarily limited to:	M	M
6.48.1 Declined Transactions	M	M
6.48.2 Lost Transactions	O	O
6.48.3 Abandoned Transactions	O	O
6.48.4 Drop offs	O	O
6.48.5 Other.	O	O
<b>PRICING</b>		

	Framework Level	Government Banking Level
6.49 Simple, transparent, easy to reconcile.	M	M
6.50 Annual audit, at Supplier's cost at a framework rather than Buyer level	M	M
6.51 Rate card for all Supplier services clearly stating under what conditions each charge will apply.	M	M
6.52 Supplier may provide some additional and optional services on chargeable basis, which shall be clearly defined.	O	O
<b>ONBOARDING</b>		
6.53 The Supplier shall provide mechanisms for onboarding Buyers which are appropriate to the Buyer size, technical sophistication and desire for speed and simplicity.	M	M
6.54 In the event of termination for any reason of supply of services which Supplier is providing to any Buyer then Supplier shall provide a simple mechanism for Buyer to obtain access to all past and current data held by Supplier pertaining to Buyer and all past and current data pertaining to Buyer's customers including but not limited to past or in-flight transaction data as required by Buyer free of charge and Supplier will provide necessary technical assistance to achieve this in a timescale that does not exceed that set by the termination mechanism or agreement and any such data shall be in a format which is machine readable and if encrypted or tokenised can be decrypted or detokenised either by Supplier prior to delivery to Buyer or on receipt by Buyer	M	M

## **PRICE MODELS, REBATES & INVOICING**

6.55 REDACTED

6.56 REDACTED

6.57 REDACTED

6.58 REDACTED

6.59 REDACTED

6.60 REDACTED

6.61 REDACTED

6.62 REDACTED

6.63 REDACTED

6.64 REDACTED

6.65 The Supplier shall issue invoices directly to the Government Banking Customer. Services shall be invoiced on a calendar month basis in arrears and must show the following as a minimum:

6.65.1 Volumes i.e. Sales, Refunds

6.65.2 Turnover i.e. Value of Sales, Refunds

6.65.3 Card Processing Fees – Interchange++ or Blended

6.65.4 Additional Fees – PoS Terminal Fees, Gateway

6.65.5 Scheme types i.e. Visa, Mastercard

6.65.6 Card type i.e. Consumer Debit, Commercial Debit (including pre-paid), Commercial Credit and Personal Credit

6.65.7 Issuers Region i.e. UK Domestic, EU, Rest of World

6.66 The Supplier will provide the following free of charge: projects, training, consultancy, changes (legislative and non-legislative).

## **UK VISAS AND IMMIGRATION (UKVI) PRICING**

6.67 REDACTED

6.68 REDACTED

6.69 REDACTED

6.70 REDACTED

## **SETTLEMENT**

6.71 The Supplier must keep Government Banking Customers' data separate from other organisations' data, to ensure there is no delay in processing transactions and monies reaching bank accounts in the agreed timescales.

- 6.72 Under no circumstances must settlement into Government Banking Customers bank accounts be delayed or fail because of issues with another client's data.
- 6.73 Settlement into the agreed Government Banking Customers bank accounts must be made at the latest on Working Day 3, (T+2). T = Transaction date i.e. when remitter makes payment (Working Day 1).
- 6.74 The Supplier will inform Government Banking (nominated persons) immediately if pay-over of settlement is not possible, or will be significantly delayed, and confirm by email, detailing actions they will take to rectify the situation.

## **PCI-DSS SUPPORT**

- 6.75 The Supplier shall provide a service to support Government Banking Customers with their PCI-DSS reporting

## **SCA EXEMPTIONS**

- 6.76 The Supplier will provide a solution to ensure low-risk transactions can be exempt or excluded from Secure Customer Authentication (SCA) checks.

## **VISA ME TO ME**

- 6.77 The Supplier must support eligible Government Banking Customers with the registration for the Visa Me to Me programme.

## **RECONCILIATION OF SETTLEMENTS**

- 6.78 The Supplier will provide settlement data to the Government Banking Customer to include at least all debits and credits and any other information as agreed between the Supplier and the Government Banking Customer before 07:00 UK time.
- 6.79 In addition to the reconciliation files, the Supplier must provide Government Banking and Government Banking Customers with online real-time access to view all acquiring transactions by MID and/or Company ID. The data must also include details of all refunds and chargebacks.
- 6.80 All card and APM transactional data must include posting and value date, description of transaction and full reference information provided by the Payer.
- 6.81 The service must have the ability to configure and produce statements and reports containing card and APM transactions. These must be available for download and export to a variety of Government Banking Customer back office system

## **REPORTING AND PERFORMANCE MANAGEMENT**

- 6.82 The Supplier shall attend Performance Management meetings at both a Government Banking and individual Government Banking Customer level if requested.
- 6.83 Government Banking and the Supplier will meet on a monthly basis to discuss the following:

- 6.83.1 Service Performance against the Service Levels
- 6.83.2 Risks and Issues
- 6.83.3 Continuous Improvements
- 6.83.4 Industry Changes
- 6.83.5 New Services and Innovations
- 6.83.6 Contract Variations

- 6.84 The Supplier must be able to provide performance data for the Service Levels detailed in Call-Off Schedule 14 (Service Levels) at both a Government Banking whole-portfolio level. The Supplier must also be able to provide the same at individual Government Banking Customer level where required.

## **MANAGEMENT INFORMATION**

- 6.85 The Supplier must provide an online Management Information portal which grants Government Banking “Super User” rights to view and produce reports across the whole Government Banking Customer base.
- 6.86 The Management Information portal must have the ability to:
- 6.86.1 Automate reports and deliver by email
  - 6.86.2 Supply reports in agreed formats
  - 6.86.3 Hold historical data for 12 months as a minimum
  - 6.86.4 Demonstrate SCA status of payments
- 6.87 The Supplier’s Management Information portal must have the capability to produce Management Information against the headings in Annex D.
- 6.88 The Supplier’s online service must have the capability provide Government Banking Customers with the capability to search for individual transactions or groups of transactions including but not limited to:
- 6.88.1 by type of payment made (e.g. business area within Department which has received the payment - cashier, catering, pharmacy)
  - 6.88.2 by transaction type
  - 6.88.3 by card and APM type
  - 6.88.4 by transaction reference.
- 6.89 The Management Information portal must ensure the Management Information portal separates Government Banking Customer data so that they only have access to data which is relevant to them.
- 6.90 The Supplier shall provide a weekly report on the projects currently in progress.
- 6.91 The Supplier shall quarterly provide Government Banking with an up-to-date list of services used by individual Government Banking Customers including but not limited to: APMs, tokenisation, APMs, MOTO etc.
- 6.92 There may be new Management Information requirements made through the life of the contract. New management information requests shall be discussed and agreed between the Supplier, Government Banking and Government Banking Customers at the point they are identified. The Supplier shall implement these free of charge.

## **VISA DIRECT & MASTERCARD SEND**

- 6.93 The Supplier should offer “VISA Direct” and “MasterCard Send” as a method for refunding.

## NOTIFICATIONS

- 6.94 **Maintenance** - The Supplier must outline their normal maintenance schedule to Government Banking. They must notify Government Banking and affected Government Banking Customers at least 4 weeks in advance of any planned downtime for maintenance or implementation of new software/hardware in relation to the Service.
- 6.95 For any major changes to software/hardware, a longer timeframe may be required and agreed with Government Banking beforehand to ensure processing is unaffected.
- 6.96 **Industry or Legislative** - The Supplier will use best endeavours to provide advice, relevant to Government Banking and its Government Banking, on any industry or legislative changes. These changes will be done as soon as the supplier becomes aware and the Supplier will look to impact assess said changes against the service, they provide to Government Banking and its Government Banking Customers and give specific advice in relation to the changes.
- 6.97 **Changes to Services, Products or Interfaces** - The Supplier will advise Government Banking and its Government Banking Customers of any changes to services, products or interfaces potentially requiring system development / enhancements, to allow these changes to be impact assessed between twelve (12) and eight (8) weeks in advance where practical.
- 6.98 Major infrastructure/industry changes (i.e. Gateway) must be notified to Government Banking and Government Banking Customers within 12 months.
- 6.99 **Interchange and Scheme Fees** - Changes including but not restricted to Interchange and Scheme fees must be communicated as soon as they become aware of implementation for consideration and impacting by Government Banking.
- 6.100 The Supplier must give prior notice before any changes to payment flows (such as removing an APM or not accepting payments from a sanctioned country).
- 6.101 For Government Banking, all Notifications must be issued to the following email addresses:
- HMRC Commercial Team: [REDACTED]
  - Government Banking Helpdesk: [REDACTED]

## CUSTOMER SERVICE

- 6.102 The Supplier shall provide helpdesk support 24 hours per day (7 days/week/365 (6) days of the year) as per Annex A - Minimum Service Level Performance Criteria
- 6.103 When communicating with Government Banking Customers via telephone, the Supplier must follow a telephone authentication process agreed with Government Banking to ensure that all calls made by the Supplier to Government Banking Customers are from genuine employees who have been approved to speak with the Customer.

## ON-BOARDING & SET UP

- 6.104 The Supplier must be able to provide where possible a straight through processes which allows approved Government Banking Customers to onboard smoothly. If the Supplier is contacted directly by a potential Customer, their process must cover the following:

- 6.104.1 Capture relevant data (required Services, potential values & volumes, account details) from the potential Customer
  - 6.104.2 Provide Government Banking with the data collected in 6.105.1 for confirmation on their eligibility to join the Call Off Contract.
  - 6.104.3 Following confirmation of eligibility, provide Government Banking with a view on timescales, pricing model, potential Change Requests and go-live for the Customer.
  - 6.104.4 Allow Government Banking to provide the final sign off, ideally via electronic means.
- 6.105 If the Government Banking refer the Government Banking Customer to the Supplier, then 6.105.2 is deemed to have been fulfilled and the Supplier shall carry out activities according to 6.105.1, 6.105.3 and 6.105.4.

## **SECURITY**

- 6.106 The Supplier shall provide a Security Management Plan as per Call-Off Schedule 9 - Security
- 6.107 The Supplier must participate in ongoing security assurance with the Government Banking Risk and Finance team via working group meetings every six months, where the Supplier will be required to report on but not limited to:
- 6.107.1 Their Security Management Plan
  - 6.107.2 Penetration Testing and vulnerability scanning
  - 6.107.3 ISO27001 or equivalent arrangements/ audits/remediation plans
  - 6.107.4 Review Business Continuity Plans
  - 6.107.5 Security events, incident reporting, post incident reporting and investigations.
  - 6.107.6 Contract exit plan
- 6.108 Where Government Banking requires a change or enhancement to be implemented to the contract, the Supplier will use the agreed Change Request Process.
- 6.109 Where the Supplier itself requires a change or enhancement to be implemented, the Supplier shall:
- a. advise Government Banking and the affected Government Banking Customers in an appropriate time frame beforehand
  - b. explain the reasoning for the change
  - c. detail what, if anything, Government Banking or the affected Government Banking Customers might be required to do, to accommodate the change; and
  - d. give details of any system outages this change implementation may entail.
- 6.110 The Supplier must provide all changes at no additional cost.

## **SANCTIONS**

- 6.111 REDACTED

## Annex A – Minimum Service Level Performance Criteria

See Call Off Schedule 14 (Service Levels)

## Annex B – Transaction, Settlement and Potential DCC Currencies

### Transaction and Settlement Currencies

Currency description	Currency Code	Settlement Currency	Settlement Currency
United Arab Emirates Dirhams	AED	Y	GBP
Australian Dollars	AUD	Y	GBP
Bangladesh Taka	BDT	Y*	GBP
Bahraini Dinar	BHD	Y	GBP
Brazilian Brazil Real	BRL	Y	GBP
Belizean Dollar	BZD	Y*	GBP
Canadian Dollars	CAD	Y	GBP
Swiss Franc	CHF	Y	GBP
Chinese Yuan Renminbi	CNY	Y	GBP
Cube Peso Convertible	CUC	Y*	GBP
Czech Republic Koruny	CZK	Y	GBP
Danish Krona	DKK	Y	GBP
Algerian Dinar	DZD	Y*	GBP
Egypt Pound	EGP	Y	GBP
Ethiopian Birr	ETB	Y*	GBP
Euro	EUR	Y	GBP
UK Sterling	GBP	Y	GBP
Hong Kong Dollars	HKD	Y	GBP
Israeli New Shekel	ILS	Y	GBP
India Rupee	INR	Y	GBP
Jordan Dinar	JOD	Y	GBP
Japanese Yen	JPY	Y	GBP
Kenyan Shilling	KES	Y*	GBP
Korea (South) Won	KRW	Y	GBP
Kuwait Dinar	KWD	Y	GBP
Kazakhstan Tenge	KZT	Y	GBP
Lebanon Pound	LBP	Y	GBP
Moroccan Dirham	MAD	Y*	GBP
Myanmar Kyat	MMK	Y*	GBP
Mexican Peso	MXN	Y	GBP
Malaysia Ringitts	MYR	Y	GBP
Norway Krona	NOK	Y	GBP
Nepalese Rupee	NPR	Y*	GBP
New Zealand Dollar	NZD	Y*	GBP
Omani Rial	OMR	Y	GBP
Philippine Peso	PHP	Y	GBP
Pakistan Rupee	PKR	Y	GBP
Polish Zloty	PLN	Y	GBP
Qatari Riyal	QAR	Y	GBP

Romania New Lei	RON	Y	GBP
Russia Ruble	RUB	Y	GBP
South Africa Rand	SAR	Y	GBP
Swedish Krona	SEK	Y	GBP
Singapore Dollar	SGD	Y	GBP
Sierra Leonean Leone	SLL	Y*	GBP
Thailand Baht	THB	Y	GBP
Tunisian Dinar	TND	Y*	GBP
Turkey New Lira	TRY	Y	GBP
Taiwan New Dollar	TWD	Y	GBP
Ukraine Hryvnia	UAH	Y	GBP
United States of America Dollars	USD	Y	GBP
Venezuelan Bolivar	VEF	Y*	GBP
South African Rand	ZAR	Y*	GBP

\*Not included in Framework but required by UK Visas and Immigration

#### Potential DCC Card Currencies

Currency description	Currency Code	Settlement Currency	Potential Card DCC
United Arab Emirates Dirhams	AED	tbd	Y
Australian Dollars	AUD	tbd	Y
Bangladesh Taka	BDT	tbd	Y
Bahraini Dinar	BHD	tbd	Y
Brazilian Brazil Real	BRL	tbd	Y
Belizean Dollar	BZD	tbd	
Canadian Dollars	CAD	tbd	Y
Swiss Franc	CHF	tbd	Y
Chinese Yuan Renminbi	CNY	tbd	Y
Cube Peso Convertible	CUC	tbd	Y
Czech Republic Koruny	CZK	tbd	Y
Danish Krona	DKK	tbd	Y
Algerian Dinar	DZD	tbd	Y
Egypt Pound	EGP	tbd	Y
Ethiopian Birr	ETB	tbd	Y
Euro	EUR	tbd	Y
UK Sterling	GBP	GBP	Y
Hong Kong Dollars	HKD	tbd	Y
Israeli New Shekel	ILS	tbd	Y
India Rupee	INR	tbd	Y
Jordan Dinar	JOD	tbd	Y
Japanese Yen	JPY	tbd	Y
Kenyan Shilling	KES	tbd	

Korea (South) Won	KRW	tbd	Y
Kuwait Dinar	KWD	tbd	Y
Kazakhstan Tenge	KZT	tbd	Y
Lebanon Pound	LBP	tbd	Y
Moroccan Dirham	MAD	tbd	Y
Myanmar Kyat	MMK	tbd	Y
Mexican Peso	MXN	tbd	Y
Malaysia Ringitts	MYR	tbd	Y
Norway Krona	NOK	tbd	Y
Nepalese Rupee	NPR	tbd	
New Zealand Dollar	NZD	tbd	Y
Omani Rial	OMR	tbd	Y
Philippine Peso	PHP	tbd	Y
Pakistan Rupee	PKR	tbd	Y
Polish Zloty	PLN	tbd	Y
Qatari Riyal	QAR	tbd	Y
Romania New Lei	RON	tbd	Y
Russia Ruble	RUB	tbd	Y
South Africa Rand	SAR	tbd	Y
Swedish Krona	SEK	tbd	Y
Singapore Dollar	SGD	tbd	Y
Sierra Leonean Leone	SLL	tbd	Y
Thailand Baht	THB	tbd	Y
Tunisian Dinar	TND	tbd	Y
Turkey New Lira	TRY	tbd	Y
Taiwan New Dollar	TWD	tbd	Y
Ukraine Hryvnia	UAH	tbd	Y
United States of America Dollars	USD	tbd	Y
Venezuelan Bolivar	VEF	tbd	Y
South African Rand	ZAR	tbd	Y

## Annex C – Descriptions of Terms

Term	Meaning
Aggregator	An aggregated service for merchants that normally would include provision of Merchant Card Acquiring Equipment (qv), Payment Gateway (qv), Merchant Card Acquiring Services (qv) and fraud prevention services and which is most applicable to smaller, less sophisticated merchants
APM	Alternative Payment Method – alternative to payment by card e.g. Paypal, Direct Debit, iDeal, Open Banking
Acquirer	A regulated and authorised financial institution that processes credit and debit card Authorisations (qv) and transactions on behalf of a merchant including full Card Scheme (qv) members and Payment Facilitators or equivalent (which are supported by a Payment Institution)
Authorisation	Method of a merchant checking with the payer's account provider, usually via intermediate entities, that they have sufficient funds or line of credit to purchase the goods or services
Blended pricing	Where the price charged to a merchant for card transactions is aggregated into a single (or a few) rates and which hides the complexity of Interchange++ pricing (qv)
Card scheme(s)	Are payment networks linked to payment cards, such as debit or credit cards, of which a bank or any other eligible financial institution can become a member and by becoming a member of the scheme, the member then gets the possibility to Issue (an Issuer qv) or acquire (an Acquirer, qv) cards operating on the network of that card scheme which may be international in scope or limited to various sub-international jurisdictions and card schemes will levy fees for their services (not being charities)
Cardholder Not Present (CNP)	A remote card-not-present (also cardholder-not-present) purchase type (or other e.g., refund) transaction (remote purchase CNP) is one where the cardholder and the card are not present at the point-of-sale for example where the point-of-sale is the merchant's eCommerce website. Also applies to APMs (qv)
Cardholder Present (CP)	A card present (also cardholder present) purchase type (or other e.g. refund) transaction (CP) is one where the cardholder and the card are present at the point-of-sale
Clearing	Method of a merchant (or intermediate entities) presenting a request for payment, usually via intermediate entities, from the payer's account provider in settlement of the debt incurred when a payer purchases goods or services, often following a successful Authorisation(qv)
CSC	Card Security Code (the 3 or 4 digits on a card) that appear on a card (front or back) that a merchant often requires a cardholder to quote or input when making a purchase by card and this is code is also known variously as CID, CVC2, CVD, CVE, CVN2 and CVV2, but not, repeat no, CVV
DCC	Direct Currency Conversion is a method where a cardholder using a card with a normal currency of Eur (example ONLY) purchasing goods or services denominated in GBP (qv) (example ONLY) will be offered an opportunity to complete the sale in Sterling and this process applies to many cross currency sales and cards
Dispute Process	The semi-automated process of managing disputes between Issuers (qv) generally on behalf of account holders and Acquirers (qv)
Dual messaging	A payment transaction that is split into two, namely an Authorisation (qv) and a Clearing (qv) although the Authorisation is not mandatory but without this certainty of Settlement (qv) is not guaranteed
Fraud Prevention Provider	An entity that attempts to eliminate fraudulent payments acting on behalf of a merchant, Merchant Card Acquiring Service, Acquirer or Issuer or APM provider (and may be an integral part of those entities) by accumulating information about payment activity based on card activity and cardholder activity
GBP	Standard currency code for UK Sterling

HTTPS	Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol for secure communication over a computer network, and is widely used on the Internet and communication protocol is encrypted using Transport Layer Security (TLS qv)
IIN (BIN)	The Issuer Identification Number is the first six digits of a PAN (qv) and is also known as a BIN (Bank Identification Number)
Interchange ++ pricing	Where the price charged to a merchant for card transactions is disaggregated into the price applicable to the Merchant Card Acquiring Service (qv) and to which is added scheme fees and interchange fees and this method is in contrast to Blended Pricing (qv)
Issuer	A regulated and authorised financial institution that provides credit and debit card account on behalf of a card holder
Merchant Card Acquiring Service	An entity that provides an interface to Acquirer (qv) and which may itself be an Acquirer
Merchant Card Acquiring Equipment	Equipment that is capable of interfacing payment cards through insertion or non-contact whether in physical or dematerialised form (e.g. payment cards details stored in smart phones) and with relevant payment details e.g. amount to intermediate entities (generally Payment Gateways, qv) and thus to process Authorisations (qv) and Clearing (qv) via intermediate entities and displaying the result to the merchant and the payer
MID	Merchant Identity which identifies a merchant in processing payments and can apply to the top level of a merchant or at many different subordinate levels e.g. branch level
MPLS	Multiprotocol Label Switching is a routing technique in telecommunications networks that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows
PAN	A payment card number, primary account number (PAN), or simply a card number, is the card identifier found on payment cards, such as credit cards and debit cards and has a standardised range of 10 (rare 13 is usually given and 16 is most common) to 19 digits
PAR	Payment Account Reference is a single reference that is a superior value that sits above multiple Token (qv) values for the same PAN (qv)
Payment Facilitator	A regulated and authorised entity performing Merchant Card Acquiring Services (qv)
Payment Gateway	An entity that sits between merchants (and Merchant Card Acquiring Equipment (qv)) and provides intermediate service for merchants including but not limited to authorisations and clearing to Acquirers (qv) and providers of APMs (qv) and will process Cardholder Not Present (qv) and Cardholder Present (qv) transactions
PCI-DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information
PISP	Payment Initiation Service Processor is a regulated and authorised service provider capable of securely initiating a payment on behalf of the payer from an account provider with payment direct to a merchant rather than depending on the infrastructure of payment cards and card schemes
Settlement	Represents the flow of funds between account providers and merchants often via intermediate entities to reimburse merchants for goods and services bought by payers and can also include funds that represent fees, interchange and refunds and depending on all values funds flow may be bi-directional
Settlement Day 0, 1, 2	The day of Settlement (qv) in relation to the Transaction Day (qv) where 0 represents the Transaction Day (qv) and 1 represents the next day and so forth
Single messaging	A payment transaction that consists of only one part, namely Clearing (qv) but where the Authorisation (qv) is contained within the Clearing
Transaction	A complete payment request by a Merchant consisting of an Authorisation (qv), if required, and an entry into Clearing (qv), if required
Transaction Day	The day when the merchant (and any intermediate entities) signals completion of a transaction so that it may be entered into Clearing (qv) for eventual Settlement (qv)

Token	Produced by at tokenisation process that transforms a PAN into an alternative string of characters and which is meaningless and from which the original PAN cannot be derived to most entities in the payment process although it shall be capable of being turned back into a PAN before application to the payer's account and maybe other entities in the journey from merchant to account provider such as external fraud checkers
TID	Terminal identity is a subordinate entity to a MID (qv) and generally identifies a payment 'terminal' which may be physical or logical
TLS	Transport Layer Security is a cryptographic protocol designed to provide communications security over a computer network and is a standard under enhancement as 'researchers' discover methods of attacking the security it provides

## Annex D – Management Information Headings

	Mandatory / Optional
<b>Authorisations</b>	
Authorisations by response message	M
Approval rate by payment method	M
Approval rate by card type	M
Approval rate currency	M
Approval rate by MCC	M
Approval rate by MID	M
Approval rate by transaction service	M
Approval rate by issuing bank country	M
Approval rate by issuing bank	M
Approval rate by digital wallet	M
Approval rate by cashback	O
<b>Sales and Refunds</b>	
Total Transactions	M
Sales	M
Refunds	M
Refund Rate	M
Sales and refund rate by payment method	M
Sales and refund rate by card type	M
Sales and refund rate currency	M
Sales and refund rate by MCC	M
Sales and refund rate by MID	M
Sales and refund rate by transaction service	M
Sales and refund rate by issuing bank country	M
Sales and refund rate by issuing bank	M
Sales and refund rate by digital wallet	M
<b>Chargebacks</b>	
Total transactions	M
Chargebacks	M
Chargeback rates	M
Chargebacks by lifecycle state	M
Chargebacks by reason code	M
Chargebacks by payment method	M
Chargebacks by card type	M
Chargebacks by currency	M
Chargebacks by MCC	M
Chargebacks by MID	M
Chargebacks by transaction source	M
Chargebacks by issuing bank country	M
Chargebacks by issuing bank	M
Chargebacks by digital wallet	M
<b>Fees</b>	

Total Fees and Taxes	O
Fees Paid	O
Chargeback rates	M
Effective rate	O
Taxes	O
Fees by description	M
Fees by payment method	M
Fees by MID	M
Fees by Invoice Number	M
Fees by Transaction Source	M
<b>Cash Flow</b>	
Net Settled Cash	O
Cash In (Sales)	O
Cash Out	O
Cash Flow by payment method	O
Cash Flow by currency	O
Cash Flow by MID	O
Cash Flow by Transaction Source	O
<b>Reported Fraud</b>	
Fraud Rate	M
Fraud 3DS	M
Sales 3DS	M
Fraud rate and amount by issuing bank country	O
Fraud Rate by payment method	O
Fraud amount by fraud reason code	O
Fraud rate and amount by PSD2 eligibility	O
Fraud rate and amount by authentication method	O
Fraud rate and amount by card type	O
Fraud rate and amount by entry method	O
Fraud rate and amount by transaction source	O