PayPoint

SUPPLIER SERVICE DESCRIPTION

As set out in the G-Cloud 15 Call-Off Contract Order Form and as further described herein.

Digital Payment Services – Service Descriptions

The Buyer acknowledges that a Group Company of the Supplier may be acting as a sub-processor for the provision of the Services under this Agreement.

Payment Channels and additional functionalities

The following payment channels and additional functionalities are available.

Payment Channel/ Additional Functionality	**Description**
Tone Masking	An agent assisted payment solution which utilises DTMF (Dual Tone Multi Frequency) masking technology providing a secure way of handling payments by phone.
Additional functionality: Event Streamer	The Supplier shall provide reporting of Transactions through its "Event Streamer" facility. Such reporting shall be delivered to the Buyer via either the Client Portal and/or the Buyer's specified URL endpoint.

Card Processing Services (please refer to Service Specific Terms – Card Processing set out herein):

Set-Up and Implementation Services

The Supplier shall facilitate the setup and implementation of Digital Payments. Such service will not be undertaken for the Buyer under the terms of this Agreement, without the prior written agreement of the Parties. Such prior written agreement of the Parties shall include:

1. Commencement and termination dates of such set-up and implementation services;
2. Test dates and test period when it is anticipated that the set-up and implementation services shall be available to the Buyer for testing;
3. Testing criteria which shall include time scales in which any failures of the set-up and implementation services are to be remedied; and
4. Transitional periods (if any) associated with the set-up and implementation services.

Such set-up and implementation services shall include any other development work as may be set out in these terms.

Card Processing Services (please refer to Service Specific Terms – Card Processing set out herein)

The Buyer provides its customers with a form of identification to enable such Customer to make a payment. The Buyer wishes the Supplier to provide it with the Services as set out in the Generic Specification for the MultiPay Platform.

SUPPLIER STANDARD TERMS

Supplier Acceptable Use Policy – terms governing the Buyer's access to and use of the Card Processing Services. This may be read in conjunction with the Supplier Service Specific Terms detailed below.

1. Exclusivity

The Buyer shall utilise the Supplier on a Non-Exclusive basis, which means the Buyer may utilise the Supplier and any other provider of services the same as or similar to the services.

2. Payment Channels

The following identifies the payment channels through which a Customer may access Digital Payments, together with services providing additional functionality, and any specific terms related thereto.

2.1 Tone Masking (DTMF Suppression) Service

The DTMF Suppression solution (also known as Tone Masking) is an agent assisted payment solution which utilises DTMF (Dual Tone Multi Frequency) masking technology. This service provides the Buyer with a secure way of handling payments by phone without bringing its environment in scope of Payment Card Industry Data Security Standard (PCI DSS). In order to achieve this, the Supplier's Tone Masking supplier integrates with the call flow and at the point of payment, intercepts any keypad tones from the customer. As a result, the agent doesn't hear or see the card data, all they see are asterisks on the screen and the last four digits of the card.

Additional terms relevant for the Tone Masking Service

1. The Buyer acknowledges that the Tone Masking Service is provided through the Supplier's subcontractor ("TMS Subcontractor").

2. The Supplier shall engage the Buyer with the TMS Subcontractor for the provision of this service and the Buyer acknowledges that provision of the service will require use of, and will require the Buyer to interface with, the TMS Subcontractor telephony system.

3. Provision of the Tone Masking Service requires the Buyer to have an existing Digital Payments account with the Supplier. In the event that such existing Digital Payment account is suspended or terminated, then the Tone Masking Service shall also be suspended/terminated.

4. The Tone Masking Service is further described in Appendix Two (Generic Specification for the Multipay Service).

Supplier Data Processing Agreement/Data Processing Terms

1. Overview

To the extent that in the course of providing the Services or using the Services a party shares Personal Data with the other or otherwise Processes such Personal Data under the Agreement(s), the provisions of this section shall apply.

2. Definitions

2.1. For the purpose of this Addendum the following definitions will apply;

Accredited Payment Processor	The payment gateway used to submit transactions to the card schemes and/or Bacs.
Accredited Services	Services in relation to processing of card payments, open banking, credit transfer and/or direct debits.
Agreement(s)	The G-Cloud 15 Call Off contract between the Supplier and the Buyer for payment services and/or technology services.
Buyer	The organisation using the Supplier Services
Controller	shall have the meaning given in the Data Protection Legislation.
Customer	shall have the mean given to it in the Agreement and if not mean has been given shall mean the customer of the Buyer.
Customer Data	Means data identifying the customer of the Buyer other than to the extent such data is a component of Transaction Data and/or Payment Data.
Data Protection Legislation	Data Protection Legislation means: i. General Data Protection Regulation ((EU) 2016/679) as applied in the United Kingdom **("GDPR");** and ii. any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK; and iii. the Data Protection Act 2018; and iv. any successor, amendment and/or replacement thereto.

	v. In each case interpreted in accordance with the DP Guidance.
Data Subject	shall have the meaning given in the Data Protection Legislation;
DP Guidance	means any and all guidelines, recommendations, best practice, opinions, directions, codes of practice and codes of conduct issued, adopted, recommended or approved the UK's Information Commissioner's Office and/or any other supervisory authority or data protection authority from time to time (whether or not legally binding) in relation to the processing of personal data, data privacy, electronic communications, marketing and/or data security.
The Supplier	PayPoint Network Limited PayPoint Collections Limited PayPoint Payment Services Limited RSM 2000 Limited To the extent any of the above are referred to in the Agreement(s) with the Buyer.
Personal Data	shall have the meaning given in the Data Protection Legislation.
Personal Data Breach	shall have the meaning given in the GDPR.
Payment Data	Means the data used to initiate and/or process a card payment or direct debit payment.
Processor	shall have the meaning given in the Data Protection Legislation.
Processing	**Processing**" shall have the meaning given in the Data Protection Legislation, and "**Process**" and "**Processed**" shall be construed accordingly
Representative	means employees, staff, (excluding Retailer/Agents) sub-contractors, service providers and invitees of the Processor, engaged or due to be engaged in the provision of the Services or required to carry out obligations of the Processor under this Agreement.

Retailer(s) or Agent(s)	means an organisation and/or individual appointed by the Supplier to provide Services via a retail outlet.
Security Breach	means any unauthorised disclosure, deletion, corruption, access or contravention of the technical and operational security requirements.
Services	The services as the same are more fully described in the Agreement(s).
Shared Data	means any Personal Data shared between the parties or otherwise Processed by either or both parties under the Agreement consisting of Transaction Data and Payment Data.
Special Categories	shall have the meaning as assigned to it in the Data Protection Legislation
Sub-processor	Means any third party processing Personal Data as instructed by the Data Processor
Transaction Data	means the payment, system and operational data used in relation to the Services.
Transfer Date	Means the date the parties agree the Personal Data is to be transferred to the Data Controller (or as the Data Controller directs) upon termination of the Agreement.

2.2. To the extent any of the Agreement(s) currently in force with the Supplier makes reference to the Processing of Personal Data this Schedule shall apply in substitution.

2.3. For the purpose of the Agreement the following exchanges of Personal Data will apply:

2.3.1. Card Payment Services – Controller (Buyer) to Processor (The Supplier).

2.3.2. Registration hosting services (if applicable) – Controller (Buyer) to the Supplier (Processor).

2.3.3. Generation of a PayByLink Request for Payment – Controller (Buyer) to Processor (The Supplier).

2.3.4. Any other exchange of personal data not listed above shall be as determined by the ICO guidance on controllers and processors together with the applicable Data Protection Legislation.

PART 1 – CONTROLLER TO CONTROLLER PROVISIONS

1. Data Sharing

1.1. The parties acknowledge in order for the Supplier to provide the Services and for the Buyer to use the Services, it is necessary for Personal Data to be shared;

1.1.1. by the Buyer to the Supplier for the processing of payments provided under the Services and for investigation and resolution of disputes between the Buyer and Customers; and

1.1.2. The Supplier to the Buyer in relation to Transaction Data, Payment Data and Retailers in relation to the Buyer's use of the Service.

1.2. The Shared Data to be shared between the parties shall be no more than is necessary in the particular circumstances.

1.3. The parties agree the Shared Data may only be used for the purpose specified in this clause 1 (Data Sharing).

2. Warranties

2.1. The party disclosing the Shared Data warrants that:

2.1.1. it has no reason to believe that it is prohibited from sharing, or that the other party is prohibited from receiving, the Shared Data in accordance with the Agreement;

2.1.2. at the time of sharing the Shared Data is accurate and up to date to the best of its knowledge; and

2.1.3. it will at all times ensure that it (and any sub-contractor) has obtained the Shared Data in accordance with Data Protection Legislation and has provided all necessary notices to Data Subjects and has procured all necessary consents, or satisfied another legal basis, to disclose the Shared Data to the party receiving it and for the party receiving the Shared Data to Process the Shared Data in compliance with Data Protection Legislation.

2.2. The party receiving the Shared Data warrants that:

2.2.1. it has no reason to believe that it is prohibited from receiving, or that the other party is prohibited from sharing, the Shared Data in accordance with the Agreement;

2.2.2. it shall not process the Shared Data for any purposes other than those set out in Clause 1 (Data Sharing).

3. Obligations

3.1. The parties shall apply appropriate security mechanisms to the Shared Data to ensure its security in transit.

3.2. The parties agree to provide such reasonable assistance as is necessary to each other to enable them to comply with any Data Subject Request made.

3.3. Each party shall comply with the requirements of the Data Protection Legislation in respect of the activities involving Shared Data which are the subject of the Agreement and shall not knowingly do anything or permit anything to be done in respect of or in connection with the Data which might lead to or cause a breach by the other party of the Data Protection Legislation.

3.4. Each party shall ensure that;

3.4.1. any sub-contract it enters into in connection with the Agreement contains terms equivalent to those set out in this Addendum and contain obligations to comply with the data protection obligations contained herein. The sub-contracting party remains fully liable to the other party for any acts or omissions of any subcontractors.

3.4.2. access to the Shared Data is limited to:

(i) those Representatives who need access to the Data to meet the party's obligations under the Agreement; and

(ii) such part or parts of the Shared Data and to the extent and manner as is strictly necessary for performance of that Representative's duties.

3.5. Each party will ensure it has in place;

3.5.1. processes and procedures to ensure that the Representatives comply with appropriate procedures and guidelines in relation to the processing of Shared Data, and ensure that all the Representatives who have access to the Shared Data are aware of and have undertaken training in applicable Laws relating to handling such Shared Data (including the Data Protection Legislation); and are subject (by way of written agreement) to a duty of confidentiality;

3.5.2. technical and organisational security arrangements, for the processing of Personal Data and procedures for keeping the Personal Data safe from unauthorised disclosure or accidental deletion;

3.5.3. measures and procedure to respond to a Data Subject Access request;

3.5.4. measures and procedures to deal with a Data Breach including processes compliant with the requirements of the Data Protection Legislation;

3.5.5. data storage and retention policies and procedures consistent with and appropriate to the Data Protection Legislation.

3.6. Save to the extent required for legal, regulatory or compliance purposes each party will cease to use the Shared Data upon termination of the Agreement.

3.7. For the avoidance of doubt the Buyer has acknowledges the Supplier as Controller has appointed the Retailers to provide services in relation to the Services.

PART 2 – CONTROLLER TO PROCESSOR PROVISIONS (Including Accredited Services)

1. Processing Activities

1.1. The Supplier will perform Processing activities in relation to Payment Data as part of the payment processing, the subject-matter, duration, nature, type of Personal Data, categories of Data Subjects and purpose of which are described more fully below in Annex 1 (the "Processing Activities").

1.2. In relation to such Processing Activities,

1.2.1. the Buyer is the Controller and the Supplier is the Processor for card processing;

1.2.2. the payment schemes, payment systems, acquirer and/or issuer is the Controller for the payment system processing;

1.2.3. the Accredited Payment Processor as identified in the Sub-Processor List is the Sub-Processor for the purposes of the Services and the Data Protection Legislation

1.2.4. The Buyer is the Controller is for direct debits and the Supplier is the Bacs Bureau (as Processor);

1.2.5. for Direct Debit Facilities Managed the Supplier is the Controller when offering payment services.

1.3. The Personal Data (or any part of such Personal Data) which may be included in Payment Data which is:

1.3.1. transmitted by or on behalf of Buyer to, or is otherwise Processed by, under this Agreement (and whether relating the Buyer, a Buyer's Customer(s) or a third party); or

1.3.2. generated under this Agreement in relation to card payments, credit transfers and/or direct debits.

2. **Processor obligations**

2.1. Where the Supplier acts as a Processor in respect of Personal Data (other than Shared Data) and the Buyer is the Controller, the Processor shall:

2.1.1. Process the Personal Data in accordance with the Agreement and any documented instructions given by the Controller from time to time. Any change in the instruction such as to vary the form of processing will be regarded as and subject to change control;

2.1.2. apply appropriate technical and organisational measures which are sufficient to comply with Article 32 of the GDPR (as appropriate) or any provisions to be applied to the transfer of Personal Data outside the United Kingdom applicable at the time of the transfer under the Data Protection Legislation;

2.1.3. ensure that its staff and any persons authorised to process the personal data have committed themselves to confidentiality through a written agreement with the The Supplier and/or its Sub-Processor;

2.1.4. in relation to any persons authorised to Process (or who may otherwise have access to) Payment Data ensure that such persons adhere to the terms of this Agreement;

2.1.5. assist the Controller in ensuring compliance with Articles 32 to 36 of the GDPR (inclusive)) taking into account the nature of Processing and the information available to the Processor. The Processor may make a reasonable charge for this assistance.

2.1.6. upon the request of the Buyer, provide assistance to the Buyer relating to the Buyer's security; impact assessment; data breach reporting requirements and data protection or data privacy authority consultation obligations under the Data Protection Legislation. To the extent such assistance is not an obligation imposed upon the Processor under the Data Protection Legislation, the Processor may charge the Buyer its reasonable costs (or the rates otherwise agreed between the parties) for its time spent and expenses incurred in providing the Buyer with co-operation and assistance as required by this clause 2 (Processor Obligations) any such assistance being subject to agreement in writing;

2.1.7. taking into account the nature of the Processing Activities, assist the Buyer by undertaking the appropriate technical and organisational measures, insofar as this is possible, to respond to requests for exercising a Data Subject's rights in accordance with the Data Protection Legislation.

3. Data Transfer

3.1. The Processor may not transfer Payment Data to a third country that is outside the EEA without the appropriate or suitable safeguards to provide an adequate level of protection such as are required under the Data Protection Legislation in order to ensure that the level of protection of natural persons guaranteed by the Data Protection Legislation is not undermined;

3.2. To the extent the transfer of Personal Data is required to enable the processing of the Payment Data in accordance with Scheme Rules, the Controller hereby gives consent to the processing subject to the Processor ensuring the appropriate controls, consents and protections are in place consistent with the requirements of the Data Protection Legislation.

3.3. The Processor will publish details of the transfers to any Sub-processors as specified in Clause 7 (Sub-processors).

4. Compliance

4.1. Each party shall at all times comply with the provisions of the Data Protection Legislation in connection with this Agreement and its performance of the Services (including the Processing Activities).

4.2. The Buyer warrants, represents and undertakes to the Supplier that;

4.2.1. The Buyer has lawful grounds for processing the Payment Data.

4.2.2. Any instruction given by the Buyer, policy or procedure shall be lawful.

4.3. The Supplier represents warrants and undertakes that;

4.3.1. The Payment Data will be processed in accordance with the Data Protection Legislation.

4.3.2. It and/or its Sub-contractors have and will for the duration of the Agreement maintain the appropriate authorisations, accreditations and/or permissions to process the Payment Data.

4.4. Each party shall promptly and without undue delay inform the other in writing:

4.4.1. if, in its opinion, an instruction or request by or on behalf of the Buyer, infringes the Data Protection Legislation;

4.4.2. in the event that it becomes aware of any breach of the Data Protection Legislation (including its Sub-Processors) in connection with this Agreement; and

4.4.3. of any provisions in any local law or of any changes in the laws of the country in which Payment Data is processed which does or could affect the Processor's ability to perform its obligations under this Schedule (Data Protection).

4.5. The parties confirm that the information relating to the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data; the categories of the data subjects; and the obligations and rights of the data controller have been set out in this Agreement and in Annex 1.

4.6. A party shall notify the other party promptly and in any event within thirty-six (36) hours:

4.6.1. if it is required by Data Protection Legislation to act other than in accordance with any of the other party's instructions, provided that the Processor party is not prohibited by law from so notifying the other party; and/or

4.6.2. if it considers, in its opinion (acting reasonably), that any of the other party's instructions infringe any of the Data Protection Legislation; and/or

4.6.3. notify the other party promptly (and in any event within thirty-six (36) hours) following its receipt of any request, notice or complaint from a Data Subject exercising their rights under the Data Protection Legislation (a "Data Subject Request") or any correspondence (whether written or verbal) from the ICO, and will provide the other party with all reasonable co-operation and assistance required by the other party in relation to any such Data Subject Request or ICO Correspondence.

5. Security

5.1. The Processor shall as appropriate;

5.1.1. taking into account the nature of the processing, state of art, the costs of implementation and the scope, context and purpose of the processing implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk;

5.1.2. apply the pseudonymisation and encryption of personal data;

5.1.3. have the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.1.4. have the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

5.1.5. process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

5.1.6. take steps to ensure that any natural person acting under the supervision of the Processor who has access to personal data does not process the Personal Data except on instructions from the Controller, unless they are is required to do so by law.

6. Data Breach Notification

6.1. The Supplier shall without undue delay notify the Buyer of a Personal Data Breach (and in any event no later than 36 hours). Such notification shall:

6.1.1. describe the nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of the Payment Data records concerned; and

6.1.2. describe the measures taken or proposed to be taken by the Processor and/or its Sub-Processor to address the Personal Data Breach, including where appropriate measures to mitigate its possible adverse effects.

6.1.3. describe the implementation of any measures necessary to restore the security of compromised Personal Data, and

6.1.4. support the Buyer to make any notifications to the UK Information Commissioner's Office ("ICO") or affected Data Subjects

7. Use of Sub-processors

7.1. The Processor may only engage Sub-processors in accordance with the requirements set forth in this clause 7 (Use of Sub-processors).

7.2. The Controller acknowledges and agrees that the Processor's group companies may be retained as Sub-processors.

7.3. To the extent the Processor uses Sub-processors to Process the Controller's Personal Data, the Processor shall make available to the Controller a current list of Sub-processors for the respective Services with the identities of those Sub-processors (the **Sub-processor List**).

7.4. The Processor shall provide the Controller access updates on the Processor's website at https://www.paypoint.com/privacy-statement/sub-processor-statement ("the Designated Web Page) to enable the Controller to have access to the relevant Sub-processor List and shall provide such updates via the Designated Web Page before authorising any new Sub-

processor(s) to Process Personal Data in connection with the provision of or use of the Services.

7.5. The Controller shall have the right to object the use of any particular Sub-processor by Processor. Such objection to be provided no later than seven (7) days after the publication of the Sub-processor's details on the Processor's Designated Web Page.

7.6. The Processor shall be liable for the acts and omissions of its Sub-processors to the same extent the Processor would be liable if performing the services of each Sub-processor directly under the terms of this Schedule, except as otherwise set forth in this Agreement.

7.7. To the extent the Controller uses a Service for which the use of a Sub-processor is included in a general authorisation, the terms of the general authorisation are set out on the Designated Web Page.

7.8. The Processor shall ensure that the Sub-processor contract (as it relates to the Processing of Personal Data) is on terms which are substantially the same as, and in any case no less onerous than, the terms set out in this Addendum.

8. Audits

8.1. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller and shall immediately inform the Controller if, in its opinion, an instruction infringes the Data Protection Legislation.

8.2. The Processor make available to the Buyer such information as the Buyer reasonably requests and the Processor is reasonably able to provide, and, permit and contribute to such audits, including inspections, conducted by the Buyer (or the Buyer's appointed auditors), as is necessary to demonstrate the Processor's compliance with the Data Protection Legislation subject to the applicable legal, regulatory and payment card accreditations. The Buyer will give reasonable notice of any audit and unless there are reasonable grounds to suspect a breach will limit audits to one annually.

8.3. Any audit is subject to the Processor's, legal, regulatory and/or payment industry accreditations including but not limited to PCI accreditation, its data processing facilities, procedures and documentation to be submitted for scrutiny, inspection or audit by the other party and/or provide the other party with written evidence of its compliance with the requirements of this clause 8 (Audits).

8.4. To the extent an audit is not permitted and/or restricted the Processor shall at all times be compliant with its obligations under this Agreement and shall demonstrate its compliance with the provision of the appropriate industry accreditation certification.

9. Retention and Transfer

9.1. If so requested by the Controller, the Processor will, during the term of the Agreement subject to legal and regulatory requirements and obligations, delete and/or transfer the Personal Data to the Controller.

9.2. The method and security of any such transfer to be agreed by the parties at the time and subject to the appropriate measures to ensure the security and integrity of the Personal Data, having account of cost and adequacy of any such measure as of the date of the transfer.

9.3. Any deletion of Personal Data undertaken by the Processor under this clause 9 (Retention and Transfer) shall be undertaken securely and in accordance with the relevant Data Protection Legislation.

9.4. Within thirty (30) days of Termination or Expiry of the Agreement, in a format acceptable to each party, to the extent permitted by law, payment card rules, payment service requirement and obligations, permanently delete, destroy or return all of the Payment Data the Buyer following termination or expiry of this Agreement and delete existing copies of such Payment Data unless (and only to the extent) the Processor is required to retain copies in order to comply with applicable law.

9.5. If following termination of the Agreement, the parties fail to agree a transfer date, format and process, the Processor may subject to legal and/or regulatory requirements, upon the provision of not less than thirty (30) days notice in writing delete the Payment Data.

9.6. The Processor may charge for any associated costs in relation to any cleansing, deletion or transfer of the Payment Data such costs and method of transfer to be agreed in writing by the parties at the time.

10. Processing Description

10.1. The legal basis for processing shall be:

10.1.1. Where necessary to carry out the Processor's obligations under this Agreement or to take steps to enter into an agreement with the Buyer; and/or

10.1.2. Where the law requires this processing; and/or

10.1.3. It is in the Processor's legitimate interests to make sure that the payment processing complies with the appropriate industry standards.

Description	**Details**
Subject matter of the processing	Provision of the following to the extent specified in the product description for the Services under the Agreement(s): • Customer registration under Multipay. • Direct Debit Services

	• Credit Transfer Services • Gift Voucher Purchase Services
Duration of the processing	Term of the Agreement.
Nature and purpose of processing	• Storage • Processing • Customer information collection via mobile applications or website • Processing in relation to retail outlets, retailer details and retailer locations. • User log on, email and IP location in relation to voucher generation or accessing reports via a portal.
Types of Personal Data	Personal Data. There are no Special Categories of Personal Data required for the processing.
Categories of Data Subject	• Customers of the Buyer • Employee and Contractors (Buyer and The Supplier) • Retailers
Plans for return or destruction of Personal Data	Please see clause 9 (Retention and Transfer) above.
Permitted Transfers	To the extent required to perform the Services as specified in the Agreement(s) including but not limited to: • Financial Conduct Authority. • HMRC and other Tax Authorities. • Police and Investigatory Bodies. • Payment systems, payment schemes, e-money schemes, card scheme (including but not limited to MasterCard Inc, Visa International Limited and American Express) • Retailers.

	• Regulatory bodies and authorities including government and quasi government organisations. • Third party service providers providing banking services. • Payment service providers and/or organisation acting as technical service provider under the Payment Service Regulations 2017. • Regulated telecommunication service providers. • Payment systems including but not limited to Pay.uk, BACS, CHAPS and/or Faster Payments. • OBIE. • Information Commissioner's Office. • Auditors • Sub-processor as per clause 7 (Sub-processors) above.
Non EEA Transfers (The Supplier)	To the extent required to provide Services under the Agreement(s) and subject to clause 3 (Data Transfer) above (as applicable); See the Designated Web Page as specified in clause 11 (Sub Processors) above. Details of The Supplier non EEA processing is available by e-mailing privacy@paypoint.com .
Special Security Requirements	To the extent the Processing of Personal Data relates to the provision of payment card processing, compliance with Payment Card Industry and/or such standard as applicable at the time shall apply. The Buyer confirms they are a merchant with an acquirer in relation to any such Processing.
Personal Data Fields	May include any of the following: • Name: • E-mail Address; • Phone or contact details: • Customer Account Numbers: • Retailer (Agent) Account or ID Numbers: • Bank account or payment account details: • E-money account details: • Customer Bank Account; • Customer Name: • Customer Bank Sort Code

	Please note, not all the above will include Personal Data or Customer Data being data that can identify a living individual when in the possession of the Processor. Personal Data will only be provided to the extent required to provide or receive Services under the Agreement.

11. Data Protection Officer

11.1. The contact details for the Supplier's Data Protection Officer are:

Data Protection Officer
PayPoint Group
1 The Boulevard,
Shire Park,
Welwyn Garden City,
Hertfordshire,
AL7 1EL
E-mail: privacy@paypoint.com

11.2. The details of the Buyer Data Protection Officer (if any) will be notified by the Buyer to the Supplier no later than 28 days after the date of this Agreement, by e-mailing privacy@paypoint.com .

Annex 1
Processing Activity

Subject matter of the processing	Transactional payment processing and ancillary services.
Duration of the processing	Transaction processing is transient at the point of time of the transaction but our policy is to retain the transaction data to support international payment card
Nature and purpose of the processing	The nature and purpose of the processing is to enable data subjects to make payments for good and services by facilitating the payment processes between the data subject, the relevant merchant or organisation providing the goods or services and the associated components of the wider financial system including acquirers, payment systems, banks and schemes.

Type of personal data	Personal data to support the payment for goods and services, including name, account details, and payment details associated with the transaction as defined by the Buyer organisation, acquirer, payment systems, bank or scheme.
Categories of data subjects	Individuals who wish to make payments for goods and services.
Obligations and rights of the Buyer	As defined in the terms in this Agreement.

SUPPLIER SERVICE SPECIFIC TERMS

CARD PROCESSING SERVICES

The service level terms and conditions are detailed below.

1 Definitions

Acquirer means a financial institution(s) with which the Buyer has entered into a Client Acquiring Contract from time to time and the Processor (such term as defined below) has entered into an agreement with or is accredited to forward payment Data for Authorisation, clearing and settlement. For the avoidance of doubt, the Supplier is not the Acquirer;
API Integration Document means the documentation and/or materials supplied to the Buyer and as updated by the Supplier (at its sole discretion from time to time) setting out the manner in which the Buyer may utilise the PayPoint Platform Integration, along with requirements and restrictions on its use, and other accompanying related information.
Authorisation means a request for and subsequent confirmation from the Acquirer or the E-Money Issuer that a payment will be credited to the Buyer in respect of any Transaction, subject to the terms of the agreement entered into by the Buyer with the Acquirer or the E-Money Issuer (whatever the case may be);
Cardholder means a holder of any Payment Card;
Card Processing means payments made by a Customer by a payment card via any of the Payment Channels;
Card Processing Transactions means the submission of a request for payment by a Customer to the Processor via the Payment Channels, whether or not the Customer has requested a Receipt;
Chargeback means an invalid or Disputed Transaction that is or may be charged to the Buyer by an Acquirer;
Client Acquiring Contract means the agreement between the Buyer and the Acquirer for acquiring services;
Client Application means web or other software services or applications developed by the Buyer that utilises or interacts with the PayPoint Platform Integration pursuant to the terms of this Agreement. Buyer Applications shall be construed accordingly.
Client Product means the goods and/or services provided to the Cardholder by the Buyer for which the Transaction is used as a means of payment;
Client Profile means the Buyer's unique profile created as part of the Services;
Client Portal means a web accessible back office portal for the Buyer to carry out such functions as described in the applicable Technical Service Documentation and clause 5 below;
Customer Data means information relating to a Customer of the Buyer (other than Payment Data), which is inputted by the Customer for the purpose of using the Services or facilitating the Customer's use of the Services;
Customisation and Development Services means a development that is agreed by the Parties for services that do not form part or any network common platform service;
Development Service Order means a service order in relation to Customisation and Development Services agreed between the Buyer and Supplier;
E-Money Account means the trust account operated by the E-Money Issuer into which monies collected from E-Money Account Holders are held for the purposes of allowing payments to Buyers;
E-Money Account Holder means a consumer who wishes to buy goods and/or services using funds the consumer has used to purchase E-Money and held in the E-Money Account;
E-Money Issuer means a financial institution that allows consumers to make purchases of goods and/or services using an E-Money Account;
Failure Notice means a notice from the Acquirer or the E-Money Issuer that a request for payment has been declined in respect of any Transaction;
Generic Specification for the Multipay Platform means the document attached hereto as Appendix Two;
Keypad means the keypad located on a gas and/or electricity meter into which a Customer may type a UTRN for the purposes of applying credit to their relevant energy account;

Operating Hours means the hours of 08:00 – 22:00 on a daily basis 7 (seven) days a week;
PayByLink Request for Payment or PBL Request for Payment means a link generated by the Supplier to enable a customer to make a Payment Card payment to the Buyer via the Accredited Payment Processor and optionally make a cash payment at an Agent Outlet (if agreed between the Parties);
PayByLink Service means the service for the generation of a PayByLink Request for Payment pursuant to the terms stated herein;
Payment Card means either a debit card or a credit card that has been issued by a financial institution to a Cardholder;
Payment Channel means the front end method by which a Customer accesses Digital Payments as further described in the Supplier Service Description;
Payment Data means all information provided by a Customer or obtained from any other source in particular the Acquirer or E-Money Issuer or Supplier that is required for an authorisation of payment and/or processing of a Payment Transaction and specified as Payment Data by the Schemes and or required to process a Payment Transaction in compliance with the Payment Services Regulations;
PayPoint Platform Integration means the application programming interface and any accompanying documentation (including the Technical Service Documentation) to enable the processing of Card Processing Transactions and associated services by Buyer Applications pursuant to the terms of this schedule and the API Integration Document;
PCI-DSS means the Payment Card Industry Data Security Standard;
PCP Service means the Payment Card processing services set out in Appendix One attached hereto;
Processor means, in relation to the Card Processing services detailed herein, a third party supplier appointed by the Supplier to provide the PCP Service; For the purpose of this section, references to "the Processor" shall include the Supplier's level one accredited PCI compliant sub-contractor but for the avoidance of doubt the inclusion of the Supplier's level one accredited PCI compliant sub-contractor shall not diminish the Supplier's liability under this Agreement;
Receipt means a page displayed on a website once an online transaction has been completed; or a reference number either provided verbally or sent via SMS to a Customer via a multi-channel solution;
Release means an upgrade, amendment and/or enhancement to software and other services in relation to the Card Processing services provided under this Service Schedule;
Release Schedule Communication means a notification to the Buyer of a Release scheduled during the Term;
Scheme Rules means the operating rules and procedures issued by the Scheme and/or E-Money Issuers and as notified to the Buyer by the Scheme, E-Money Issuer, BACS, the Supplier and/or the Acquirer;
Security Data means any codes or other security measures relating to a Payment Card or an E-Money Account and used to verify the identity of the Cardholder or E-Money Account Holder and/or the authenticity of a Transaction (including verification number, also known as CVV, CSV or CVC codes);
Settlement File means the file of Transactions submitted to the Buyer's Acquirer each day;
SMART Card means a magnetic swipe card or other such media that is provided to a Customer by the Buyer or a Third Party Supplier of the Buyer;
Technical Service Documentation means the specifications and any other relevant documentation included as part of the Services and as set out herein;
Transaction means the submission of a request for payment to the Processor via the Payment Channel as whether or not the Customer has requested a Receipt;
User Acceptance Testing or UAT means the final testing performed when function, system and regression testing is completed.
UTRN means the code number provided by the Buyer to Supplier (or a Third Party Supplier on behalf of the Buyer), and which may be requested by a Customer using the IVR Service;
Virtual Terminal means a service that enables the Buyer to submit Card Processing Transactions via the Client Portal.

2. Service Updates

2.1 The Supplier has in place a discretionary programme of updates and improvements to the Card Processing services which includes the provision of new Releases, which shall be provided at no cost. For the avoidance of doubt, this does not include any bespoke development work carried out as stated herein.

2.2 The Release Schedule Communication will be sent to the nominated Buyer contact.

2.3 The Release Schedule Communication shall include:
- 2.3.1 Information in relation to the content of the Release;
- 2.3.2 Test dates and test periods when the Buyer may participate in the testing of the Release (if applicable);
- 2.3.3 Transitional periods associated with a Release (if applicable); and
- 2.3.4 Functionality that may cease to be available upon implementation of the Release.

2.4 Where the Buyer has implemented their own functionality or link within the interfacing of the solution (for example, but not limited to, links to/from client websites, consumer advice, marketing messages, FAQs, terms and conditions) then the Buyer will need to be responsible for all testing and works to ensure compatibility with Releases, the Supplier shall provide reasonable co-operation and information to the Buyer.

2.5 The Supplier may from time to time, notify the Buyer that a function or service is to be retired, or where such function or service is linked to a decline in consumer usage and/or supporting infrastructure becoming obsolete, the Supplier will consult with the Buyer. The Supplier shall use reasonable endeavours to assist the Buyer to migrate to a reasonably comparable Service.

3. Obligations of the Supplier

3.1 Where the Buyer has elected to receive reporting via Event Streamer, the Supplier does not warrant for the timeliness of receipt of any reporting by the Buyer's system when using such service.

3.2 Once the User Acceptance Testing (or other testing as agreed between the Parties as necessary) has been successfully completed, the Supplier shall, during the term of this Agreement, provide the Services as set out in accordance with the Technical Service Documentation.

3.3 The Supplier will provide the Buyer with access to the Services in accordance with (i) the terms stated herein as may be amended by agreement with the Buyer in writing from time to time; (ii) the Technical Service Documentation.

3.4 The Supplier shall, as part of the Services and at no additional cost to the Buyer, provide the Buyer with the Supplier's standard support services. The Supplier may amend its standard support services in its absolute discretion from time to time.

3.5 The Supplier shall use reasonable endeavours to ensure that any scheduled maintenance, upgrades or modifications to the Services are conducted outside of Operating Hours. In the event

such scheduled work is required during Operating Hours and this shall only be required in the event of emergency, then the Supplier shall use reasonable endeavours to provide no less than 14 (fourteen) days' prior notice to the Buyer.

3.6 The Supplier shall advise the Buyer of the identity of the Processor and shall notify the Buyer if the identity of the Processor changes.

3.7 In addition to the Supplier's right to terminate or suspend the provision of Service for breach by the Buyer of its obligations under this Agreement, the Buyer acknowledges that its access to the Client Portal or its Customers' access to the Service may be immediately suspended if:

3.7.1 Emergency maintenance is required, although the Supplier will use all reasonable endeavours to ensure that such suspension is for a short a period of time as reasonably possible;

3.7.2 there is, or there is suspected to be, a security breach or denial of service attack or other attack on the Services, in which event the Supplier shall use all reasonable endeavours to rectify the security breach or attack on the Services as soon as reasonably possible;

3.7.3 there is any other event, including fraud, which, at the Supplier's sole discretion, may create a risk to the Services, the Buyer or any other of the Supplier's clients, if the Services are not suspended, in which event the Supplier shall use all reasonable endeavours to eliminate the risk to the Services as soon as reasonably practicable; or

3.7.4 It is required due to regulatory or legal reasons.

3.8 In addition to its obligations in this clause 3, the Supplier shall undertake further obligations where it is providing to the Buyer the PayPoint Platform Integration, such obligations as stated in the Service Description.

4. Obligations of the Buyer

4.1 The Buyer shall:

4.1.1 provide to the Supplier, and/or its Customers (as appropriate) all information, which shall include, but not be limited to, Data and/or any other materials to enable the Supplier to provide the Services.

4.1.2 co-operate with the Supplier, and any relevant subcontractor of the Supplier in conducting any scoping activities and tests that may be required to enable implementation of the Services, and any agreed variations to the Services and any agreement between the Parties to provide any additional services;

4.1.3 ensure that

4.1.3.1 all information provided by or on behalf of the Buyer for processing shall be in a format which is suitable for such use, and in such condition for processing as the Supplier may specify from time to time (provided that, the Supplier has

provided the Buyer with any information necessary for the Buyer to comply with this obligation);

4.1.3.2 access by Staff to the Supplier's System and/or the Supplier Information is only as required for the performance of this Agreement; and

4.1.3.3 physical access by Staff to computer equipment having access to the Supplier's Systems and/or or storing or having access to the Supplier Information is restricted to reflect the obligations set-out in sub-clause 4.1.3.7 and clause 18 "what you must keep confidential" of the G-Cloud 15 General Terms; and

4.1.3.4 no viruses or malicious code (as the expressions are generally understood in the computing industry) are introduced to and that there is no corruption of the Supplier's System and/or the Supplier's Information; and

4.1.3.5 onward linking or 'bridging' onto the Supplier's System and/or the Supplier's Information by the Buyer's third party suppliers is prevented; and

4.1.3.6 the Supplier is notified of any changes affecting access to the Supplier's System and/or the Supplier's Information including users who change function within, or leave, the Buyer; and

4.1.3.7 any and all of the Supplier's Information transmitted across public networks including the internet is encrypted to protect its confidentiality; and

4.1.3.8 it complies with all the Supplier's further and reasonable requirements for access and security of the Supplier's System and the Supplier's Information as notified to the Buyer from time to time; and

4.1.3.9 any breach of the security or compliance with the terms of this Agreement is reported immediately to the "Supplier's IT Operations 24 x 7 Team".

4.2 The Buyer shall undertake further obligations as set out in the Supplier Standard Ter,mswhere it is utilising the PayPoint Platform Integration.

5. Client Portal

5.1 This clause is relevant where the provision of Services under the G-Cloud 15 Call Off Contract includes access by the Buyer to and/or delivery of Services and/or reporting via the Client Portal.

5.2 The Supplier shall create a Client Profile and shall provide the Buyer with the Supervisor Access Identifier and Access Identifiers for all initially requested Users.

5.3 The Supplier shall provide initial training material to the Buyer on using the Client Portal.

5.4 In addition to the Supplier's right to terminate or suspend the provision of Service for breach by the Buyer of its obligations under the G-Cloud 15 Call Off Contract, the Buyer acknowledges that its access to the Client Portal may be immediately suspended if:

5.4.1 Emergency maintenance is required, though the Supplier will use all reasonable endeavours to ensure that such suspension is for a short a period of time as reasonably possible;

5.4.2 There is, or there is suspected to be, a security breach or denial of service attack or other attack on the Services, in which event the Supplier shall use all reasonable endeavours to rectify the security breach or attack on the Services as soon as reasonably possible;

5.4.3 There is any other event, including fraud, which, at the Supplier's sole discretion, may create a risk to the Services, the Buyer or any other of the Supplier's clients, if the Services are not suspended, in which event the Supplier shall use all reasonable endeavours to eliminate the risk to the Services as soon as reasonably practicable; or

5.4.4 It is required due to regulatory or legal reasons.

6. Service updates

6.1 For the avoidance of doubt, the Supplier will be required to issue a Release Schedule Communication in advance (in the event that this is reasonably possible) if the Release is required to comply with payment Scheme Rules, legislative developments which are not previously notified to the Supplier and/or security processes or procedures.

6.2 If the Release is the provision of a new Service module, such variation will need to be dealt with in accordance with the G-Cloud 15 Call Off Contract.

7. Limitation of Liability

7.1 Whilst the Supplier will exercise the care of a Reasonable and Prudent Operator in the performance of the Services and use all reasonable endeavours to provide the Buyer with a good level of accuracy and timeliness in performing the Services, the Buyer acknowledges and accepts that the Supplier relies on the services of third party for example acquirers (in accordance with the Buyer's Client Acquiring Contract in performing certain elements of the Services, and no warranty, guarantee or representation can be made by the Supplier that the Services are completely free from delays, errors, inaccuracies or omissions. As a result, the Supplier liability is limited to its failure of the Performance Standards.

8. Fees

8.1 All Fees shall be as stated and payable in the G-Cloud 15 Call Off Contract.

8.2 Any Scheme fees and/or charges shall be levied and or payable by the Buyer specific to a Payment Transaction and/or as required by the Scheme Rules and are in addition to the Charges specified and due to the Supplier in the G-Cloud 15 Call Off Contract.

9. Audit

9.1 Any audit under this clause will not require any member of the Supplier Group or the Processor to breach or compromise the Supplier's obligations under the Data Protection Legislation and/or the Processor's PCI accreditation. The audit rights shall not include any right to audit: the Supplier Systems, software, Supplier's service, payment Data and/or any data or information relating to any third party or other clients.

Appendix One: Additional terms governing the Buyer's access to and use Payment Card Processing ("PCP") for the Card Processing services. This may be read in conjunction with the Supplier Service Specific Terms detailed above.

1. Service description

1.1 This section sets out the Services provided by the Processor to the Buyer for:

(a) The receipt of Payment Data;

(b) The electronic transmission of Payment Data to an Acquirer or the E-Money Issuer; and

(c) Communication between:

- the Supplier, the Acquirer and the Buyer; and
- the Supplier, the E-money Issuer and the Buyer

For the purpose of facilitating the settlement of Payment Card and E-Money Account payment requests.

1.2 For the avoidance of doubt, a) neither the Supplier nor the Processor provide Acquirer services, b) neither the Supplier nor the Processor are the Acquirer.

1.3 The Processor will accept Card Processing Transactions on behalf of the Buyer and submit Payment Data to the relevant Acquirer and the E-Money Issuer. On receipt of an Authorisation or Failure Notice, the Processor shall provide details of the same to the Buyer via a payment notification.

1.4 The Processor can only provide the Service if the Buyer has a Client Acquiring Contract with an Acquirer and or an agreement with an E-Money Issuer.

1.5 The Processor supports the payment methods as specified from time to time. The Processor is not required to support and or process any payment methods other than those specified.

1.6 The Processor is responsible for maintaining its interfaces to an Acquirer with which the Processor has an agreement to submit Transactions.

1.7 If there is a change in circumstances affecting the provision of the Service (including any regulatory or other change affecting the payment processing industry and/or any revised policies, guidelines or regulations issued by a Scheme direct to the Buyer or via the Acquirer or E-Money Issuer), the Processor reserves the right in its sole option to make such alterations to the Service it deems reasonably necessary from time to time provided that such alterations shall not unless as a consequence of legislative, regulatory or Scheme developments or due to circumstances reasonably beyond the Processor's control have a material adverse effect on the functionality of the Service.

1.8 Any alterations to the Service that are introduced pursuant to clause 1.7 of this PCP Appendix shall be notified to the Buyer.

1.9 The Agreement is personal to the Buyer and in no event shall the Buyer use the Service for the processing of Transactions on behalf of a third party in contravention of the Client Acquiring Contract.

2.1 Acceptance of any Transaction for processing by the Processor and its online confirmation of an Authorisation to the Buyer and/or a Customer (whatever the case may be) does not guarantee the settlement of any Transaction.

2.2 The Buyer acknowledges that the Acquirer and the E-Money Issuer shall be solely responsible for paying the remittance to the Buyer and for the Authorisation and settlement of Transactions in accordance with the terms of the Buyer's agreement with the Acquirer and E-Money Issuer.

2.3 The Buyer is responsible for reconciling the settlement monies received from the Acquirer with the Transactions submitted to the Processor for processing and to immediately notify the Processor if there is any material discrepancy.

2.4 For clarification purposes, neither the Processor nor the Supplier accepts any liability to the Buyer for any losses, damages, costs or expense arising out of any failure to pay a remittance to the Buyer on the relevant due date. This is because the Processor does not perform the settlement function and will not enter into possession of and or have control over any settlement funds at any time.

2.5 Transactions submitted to the PCP Service are settled via electronic delivery of Settlement Files to the Acquirer.

2.5.1 Delivery of such Settlement Files to the Acquirer will be accomplished within 2 (two) Business Days from when a Transaction is submitted to the Processor.

2.5.2 The Processor will make reasonable attempts to deliver the files but is not responsible for acceptance of the file by the Acquirer and or the Acquirer's system, the Scheme and or network.

2.5.3 The Processor will take all reasonable steps to process the Transactions in such a way that the Data is delivered to the relevant financial agent in a way acceptable to the relevant Acquirer and in accordance with the agreed formats.

2.5.4 If an Acquirer informs the Processor of an issue with the format of the file, the Processor will take reasonable steps to resolve the formatting issues and re-submit the Transaction Data to the Acquirer.

2.5.5 The Processor will not be responsible for any settlement problems providing the data is delivered in the correct formats to the relevant financial agent in a way acceptable to the relevant Acquirer.

2.5.6 The Buyer is responsible for reconciling payments received with Transactions processed, and should notify the Processor immediately if the Buyer becomes aware of a discrepancy in the payments received in settlement, the reporting available to the Buyer via the Payment Processing Service.

3. **PCI-DSS**

3.1 The Supplier warrants that the Processor will comply with all or any of its PCI-DSS obligations and or requirements in accordance with the Processor's accreditation.

3.2 The Processor is responsible for securing Payment Data which is solely in the possession of and under the control of the Processor. The Processor complies with its accreditation as PCI-DSS service provider. PCI-DSS sets out the industry standards for maintaining a secure environment.

A copy of the Processor's PCI-DSS compliance certificate can be requested by contacting the Processor's Buyer support team via the contact details displayed on the Processor's web site.

3.3 The Buyer warrants it will comply with all or any PCI-DSS obligations and or requirements including but not limited to the Buyer's reporting, scanning and Payment Data obligations and or such other fraud protection policies as may be approved or required by the Schemes from time to time and shall provide the Processor with immediately notification of any breach or failure to comply;

3.4 The Buyer will not retain or store any Security Data except to the extent necessary for the authorisation of the relevant Transaction. The Buyer undertakes immediately after completion of each Transaction to procure the secure deletion or destruction of all associated Security Data. If the Buyer knows or has reason to believe that any Payment Data (including Security Data) has been or may be lost, stolen or otherwise compromised, it shall immediately notify the Processor of the same and provide full details of the circumstances leading to the relevant security breach.

3.5 The Buyer is responsible for securing Payment Data in the Buyer's possession and for compliance with the Buyer's PCI-DSS obligations.

3.6 The Parties agree the content of this Agreement may be disclosed to an approved PCI-DSS auditor for the purpose of a PCI-DSS audit.

4. **Compliance**

4.1 The Buyer will comply with all Scheme Rules, applicable laws, regulations and codes of practice in the execution and performance of the Agreement and shall not use the Service or permit the Service to be used in any manner which could, in the Supplier's reasonable opinion, damage the Supplier's reputation, the Processor's reputation or the reputation of any company within the Supplier Group.

4.2 The Buyer warrants in submitting Transactions for processing, the Buyer is fully and promptly complying with:

4.2.1 Scheme Rules, E-Money Issuer instructions and or the terms of the Client Acquiring Contract;

4.2.2 The Processor's Acceptable Use Policy and Buyer Operational Guide and any reasonable operating instructions or procedural guides which the Processor may issue from time to time;

4.2.3 Applicable laws, regulations, licensing obligations, restrictions and orders including but not limited to the appropriate declarations, payments, approvals and or disclosures required to be made to or received from any regulatory and or tax authority as a consequence of or arising in connection with the Transaction;

4.2.4 In relation to accepting Payment Cards or E-Money Account payments (whatever the case may be) in payment for goods and/or services supplied by the Buyer.

4.3 Any breach by the Buyer of the provisions of this paragraph 4 shall be deemed a material breach that is not capable of remedy for the purposes of this Service Schedule.

4.4 The Buyer shall take all reasonable steps to detect and prevent fraud against the Supplier or any Customer or other party involved in a Transaction. The Buyer shall immediately notify the Supplier and the Processor if it knows or has reasonable grounds to suspect any fraudulent activity is being or may be committed in relation to the Service.

5. **<u>Buyer obligations – Payment Processing</u>**

5.1 The Buyer shall promptly provide to the Supplier and/or the Processor such information (including details of its account with the Acquirer and where relevant with the E-Money Issuer) as may be requested by the Processor for the purposes of activating the Service.

5.2 The Buyer acknowledges that any delay or failure to provide information and to comply with its obligations under this paragraph 5 may result in the Supplier being unable to provide the Service. Neither the Supplier nor the Processor accept responsibility for any losses, costs, damages or other liabilities arising from their inability to provide the Service in such circumstances.

5.3 The Buyer represents and agrees that:

5.3.1 it has obtained all permissions, approvals, consents and releases necessary in connection with the Buyer Product provided in relation to the Transactions (including but not limited to the Intellectual Property Rights of any third party) and that the Transaction and the Client Product relating to the Transaction is not in any way unlawful;

5.3.2 All information provided to the Supplier in connection with its application for Services and any other information it provides under this Agreement is correct and that no information has been withheld which could reasonably be expected to have adversely affected the Supplier's decision to enter into the Agreement;

5.3.3 In submitting Transactions for processing, the Buyer is complying with all applicable licensing obligations, Scheme Rules, Acquirer instruction, laws, regulations, restrictions and orders including but not limited to the appropriate declarations, payments, approvals and or disclosures required to be made to or received from any regulatory, tax authority, Scheme and or third party as a consequence of or arising in connection with the Transaction;

5.3.4 It will notify the Supplier of any and or all Buyer web site(s) selling and or providing the Customer with the Client Product and to be supported by the Service under this Service Order;

5.3.5 It has or will have prior to processing any Transactions a Client Acquiring Contract and that no Transactions will be submitted to the Processor unless a valid and current Client Acquiring Contract is in place

5.3.6 The Buyer will comply with the Processor's Acceptable Use Policy.

5.3.7 The Buyer has and will maintain all necessary consents to enable the Buyer to submit a recurring Transaction to the Acquirer for processing and will comply with any legal and/or regulatory obligations applicable thereto.

5.3.8 Where the Buyer submits as Scheduler for fixed and/or variable payments to be processed, the Buyer is responsible for the accuracy of any data including but not limited to Payment Data included therein.

5.4 The Buyer is responsible for resolving all disputes with Customers or other parties to a Transaction and undertakes to act in a reasonable manner to resolve them and shall ensure that the neither the Supplier nor the Processor is cited, contacted or requested for information in relation to such disputes. The Buyer acknowledges that neither the Supplier nor the Processor provide support to Customers and the Buyer agrees to take sole responsibility for dealing with any questions, complaints or enquiries raised by any Customer in relation to a Transaction.

5.5 Any Transaction which has been accepted where the Customer is not present is taken entirely at the Buyer's own risk. The Buyer acknowledges and accepts that a Transaction of this nature may be subject to a later dispute, even where an authorisation was provided at the point of sale. The Buyer acknowledges that the Buyer is responsible for any Chargeback arising from a Transaction.

5.6 The Buyer is responsible for complying with the Site Content Policy (a copy of which can be provided upon request). Neither the Supplier nor the Processor shall be responsible for any losses, liabilities and expenses due to or arising from any failure by the Buyer to comply with

the Site Content Policy and or the Buyer instructions available on such site or notifications emailed to the Buyer.

6. **Acquirer Client Acquiring Contract**

6.1 The acquisition services offered by the Acquirer are subject to a separate contract. Nothing in this Agreement shall purport to limit the ability of the Acquirer to terminate the Acquirer's Client Acquiring Contract and or vary any terms that apply therein.

6.2 Neither the Supplier nor the Processor is authorised to vary the terms or conditions contained in an Acquirer's Client Acquiring Contract.

6.3 The Buyer acknowledges that the Processor may not process Card Processing Transactions unless the Buyer has a valid and current Client Acquiring Contract.

6.4 Any changes to the Acquirer are subject to the prior written consent by the Supplier and/or the Processor such consent not to be unreasonably withheld or delayed and may include a variation and or increase in the Charges for the Service.

6.5 The Buyer acknowledges that changes to the Buyer's Acquirer may result in an interruption to the Service. The Supplier shall take reasonable steps to notify the Buyer if the Supplier believes the change in the Buyer's Acquirer will cause any such interruption to the Service.

6.6 If so requested by the Buyer, the Supplier or the Processor may introduce the Buyer to a new Acquirer for the purpose of obtaining a Client Acquiring Contract. The Parties acknowledge that the Acquirer is not required to offer a Client Acquiring Contract to the Buyer and the Buyer's application for a Client Acquiring Agreement will be subject to the Acquirer's own acceptance criteria including risk, regulatory and compliance review.

7. **Acceptance and authorisation**

7.1 If so offered by a Customer, the Processor will accept for processing a Payment Card or other payment which the Processor is authorised to accept. Acceptance for processing and on-line authorisation of the Transaction does not guarantee payment by the Customer or otherwise.

7.2 Acceptance of a Transaction by the Processor shall in no way either directly or indirectly prove or be deemed to prove the validity of any Transaction or Transaction receipts. The Processor gives the Buyer no assurances that any Transaction will be honoured or that the Processor shall not exercise any Chargebacks or other rights of reduction or set-off under this Agreement even where such Transaction has been authorised.

7.3 In accepting the Transaction for processing, the Supplier shall not be required to validate or confirm the consents and/or authorisations obtained by the Buyer from the Customer.

8. **Scheme Processing Instructions**

8.1 The Buyer acknowledges that in accordance with Scheme Rules the data controller of personal data relating to the Transaction is the Acquirer, E-Money Issuer, Payment Card Issuer and/or the Scheme and the Scheme Rules will be the instruction applicable to any such processing.

8.2 The Buyer agrees that the Processor will not be required to process Payment Data other than in accordance with the data controller's instructions as specified in the Scheme Rules including but not limited to any obligations imposed under PCI.

9. **Exclusions**

9.1 Subject to clause the limitation of liability clause in the G-Cloud 15 Call Off Contract , neither the Supplier nor the Processor shall be liable to the Buyer whether in contract (including under any indemnity or warranty), in tort (including negligence), under statute or otherwise for any:

9.1.1 Loss or corruption of Payment Data where the Supplier is unable (due to circumstances beyond its control) to provide back-up data;

9.1.2 Buyer processing charges with third parties; or

9.1.3 At the request of the Buyer, integration to the Supplier and or other systems or operational costs associated with the Buyer's use of the Services;

9.1.4 Cardholder compensation payments (including but not limited to not ex gratia payments) or and costs associated with Cardholder disputes.

10. **Payment Transaction Information**

The Buyer will also pay the Acquirer for the acquiring services received by the Buyer under the Client Acquiring Contract. Details of these fees and charges are contained in the Client Acquiring Contract and do not form part of this G-Cloud 15 Call Off Contract.

11. **Retention of Data**

11.1 The Supplier shall not be required to retain Customer Data and/or Payment Data provided in relation to or processed in relation to this Service upon termination of the Service.

11.2 Upon termination of this Agreement for any reason, the Buyer shall be required no later than 28 (twenty-eight) days from the date of termination to arrange for either:

11.2.1 The Data to be transferred to the Buyer and/or a third party nominated by the Buyer; or

11.2.2 Provide instructions to the Supplier to delete the Data

Providing always that Payment Data may only be transferred in accordance with the Supplier's PCI obligations.

11.3 If the Buyer fails to provide instruction to the Supplier within 14 (fourteen) days of termination of the Services, the Supplier shall, within 28 (twenty-eight) days of the date of termination, delete the Customer Data and within 180 (one hundred and eighty) days of the date of termination, delete the Payment Data.

11.4 If the Buyer wishes the Customer Data or the Payment Data to be transferred by the Supplier the Data migration process as set out in paragraph 12 below will apply.

12. **Data migration**

12.1 Inward migration: If, in order to perform the Service, Data has to be transitioned or migrated from the Buyer and/or the Buyer third party to the Supplier, the Parties shall, within 28 (twenty-eight) days of the Commencement Date, use their reasonable endeavours to agree a detailed, specific and itemised chronological transition and migration plan ("Inward Migration Plan").

12.2 Outward migration: Within 10 (ten) Banking Days of a notice of termination, the Parties shall meet in good faith to agree a plan and methodology ("Migration Plan") for the transfer of the Buyer's Customer Data and Payment Data (individually and collectively "Migration Data").

12.3 The Migration Plan shall consider the following:

12.3.1 Encryption technology to be used to protect the Migration Data in transit.

12.3.2 A mechanism for obtaining and applying the encryption keys required to access the Migration Data upon receipt by the Buyer and/or Buyer's service provider.

12.3.3 Data format and fields.

12.3.4 Name, address and contact details of the recipient of the Customer Data;

12.3.5 Name, address and contact details of the recipient of the Payment Data (if different to the Customer Data recipient).

12.3.6 Validation procedures for ensuring the Payment Data is transferred to a PCI compliant organisation or such similar accreditation level applicable to the recipient as required by the Schemes at the time of the Transfer;

12.3.7 The Transfer Date for the Migration Data such date to be no later than the date of termination of the Services;

12.3.8 The method of Transfer of the Migration Data;

12.3.9 Duplicate Migration Data is to be held by the Supplier post the Transfer Date;

12.3.10 The date the Supplier should cease processing if the Transfer Date precedes the termination date of the Services;

12.3.11 The date for deletion by the Supplier of the duplicate Migration Data being no later than 180 (one hundred and eighty) days from the date of termination of the Services.

12.3.12 The Charges payable by the Buyer for the Migration Plan activities, if any additional, which shall not exceed the Supplier's standard applicable charges for such services.

12.4 Nothing in this paragraph 12 will require the Supplier to transfer Payment Data to an organisation that is not a PCI compliant party and/or that meets the PCI standards required for receipt of such Payment Data in compliance with PCI-DSS standards.

Appendix Two: Generic Specification for the Multipay Platform

MultiPay Specification

Version 1.3

No part of this publication may be reproduced or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, or stored in a retrieval system of any nature without the written permission of PayPoint plc.

VERSION HISTORY			
Issue No.	Date	Author	Description
1.0	May 2020	Neal Simmons	Rewrite of the previous Generic Online Specification
1.1	Nov 2020	Neal Simmons	Inclusion of Instalment Plans to PaybyLink functionality
1.2	Jun 2021	Neal Simmons	Inclusion of Customer balances in Mobile App
1.3	Jan 2022	Neal Simmons	Inclusion of Open Banking Payments & DTMF Tone Masking Virtual Terminal

TABLE OF CONTENTS

MultiPay Solution Summary

PayPoint have created a multi-channel payment hub solution, called MultiPay. The MultiPay Solution contains the following services and payment channels

- Card Payment Acceptance – The core of the MultiPay Solution is to provide client's a resilient payment processing service that is PCI DSS compliant and secure.
- Open Banking – enabling a customer to make a payment direct from their own bank account to the clients using the banking network and Open Banking Framework.
- Transaction & Customer Management – The client can view real time data on their transaction and customer statuses using a client portal, event streamer and reconcile using the end of days SFTP files.
- Energy Sector Vend Service – Direct integration to the client energy vend service to allow the Vend Code (UTRN) to be returned to the customer.
- Multiple Payment Channels
    - White labelled Web Portal
    - White labelled Mobile APP
    - Direct API Integration
    - Pay by IVR
    - Pay by SMS
    - MOTO via a Virtual terminal
    - Recurring Payment Scheduler
    - PaybyLink
- Direct Debit bureau service - enabling the client using their own SUN to create Direct Debit schedulers.

Card Payment Acceptance

The MultiPay core service is to allow clients to accept credit/debit card payments from a range of ecommerce and MOTO channels. To achieve this the MultiPay solution has a payment processing platform that sends the card payments request for authorisation with the customer's card issuer. It also contains a tokenisation service to provide an additional layer of security and to ease the client's own PCI DSS compliance requirements.

Payment Processing

The MultiPay payment processing platform is hosted in a PCI DSS level 1 environment making sure that all payment card data stored or transmitted is secure and compliant.
The payment processing platform in addition integrates directly with two Payment Service Providers (PSP) allowing for automatic failure between the PSP's thus ensuring resilience of processing a payment request.
Upon receiving a payment pre-authorisation request from a Card Payment Channel the processing platform will create a transaction record, transform and send the request to the PSP. The result of the pre-authorisation is returned to the customer and if success we will send a capture request so the funds will be settled to the client's Merchant Account with their Acquirer.
The platform also contains a cleaner process which monitors for inconsistent transaction data and will attempt to complete a transaction by either voiding or capturing the transaction.

Tokenisation Service/Card Vault

The Tokenisation Service is hosted on a PCI DSS level 1 environment and generates a short-term token from the submission of the customer credit/debit card PAN. This token is then used instead of the credit/debit card PAN when submitting a payment request from a Card Payment Channel.
The short-term token is a short-lived token which is only valid for a period of time (5 minutes), after which the token will not be mapped back to the original PAN. During the creation of the short-term token the PAN is encrypted and stored in a distributed memory cache. It will be removed from the cache either during processing of the payment request or after 5 minutes.
When customers add their credit/debit card to their MultiPay account, we securely encrypt and store the credit/debit card details in a HSM Card Vault and create a stored card Id for that card. This stored card Id is then used instead of the credit/debit card details when the customer submits a Stored Card Payment.
When sending the payment request for authorisation with the card issuer, our PCI DSS compliant MultiPay solution uses the token/stored card id to retrieve the credit/debit card details from the Card Vault or distributed memory cache need by the card issuer for authorisation.

Transaction receipts

As part of the card payment acceptance, we can produce a transaction receipt that is sent to the customer as either an email or SMS message.

Email

Registered customers can choose whether they want to receive receipts by email. For a non-registered payment, the email receipt is optional and the user receives an email receipt by entering their email address at the payment stage.
All emails are sent from noreply@paypoint.com. The client must provide the sender name which the emails are sent 'from'.

SMS

The client may choose if SMS receipts should be sent to the customer across all their channels. If the client choice is 'yes' to SMS then the customer is prompted to enter an optional mobile phone number for a non-registered Payment across all channels. If the client has chosen to provide SMS receipts a registered customer can update their 'User Details' to 'Yes' for SMS receipts across all channels. If they then make payment by IVR, web or mobile app an SMS receipt is sent to their confirmed mobile phone number.
When the client choice is not to provide SMS receipts the IVR flow does not have the option to receive SMS receipt and the customer is able to listen to the receipt information at the time of the call.
There is an additional charge for SMS receipts.

Open Banking Payments

Upon request we can provide an Open Banking service that allows customer to make a payment direct from their own bank account to the client's bank account via a bank transfer. But instead of having to login to their online banking and manually go through the payment process step-by-step, with Open Banking this process can be initiated by our web and app payment channels, making the process faster and just as secure as the account holder explicitly consents to the payment request.

To make a one-off Open Banking payment the customer will need to add a service/product number which is then validated against the Client's own predefined validation rules. The customer will also need to choose/add the payment amount and select they wish to pay by Bank Transfer. The customer is then

presented list of banks where they will need to select the bank, they hold an account with. The customer then provides consent to access their bank account and is required to authenticate themselves with their bank. One authenticated the customer can authorise the Bank Transfer and funds will be transferred from their bank account to the client's bank account.
The payment response page is then displayed to the customer, detailing the confirmation of their payment consent and a valid Vend Code (UTRN), if applicable.
If the customer provided an email address, they would also receive an email transaction receipt.

Transaction & Customer Management

The client is provided with a range of management and reporting tool so they can have real time data on their transaction and customer statuses.

Client Portal

An online portal that allows the client's staff to respond to any card payment queries from their customers. The online client portal includes the following features:

- Search and export transaction records
- Perform refunds against transactions.
- A real-time dashboard view of payment activity
- Transactional volume and value analysis dashboard.
- Take a payment over the phone using the Virtual Terminal
- Request a payment from a customer using the PayByLink service
- Create a customer payment schedule for recurring or instalment payments
- Query and manage your customers activation status
- Reset a customer's password
- Preloaded customer and transactional reports
- Manage your own Admin portal users and security levels

End of Day Files and Event Streamer

The client can by request receive three daily end of day text files via SFTP:

- Payment Processing File – Transaction that have been completed and are due for settlement with the acquirer
- Transaction Activity File – All transactions including declines and vend retrieval requests
- Customer Activity File – Details of new customer registrations and existing customer changing their setup.

The client can also receive real time notification of a transaction using the PayPoint Event Steamer.
The PayPoint Event Steamer has been designed to allow the client's back office services to be informed when a transaction has occurred. The client will need to provide URLs for their endpoints/webhooks to receive real time transaction events. Once setup the client can receive real time transaction events from both the MultiPay Service and OTC Cash Payments made via PayPoint's Retail Network.

Energy Sector Vend Service

The MultiPay solution allows clients to be part of the online transaction flow, where we inform the client's vend services of a payment authorisation and a valid Vend Code (UTRN) is returned allowing for the transaction to be completed and funds captured.

Our real-time switch converts the customer details and transaction amounts into to APACS30 message and routes the request to the client's vend service or DCC adaptor. The result of the vend request is then returned to our MultiPay service where we complete the transaction and include the valid Vend Code (UTRN) in the transaction record and customer receipts.
When a transaction routed to the client's vend service fails to return a Vend Code (UTRN), then the MultiPay service will reverse the payment authorisation and inform the customer of the transaction failure.

Multiple Payment Channels

The MultiPay Solution provides Multiple Channels for customers to make a card payment, including:

White labelled Web Portal

The web portal is mobile responsive so can be viewed on any device and screen size. The customer accesses the white labelled web portal from their browser by visiting the URL:
https://<clientname>payments.paypoint.com/
Based on the URL the web portal identifies the client and uses their configurable parameters to apply the client's logo, colour and links to FAQ and T&C's.
The web portal provides the following functionality:

Non-Registered Card Payment

Customer can make a non-registered payments or Guest Payment, if they do not want to store their payment card details, where the customer is making the payment on behalf of someone else or when the customer wishes to only make a one-off payment.
The customer will need to add a service/product number which is then validated against the Client's own predefined validation rules. The customer will also need to choose/add the payment amount and securely enter their credit/debit card details.
The customer will then be prompted for addition cardholder authentication using 3D Secure (3DS) (according to the PSD 2 SCA & card scheme rules) when submitting the payment for authorisation.
The payment is sent for pre-authorisation with the customer's card issuer to check that the card is valid and that there are sufficient funds. Once authorised, if the client is using the Energy Sector Vend Service, the service will hold the capturing of the funds until a successfully and valid Vend Code (UTRN) is returned.
Where clients are not using the Energy Sector Vend Service the capture request is sent upon receiving the authorisation from the customer's card issuer.
The payment response page is then displayed to the customer, detailing the confirmation of payment details and the valid Vend Code (UTRN), if applicable.
If the customer provided an email address they will also receive an email transaction receipt.

Customer Registration

The Web Portal allows for customer to register for a MultiPay user account, which then allows the customer to make stored card payments against a stored service/product number.
When the customer registers the MultiPay solution displays the client's list of predefined service/product types where the customer select the first type and enters their associated service/product number. The MultiPay solution checks that this is a valid number by performing the validation rules configured for the client and the service.
For the Energy Sector Vend Service the service/product number must follow a defined 19 digit structure of:

Issuer Identifier Number (IIN)/Service specific code/Customer Account Number/Luhn Check Digit

The customer is then asked to provide an email address and the MultiPay solution will send an activation email containing a secure link and an activation code both of which are valid for 48 hours.

The customer can either click on the link in the email and is then able to provide their personal details and create a password. Alternatively the customer can enter the activation code into their website's registration page to then provide their personal details and create a password.
The MultiPay platforms user account security mechanisms based on the OAuth 2.0 standard

Storing and managing a service/product number

Once a customer has registered, they can add or delete additional service accounts from their user account. The customer can add a service by specifying the service/product number associated with the service and the solution checks that this is a valid number by performing the validation rules configured for the client and the service.
Service/product numbers must be added before a stored card payment can be made.

Storing and managing a payment card

Customers can either enter their chosen payment card during every transaction or they can securely add the payment card so that it is saved for future use. Customers are able to view all cards already setup, (part of the card number obfuscated), and can add additional cards or remove existing cards.
The customer can register and store an unlimited number of payment cards. A customer can define the default payment card that will be used when they request payments on the SMS channel and that will be selected first when making payments on Web and App.
All elements of the MultiPay platform used to capture payment card data are hosted in a PCI environment and make use of an API to replace a PAN with a short-term token. See Tokenisation Service.

Stored Card Payment

When making a registered payment the customer needs to choose the service/product account, choose/add the payment amount, and then select a stored payment card (the default payment card will be selected initially if there is more than one card stored). The customer will then need to add the stored card's CVV (Card Verification Value) and will be prompted for addition cardholder authentication using 3D Secure (3DS) (according to the PSD 2 SCA & card scheme rules) when submitting the payment for authorisation.
The payment is sent for pre-authorisation with the customer's card issuer to check that the card is valid and that there are sufficient funds. Once authorised, if the client is using the Energy Sector Vend Service, the service will hold the capturing of the funds until a successfully and valid Vend Code (UTRN) is returned.
Where clients are not using the Energy Sector Vend Service the capture request is sent upon receiving the authorisation from the customer's card issuer.

Payment History

Customers have access to a single view of all of their transaction history across all MultiPay channels, including: Web, Mobile, IVR, SMS and MOTO.
Retail (in store, cash) and Open Banking transactions can also be displayed on request.
The payment history shows from the earliest date the service/product number was registered by the customer and not older than 13 months.

User Management

Customers can amend their user account details, including name, mobile number, email address and password.
Mobile numbers are verified by SMS – a unique code is returned to the user's mobile phone which must be entered when they log back in to the system.

When a customer chooses to change their email address, a notification email is issued to the new email address with a link to activate it. A notification is also emailed to the previous email address for security reasons, to alert of the email address change.

White labelled Mobile APP (iOS/Android)

The MultiPay APP is a native mobile app, developed for both iOS and Android devices, which delivers the same functionality as the Web Portal service. The mobile app however offers an enhanced user experience, in terms of look and feel, over the mobile rendered responsive web portal and is available for free download from iTunes and Google Play.

The mobile app offers the following functionality:

- Non-Registered Payment
- Customer Registration
- Storing and managing a service/product number
- Storing and managing a payment card
- Stored Card Payment
- Payment History
- Balance Details
- User Management
- Display barcode for each store service/product card, so that it can be used to make Retail payments via the PayPoint Retail network.

The mobile app remains the property of PayPoint and is managed internally, but can be customised to match the client's icons, imagery and colour scheme.

Direct Integration

MultiPay also offers a public API which can be used by the clients to build their own channel apps. The API will expose the same functionality offered by the MultiPay web channel application and is built on the same underlying service stack.

The public API will offer the following functionality to the user:

- Tokenisation of a payment card
- Make a guest payment request
- Register a new MultiPay user and manage their credentials
- The ability to associate customer accounts with a MultiPay user account
- Retrieval of all user accounts and balances
- Activation and deactivation of MultiPay user accounts
- Updating customer account balances*
- Adding / deleting and managing payment cards
- Make a Payment with stored card details
- Getting the MultiPay users' payment history
- Creating and Managing PayByLink requests
- Making Account Verification and Merchant Initiated Payment requests for Payment Schedules
- Creating and Managing Payment Schedules

The public API is load balanced across two regions and will have 99.95% availability. Limits will be set on the rate at which each client can send requests to the API. Each response from a request will provide the client with their current rate and the rate limit, which the client can use to throttle transactions. The purpose of this is to protect the platform and all clients, when the platform is experiencing an unexpectedly high number of requests.

* As part of the Balance Enquiry functionality the service can send either a SMS or email to the customer when their balance is below a defined threshold.

Tokenisation Service API

The Public API includes a standalone service to enable the customer's Credit/Debit card number to be tokenised. The Tokenisation Service API is hosted on a PCI DSS level 1 environment and will provide the client with a short-term token which will be submitted in subsequent Public APIs call in place of the payment card PAN.
The short-term token is a short-lived token which is only valid for a period of time (5 minutes), after which the token will not be mapped back to the original PAN. During the creation of the short-term token the PAN is encrypted and stored in a distributed memory cache. It will be removed from the cache either during processing of the payment or penny-authentication or after 5 minutes.

Hosted Field

The Hosted Field solution allows the client to submit card payment authorisation requests from their website without the complexity of becoming PCI DSS complaint.
The Hosted Field solution renders the sensitive Credit/Debit Card Number input field into the client's website using an iframe that is hosted by PayPoint in our PCI DSS compliant zone.
The cardholder simply completes the Card Number (PAN) input field on our server, we then encrypt the cardholder's PAN and generate a Token which is then returned to the customer's browser. The Hosted Field solution provides a JavaScript Callback to receive the Card Token along with the Card's Scheme and Type.
The hosted Card Number (PAN) input field can also be easily customised to fit into your payment page design.

Developer Portal

The MultiPay API developer portal will be the central location for clients to obtain all information about the API and manage developer accounts. The portal will be used to host detailed API developer documentation defining the end points and signatures and will also provide developers with use cases and sample code.
A sandbox will also be provided for clients to allow them to develop their applications and allow them to perform transactions which are a facsimile of a full end to end transaction:

- A predefined set of payment card PANs will be defined and provided to allow the client to perform payments against them.
- Predefined PANs will also be defined and provided to allow the test Vend service to generate UTRNs.
- Certain combinations will be used to trigger failures in the payment and vending flows to allow clients to test their error handling.

The API sandbox environment is not a UAT or pre-production environment and will not allow the client to perform any load testing. This will be enforced by lower transaction rate limits.

Pay by IVR

MultiPay offers an IVR (Interactive Voice Response) channel for accepting customer payments. The IVR includes the facility for customers to make both non-registered payments and registered (stored payment card) payments using touch tone for data entry.
The client is assigned and provided with a unique UK geographic telephone number that customers can directly call. Alternatively, the client can choose to accept calls into their own chosen number and redirect that number to the MultiPay IVR.

The IVR flow is pre-recorded and dynamically uses the client's IVR configurations, to offer and validate appropriate options during the customer journey, such as: accepted payment card types, transaction limits, SMS receipts and transfers back to client's Contact Centre.
The client can also customise three of the IVR message prompts for an additional charge and potential increased to their on-boarding timescale.
The client and customise the Welcome, Goodbye messages and the default message that prompts the customer to enter their Customer ID/PRN PAN.
Customers who registered via the web/app, can see payments made via the IVR in their payment history.

Pay by SMS

SMS payments can be made by customers who have previously registered their service/product number on the web portal or mobile App.
PayPoint supplies the client a unique telephone number for customers to submit SMS payments. The number to which the customer sends the SMS is subject to standard mobile network text message rates.
Users must send an SMS in the correct format in order for the system to complete the validation rules.
PAY <CustomerId/PRN/PAN> <space> <amount> <space> <CVV>
CVV (Card Verification Value) is the security code located on the signature strip on the reverse of the payment card.
The SMS payment request then looks up the default stored payment card and sends a full payment request for authorisation with the card issuer and a SMS confirmation response is returned i.e.
Payment to Acc. 123456789 Total paid: £XX.XX Payment code: 12345 12345 12345 12345 Ref: 1231231231

If the customer has not set up a default payment card or the default stored payment card has expired, then the payment fails, and a message is displayed. Payments against the registered account appear in the customers payment history as payment type 'SMS'.

MOTO

A client can accept payments from customers by Mail Order and Telephone Order (MOTO) using a Virtual Terminal.
The Virtual Terminal can be used as a standalone service or in conjunction with accepting card transactions from our other channels.
The client accesses the Virtual Terminal via the Client Portal. The client portal user then enters an amount and the customer card details into the client portal to submit an authorisation request.
The payment will be sent for authorisation and the result will be displayed in the Client Portal. The transaction will be have the MOTO channel recorded against it allowing you to search by channel in the transaction search and EOD files.

DTMF Tone Masking Virtual Terminal

DTMF Tone Masking Virtual Terminal is an agent assisted payment solution for accepting Mail Order and Telephone Order (MOTO) transactions that utilises DTMF (Dual Tone Multi Frequency) masking technology. This solution integrates with the call flow and at the point of payment, intercept any keypad tones or speech from the customer. Meaning the agent doesn't hear or see the card data, all they see are asterisks on the screen. The customer and the agent can still converse throughout the process but the sensitive card data, the PAN and the CSV, are prevented from reaching the agent or your environment, drastically reducing the scope of PCI compliance.

The payment will be sent for authorisation and the result will be displayed to the agent in the DTMF Tone Masking Virtual Terminal. Following a successful payment, a confirmation receipt can be sent to the customer via an SMS or email.

Recurring Payment Scheduler

A client can take recurring/instalment payments from their customer either using their own Payment Scheduler and our direct API integration, or via our Payment Scheduler service.
The Payment Scheduler service is part of the Client Portal and allows the client to create and manage recurring/instalment payment schedules for their customers. A payment schedule is an agreement between the customer and the client to make a fixed payment on a regular interval. There are two types of payment schedule:

- **Recurring** – A transaction in a series of transactions processed for the purchase of goods or services provided at regular or fixed intervals.
- **Instalment** – A transaction in a series of transactions processed over a set period and number of payments for a single purchase of goods or services.

To create a payment schedule the client will need to log into the client portal and complete the 3 stages needed to create a new payment schedules.
The first stage is to complete the customer details which includes their email address used to notify the customer of the creation, edit and cancellation of their payment schedule.
The second stage requires the client to collect the customer card details. These card details are then submitted for account verification by the card issuer and authorised for use for continuous authority of subsequent scheduled payments.
The third stage is to complete the details of the payment schedule:
A recurring schedule requires a start date, the fixed amount of each payment, and the interval (weekly, fortnightly, monthly, quarterly or annually) and the schedule will run until it has been cancelled.
An instalment schedule requires a start date, the total amount to be paid, the interval (weekly, fortnightly, monthly, quarterly or annually) and then either the number of instalments or when the schedule needs to end. The solution then calculates each of the interval amounts and will run the schedule until the last payment has been taken determined by the payment count or end date.
Once created our Payment Schedule daily reviews all schedules that are due for payment and will send the payment request as a Merchant Initiated Transaction (MIT) for authorisation with the customer's card issuer.
The client can cancel a schedule or change the card used by the schedule using the Manage Schedule interface or APIs.

PaybyLink Service

The PaybyLink service allows clients to request a payment or repayment plan from their customers by sending the customer a URL to a pre-populated and Client Branded online payment page.
The client can generate a request for one off payment or a payment instalment plan directly by integrating into the PaybyLink service using our RESTful JSON API, alternatively can use the MultiPay Client Portal to raise a single request or multiple request using a bulk upload facility.
When the customer receives a request for one off payment or a payment instalment plan either via an SMS sent by the PaybyLink service or via the client's own communication channel, they will be presented a URL which will direct them to PayPoint's Hosted Payment Page.
The Hosted Payment Page renders the details of the client's request for one off payment or a payment instalment plan including the reason or passphrase and the Customer ID/PAN as a barcode so that it can be

used to make Retail payments via the PayPoint Retail network. The customer adds their card details into the fields provided and submits the one off payment or a payment instalment plan account verification to MultiPay' PCI DSS level 1 payment processing platform for authorisation.
The Hosted Payment Page can be customised by PayPoint to include the client's Logo and colour scheme. After the result of the authorisation request via the MultiPay payment processing platform, the Hosted Payment Page will display the response to the customer, in addition the PaybyLink request will be flagged with the appropriate status and if enabled a transaction callback is sent to the client.
A client using the MultiPay Client Portal can make a one off payment or a payment instalment plan request by finding an existing customer using the customer search and then selecting the Request a Payment button on the customer record. This will prepopulate the PaybyLink screen with the customer details and allows the client to add a reason/passphrase for the payment request and the amount. If a new customer, the client can still make a request for payment but is required to complete the customer details including name, and mobile number. The MultiPay Client Portal also provides a Bulk Upload screen where the client can upload a CSV file containing details of their request for a one off payment or a payment instalment plan, the Portal then reads the file and processes each request individually in the PaybyLink service.
The client portal reports on all PaybyLink requests raised and their status, from being SENT to OPENED and finally PAID/SCHEDULE CREATED.
The client can also customise the SMS message sent for PaybyLink request. Custom client SMS messages can occur an additional Fee if the SMS contents exceeds a 160 character segment limit.

Direct Debits Bureau Service

PayPoint offers a Direct Debit bureau service to our clients enabling them using their own SUN to create Direct Debit scheduler. The Bureau service provides clients with a web portal to allow the management of their Direct Debits. The Bureau service sends the scheduled Direct Debit Pull request to the BACs network for processing and provides reports on the responses.
PayPoint's Cloud- based Direct Debit portal is extremely flexible; offering everything from a gateway for submitting BACS files through to a fully comprehensive management portal.
Existing Direct Debits are seamlessly migrated across and new Direct Debit Mandates merged. Where PayPoint manages the Scheduling of Direct Debits, there is no disruption to Direct Debit collections, and the customer does not need to complete a sign up form again.

Supplier SLA
Card Processing Services

1. Performance Standards

Number	Performance Standards	Measure	Measurement Period
1	Availability of the Services	99.9% of hours	Quarterly
2	Provide the Daily Transaction File within 12 (twelve) hours of the end of the previous day	98.0% of files	Annually

2. Exceptions

The Buyer shall not receive any service credits in connection with any failure or deficiency of Services caused by or associated with any of the following:

2.1 Circumstances beyond the Supplier's reasonable control as set out herein.

2.2 Unavailability of or interruption or delay in telecommunications or third party services, or distributed denial of service attacks, failure of third party software or hardware, or inability to obtain raw material, supplies or power used in or equipment needed for provision of the Services save that the Supplier will use reasonable endeavours to procure that the relevant third party remedies the interruption as soon as reasonably possible.

2.3 Failure of access circuits to the Supplier's Network and/or Data Centre or processing facility owned and controlled by the Supplier, unless such failure is caused solely by the Supplier and in any event the Supplier will use reasonable endeavours to rectify such failure as soon as reasonably possible.

2.4 Scheduled maintenance, scheduled downtime, permitted maintenance, permitted downtime, emergency maintenance and upgrades provided that this is in accordance with the terms herein.

2.5 Domain Name Service ("**DNS**") propagation issues outside the direct control of the Supplier.

2.6 Issues with Buyer access to file transfers not caused by the Supplier.

2.7 Service level failures incorrectly reported as a result of outages or errors of any monitoring systems.

2.8 The Buyer's acts or omissions (or acts or omissions of others engaged or authorised by, including, without limitation, customer scripting or coding (e.g. CGI, Perl, HTML, ASP etc.); any negligence, wilful misconduct or use of the Services in breach of the Supplier Service Specific Terms, email or webmail delivery and transmission.

2.9 Internet routing issues outside the control of the Supplier.

2.10 Browser or DNS caching that may make the Service appear inaccessible.

2.11 The Buyer's Third Party Suppliers and/or Third Party Data Service Supplier, acquiring bank interface failures, failovers and outages whether primary (main server) or secondary (routing, VPN X25 connections etc.).

2.12 Use of an element of the Services released by the Supplier as a "Beta" or "Pilot" version.