Schedule 9 - Data Processing Terms and Conditions

1. INTRODUCTION

1.1 This Schedule 9 shall only apply to the extent that DNAP is Processing Protected Data.

1.2 In the case of any conflict or ambiguity between any of the provisions of this Schedule 9 and the other Schedules of this Agreement, the provisions of this Schedule 9 will prevail.

2. DATA PROCESSING

2.1 Each party acknowledges and agrees that for the purposes of Data Protection Legislation and this Agreement:

2.1.1 Unless specified otherwise, the Merchant shall be the Controller and DNAP the Processor in respect of the Protected Data for the purposes of Data Protection Legislation..

2.1.2 Notwithstanding anything to the contrary, in respect of the following circumstances, DNAP shall act as Controller over the Protected Data:

- where required for the purposes of DNAP's Anti-Money Laundering and Fraud obligations;
- to the extent required to comply with applicable legal obligations;
- to the extent required to comply with the Card Scheme Rules, or with any payment scheme rules or participant agreement applicable to DNAP.

2.1.3 When acting as a Controller, the Merchant remains responsible for its compliance obligations under the Data Protection Legislation, and for the written Processing instructions it gives to DNAP.

2.1.4 The Merchant shall, as a condition precedent to DNAP Processing the Protected Data, inform all Data Subjects concerned of the Processing of their Protected Data pursuant to the Agreement and, where required by Data Protection Legislation, such data subjects have given their unambiguous consent to such Processing in accordance with Data Protection Legislation in so far as such consent is necessary;

2.1.5 The Merchant shall ensure all Protected Data transferred to DNAP is accurate and up to date at the time it is collected and has at all times been collected, processed and transferred by and on behalf of the Merchant in accordance with Data Protection Legislation.

2.1.6 The Merchant shall, prior to any Protected Data being transferred to DNAP, from time to time , ensure that each Data Subject has been provided with sufficient information (in an appropriate form) so as to enable fair, transparent and lawful Processing of the Protected Data in accordance with the obligations under the Data Protection Legislation.

2.2 DNAP shall only Process the types of Protected Data relating to the categories of data subjects for the specific purposes in each case as set out in Annex 1 to this Schedule 9 and shall not Process the Protected Data other than in accordance with the Merchant's documented instructions (whether in the Agreement or otherwise) unless Processing is required by applicable law to which DNAP is subject, in which case DNAP shall, to the extent permitted by such law, inform the Merchant of that legal requirement before or as soon as possible after Processing that Protected Data.

2.3 DNAP shall inform the Merchant if, in its opinion, an instruction it receives from the Merchant pursuant to the Agreement or otherwise infringes or is likely to infringe Data Protection Legislation.

3. MERCHANT WARRANTY

3.1 The Merchant warrants that it has all necessary rights and has provided all relevant notices to data subjects to provide the Protected Data to DNAP for the Processing to be performed in relation to the Services.

3.2 The Merchant must notify DNAP promptly of any changes to the Data Protection Legislation or its activities that may reasonably be interpreted as adversely affecting the Merchants performance of this Agreement.

4. DNAP PERSONNEL

4.1 DNAP shall treat all Protected Data as confidential and shall use reasonable efforts to inform all its relevant employees, contractors and/or any Sub-processors engaged in Processing the Protected Data of the confidential nature of such Protected Data.

4.2 DNAP shall take reasonable steps to ensure the reliability of any employee, contractor and/or any Sub-processor who may have access to the Protected Data, ensuring in each case that access is limited to those persons or parties who need to access the relevant Protected Data, as necessary for the purposes set out in clause 2.2 in the context of that person's or party's duties to DNAP.

4.3 DNAP shall ensure that all such persons or parties involved in the Processing of Protected Data are subject to confidentiality undertakings or are under an appropriate statutory obligation of confidentiality.

5. SECURITY

5.1 Both the Controller and the Processor shall maintain written security policies that are fully implemented and applicable to the processing of Personal Data. At a minimum, such policies should include assignment of internal responsibility for information security management, devoting adequate personnel resources to information security, carrying out verification checks on staff who will have access to the Personal Data, conducting appropriate background checks, requiring employees, vendors and others with access to Personal Data to enter into written confidentiality agreements, and conducting training to make employees and others with access to the Personal Data aware of information security risks presented by the Processing.

5.2 DNAP shall implement appropriate technical and organisational measures, including those set out in Annex 2 to this Schedule 9, to ensure a level of security of the Protected Data appropriate to the risks that are presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data, as required under Data Protection Legislation.

6. SUB-PROCESSING

6.1 The Merchant hereby grants its general authorisation to the appointment of Sub-processors by DNAP under the Agreement.

6.2 As at the Commencement Date, the Merchant hereby authorises DNAP to engage those Sub-processors set out in Annex 1 to this Schedule 9.

6.3 DNAP shall inform the Merchant of any intended changes concerning the addition or replacement of such Sub-processors, thereby giving the Merchant the opportunity to object to such changes.

6.4 With respect to each Sub-processor, DNAP shall:

6.4.1 enter into a written contract with the Sub-processor which shall contain terms materially the same as those set out in this Schedule 9;

6.4.2 remain liable to the Merchant for any failure by the Sub-processor to fulfil its obligations in relation to the Processing of any Protected Data.

7. DATA SUBJECT RIGHTS

7.1 DNAP shall without undue delay, and in any case within three (3) Business Days, notify the Merchant if it receives any Data Subject Request and shall provide full details of that request. It shall be the Merchant's responsibility to reply to all such requests as required by applicable law.

7.2 Insofar as possible, DNAP shall provide such assistance as reasonably requested by the Merchant to enable the Merchant to comply with any Data Subject Request in accordance with the Data Protection Legislation provided the Merchant promptly notifies DNAP in writing of the information and/or assistance it reasonably requires.

8. INCIDENT MANAGEMENT

8.1 In the case of a Personal Data Breach, the affected party shall without undue delay and, in any event, not later than twenty-four (24) hours after having become aware of it, notify the Personal Data Breach to the other providing the other with sufficient information which allows the party to meet any obligations to report a Personal Data Breach under Data Protection Legislation.

8.2 Where a party becomes aware of any Personal Data Breach, it will, without undue delay, also provide the other party with the following written information:

(a) description of the nature of the Personal Data Breach including the categories of Protected Data and approximate number of both Data Subjects and the Protected Data records concerned;

(b) the likely consequences; and

(c) a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

8.3 Immediately following any accidental, unauthorised or unlawful Protected Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Merchant will reasonably co-operate with DNAP at no additional cost to DNAP, in DNAP's handling of the matter, including but not limited to:

(a) assisting with any investigation;

(b) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by DNAP; and

(c) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Protected Data Processing.

8.4 The parties will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Protected Data and/or a Personal Data Breach without first obtaining the other's written consent, except when required to do so by applicable law.

9. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

9.1 DNAP shall, at the Merchant's request, provide reasonable assistance to the Merchant with any data protection impact assessments which

are required under applicable Data Protection Legislation and with any prior consultations to any data protection supervisory authority of the Merchant which are required under Data Protection Legislation, in each case in relation to Processing of Protected Data by DNAP on behalf of the Merchant and taking into account the nature of the Processing and information available to DNAP.

10. DELETION OR RETURN OF THE PROTECTED DATA

10.1 Subject to clause 10.2, DNAP shall promptly and in any event within ninety (90) calendar days of the earlier of: (i) cessation of Processing of Protected Data by DNAP; or (ii) termination of the Agreement, at the choice of the Merchant either:

10.1.1 return a complete copy of all Protected Data to the Merchant by secure file transfer in such commercially reasonable file format as notified by the Merchant to DNAP and securely wipe all other copies of Protected Data Processed by DNAP or any Sub-processor; or

10.1.2 securely wipe all copies of Protected Data Processed by DNAP or any Sub-processor,

and in each case provide written certification to the Merchant that it has complied fully with this clause 10.1.

10.2 DNAP shall not be required to return or delete any Protected Data in accordance with clause 10.1 where it is required to retain such data in order to comply with applicable laws.

11. AUDIT RIGHTS

11.1 At the request of the Merchant, when acting as a Processor, DNAP shall demonstrate the measures it has taken pursuant to this Schedule 9 and shall allow the Merchant to audit such measures no more than once a year, unless the Merchant can demonstrate it suspects there has been a material breach by DNAP of its obligations under this Schedule. Unless otherwise required by a Supervisory Authority of competent jurisdiction, the Merchant shall be entitled on giving at least 30 days' notice to DNAP to carry out, or have carried out by a third party who has entered into a confidentiality agreement with DNAP, such audit under the present Clause 11.

11.2 Prior to conducting any audit pursuant to clause 11.1, the Merchant must submit an audit request in writing to DNAP and the Merchant and DNAP must agree the start date, scope and duration of and security and confidentiality controls applicable to any such audit.

11.3 DNAP may (acting reasonably) object to the appointment by the Merchant of an independent auditor to carry out an audit pursuant to clause 11.1 and, where this is the case, the Merchant shall be required to appoint another auditor who is not a competitor of DNAP, in DNAP's reasonable opinion.

11.4 Any such audit will be limited to a document audit only and no in-person audits of DNAP will be permitted to the fullest extent permitted by applicable law.

12. INTERNATIONAL TRANSFERS OF PROTECTED DATA

12.1 In the event that a transfer of the Protected Data to DNAP is reasonably considered to involve a transfer of the Protected Data outside of the UK which is not recognized by the European Commission as ensuring an adequate level of protection for Personal Data, DNAP shall, upon request, enter into Standard Contractual Clauses or a IDTA as appropriate with the Merchant or other relevant Sub-processor for such transfer of Protected Data.

13. COSTS

13.1 If Merchant's instructions exceed instructions reasonably required of a processor under Data Protection Legislation, DNAP shall notify Merchant without delay. Following notification DNAP shall be entitled to charge a reasonable fee for complying with such instructions. The Merchant shall pay any reasonable costs and expenses incurred by DNAP in meeting the Merchant's requests made under clauses 7, 9 and 11.

14. MISCELLANEOUS

14.1 Any obligation imposed on DNAP under the Agreement in relation to the Processing of Protected Data shall survive any termination or expiration of the Agreement.

14.2 The provisions of this Schedule 9 shall survive termination or expiry of this Agreement..

14.3 Any beach by the Merchant of any of its obligations under this Schedule 9 shall be regarded as being a material breach for the purposes of this Agreement.

15. INDEMNITY

15.1 The Merchant shall indemnify and keep indemnified DNAP against all losses, claims, damages, liabilities, fines, sanctions, interest, penalties, costs, charges, expenses, compensation paid to Data Subjects, demands, and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a supervisory authority) arising out of or in connection with any material breach by the Merchant of its obligations under this Schedule 9.

ANNEX 1: DATA PROCESSING INFORMATION

This Annex 1 to Schedule 9 includes certain details of the Processing of Protected Data as required by Article 28(3) GDPR.

Subject matter, nature and purposes of the Processing of Protected Data	Processing for the purposes of provision of the Services.
Duration of the Processing	The duration of the Agreement.
Type of Protected Data	Personal data including: • Addresses • Bank account number and bank routing number • Card information (such as Card Number, expiry date etc.) • Date of birth • Email address • Fax number • Gender • Government ID/Passport information • IP address • Nationality • Names • Telephone number • Transaction information • Username
Categories of data subjects	Customers.
Sub-processors	Relevant Acquirers.

ANNEX 2: SECURITY MEASURES

DNAP shall implement the following technical and organizational measures to protect Protected Data against accidental loss and unauthorised access, disclosure or destruction:

1. Governance and policies

DNAP assigns Personnel with responsibility for the determination, review and implementation of security policies and measures.

DNAP has documented the security measures it has implemented in a security policy and/or other relevant guidelines and documents.

2. Intrusion, anti-virus and anti-malware defences

DNAP IT systems used to Process Protected Data have appropriate security software installed on them.

3. Access controls

DNAP limits access to the Protected Data by implementing appropriate access controls. Access controls can include:

- Requiring authentication and authorisation to gain access to IT systems (i.e. require users to enter a user ID and password before they are permitted access to the IT systems);
- Only permit user access to Protected Data which the user needs to access in order to perform their job role or the purpose they are given access to DNAP's IT systems;
- Having in place appropriate procedures for controlling the allocation and revocation of access rights to the Protected Data. For example, having in place appropriate procedures for revoking employee access to IT system when they leave their job or change role.

4. Availability and back-up of Protected Data

DNAP regularly backs up information on IT systems and keep back-ups in separate locations.

5. Segmentation of Protected Data

DNAP will, as appropriate, separate and limit access between network components and where appropriate implement measures to provide for separate Processing (storage, amendment, deletion, transmission) of Protected Data collected and used for different purposes.

6. Encryption

DNAP uses encryption technology where appropriate to protect the Protected Data.

7. Transmission or transport of the Protected Data

Appropriate controls will be implemented by DNAP to secure the Protected Data during transmission or transit.

8. Physical security

DNAP implements physical security measures to safeguard Protected Data. Such measures may include:

- buildings are appropriately secured;
- measures taken to prevent Protected Data from being read, copied, amended or moved by any unauthorised persons;
- hard copy documents containing Protected Data are only taken off site where necessary to achieve the purposes of the Agreement; and
- paper records which contain confidential information (including Protected Data) must be shredded after use in accordance with industry standards.

9. Staff training and awareness

DNAP carries out staff training on data security and privacy issues relevant to employees' job role and ensures that new starters receive appropriate training before they start their role (as part of the on boarding procedures).

Staff are subject to disciplinary measures for breaches of DNAP's policies and procedures relating to data privacy and security.

10. Selection of service providers

DNAP assesses service providers' ability to meet their security requirements before engaging them.

DNAP has written contracts in place with service providers which require them to implement appropriate security measures to protect the Protected Data they have access to and limit the use of Protected Data in accordance with DNAP's instructions.