Effective 27th December 2022

BLUESNAP DATA PROTECTION ANNEX

This BlueSnap Data Protection Annex ("**DPA**") applies between Merchant and BlueSnap and replaces and cancels any prior DPA between the parties. The parties agree that the Standard Contractual Clauses applicable pursuant to this DPA take priority over any conflicting terms in this DPA. If there is any conflict between this DPA and the Agreement regarding BlueSnap's privacy and security obligations, the provisions of this DPA shall control.

1. Definitions

1.1 In this DPA, the following terms have the meaning given to them below:

"**CCPA**" means the California Consumer Privacy Act 2018 and any legislation and/or regulation implementing or made pursuant thereto, or which amends, replaces re-enacts or consolidates.

"**Customer**" means a customer of Merchant purchasing products and/services.

"**Customer Personal Data**" means the personal data relating to Customers which is processed by BlueSnap in the provision of the BlueSnap Services to Merchant.

"**EEA**" means the European Economic Area.

"**European Privacy Law**" means any data protection, privacy, confidentiality or security laws or regulation of Switzerland, the United Kingdom or a country within the EEA (including, as applicable, the GDPR) applicable to the processing of personal data under this Agreement..

"**European Personal Data**" means Merchant Personal Data and Customer Personal Data the processing of which is within the material and territorial scope of European Privacy Law.

"**EU SCCs**" means the applicable module (as stated in clause 8.2 of this DPA) of the standard contractual clauses for the transfer of personal data to third countries adopted pursuant to the European Commission's Implementing Decision (EU) 2021/914 of 4 June 2021 and, for the purposes of Merchant Restricted Transfers, on the basis that:

(i) where module 2 (transfer controller to processor) applies in accordance with clause 8.2 of this DPA, for the purposes of clause 9 of the EU SCCs, option 2 (general written authorisation) applies and the specified time period is 7 days before such changes take effect;

(ii) where either module applies:

(a) the optional docking clause 7 is deleted;

(b) the independent dispute resolution option in clause 11 of the EU SCCs does not apply;

(c) for the purposes of clause 13(a) of the EU SCCs: (i) where the Merchant is established in an EEA Member State, the supervisory authority with responsibility for ensuring compliance by the Merchant with European Privacy Law as regards the data transfer shall act as the competent supervisory authority; and (ii) where the Merchant is not established in an EEA Member State but falls within the territorial scope of application of European Privacy Law according to Article 3(2) of the GDPR (or equivalent), the supervisory authority of the Member State in which the Merchant has appointed a representative within the meaning of Article 27(1) GDPR (or equivalent) shall act as competent supervisory authority;

(d) for the purposes of clause 17 of the EU SCCs, the chosen option is option 1 and the chosen law is the law of Ireland;

(e) for the purposes of clause 18(b) of the EU SCCs, the chosen courts are courts of Ireland;

(f) Appendix 1, Section A of this DPA operates as Annex I to the EU SCCs; and

(g) Appendix 1, Section B of this DPA operates as Annex II to the EU SCCs.

"**GDPR**" means Regulation (EU) 2106/679.

"**Merchant Personal Data**" means personal data, other than Customer Personal Data, that is provided by or on behalf of Merchant to BlueSnap under the Agreement.

"**Merchant Restricted Transfer**" means a transfer by the Merchant of European Personal Data to BlueSnap in a country or territory which does not ensure an adequate level of data protection within the meaning of European Privacy Laws to the extent European Privacy Laws apply to the Merchant's processing when making that transfer.

"**Personal Data Breach**" means a personal data breach in respect of Customer Personal Data processed by BlueSnap as processor pursuant to clause 2.1(i)(c) of this DPA.

"**Privacy Law(s)**" means data protection, privacy, confidentiality or security laws or regulation, including, but not limited to, European Privacy Law, US Federal or state law applicable to the processing of personal data under the Agreement.

"**Standard Contractual Clauses**" or "**SCCs**" means:

(i) the EU SCCs for Merchant Restricted Transfers made by the Merchant to BlueSnap in respect of European Personal Data, to the extent European Privacy Laws of the EEA apply to the Merchant's processing when making that transfer;

(ii) the Swiss SCCs for Merchant Restricted Transfers made by the Merchant to BlueSnap in respect of European Personal Data, to the extent European Privacy Laws of Switzerland apply to the Merchant's processing when making that transfer, and

(iii) the UK SCCs for Merchant Restricted Transfers made by the Merchant to BlueSnap in respect of European Personal Data, to the extent European Privacy Laws of the UK apply to the Merchant's processing when making that transfer.

"**Sub-processor**" means any processor engaged by BlueSnap to process Customer Personal Data.

"**Swiss SCCs**" means the EU SCCs, as amended by Appendix 2 of this DPA.

"**UK SCCs**" means the UK SCC Addendum on the basis that:

(A) Table 1 and Table 3 of the UK SCC Addendum are deemed to have been completed with the corresponding details set out in Appendix 1 to this DPA and, for the purposes of Table 1 of the UK SCC Addendum,

i. the "Start Date" is the later of the effective date of this DPA and the commencement of the Merchant Restricted Transfer (to which European Privacy Laws of the UK apply); and

ii. the official company registration numbers (where applicable) of the parties are as set out in the Agreement;

(B) for the purposes of Table 2 of the UK SCC Addendum, the first box is ticked and (1) the version of the "Approved EU SCCs" is the EU SCCs; and (2) the applicable modules are as set out in clause 8.2 of this DPA; and

(C) "Importer" is deemed to have been chosen for the purposes of Table 4 of the UK SCC Addendum.

"**UK SCC Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B.1.0) issued by the UK Information Commissioner and laid before UK Parliament in accordance with s119A of the UK Data Protection Act 2018 on 2 February 2022.

1.2 In addition, the terms "controller", "processor", "data subject", "personal data", "process", "processing", and "processor" have the meanings given to them in the GDPR.

2. Data Processing Roles (European Privacy Law).

2.1 With respect to the processing of:

(i) Customer Personal Data within the material and territorial scope of European Privacy Law:

(a) Customer Personal Data is provided by or on behalf of Merchant, as independent controller, to BlueSnap;

(b) BlueSnap receives and processes Customer Personal Data, as independent controller, for the purposes of (1) monitoring and preventing fraudulent transactions; (2) BlueSnap's compliance with BlueSnap's legal and regulatory obligations relating to the collection, processing, storing or retention of Customer Personal Data following a transaction; and (3) acting as merchant of record as set out in Section I.B. of the Merchant Agreement;

(c) Merchant instructs BlueSnap, in other respects, to receive and process Customer Personal Data, as Merchant's processor, in the provision of the BlueSnap Services to Merchant.

(ii) Merchant Personal Data within the material and territorial scope of European Privacy Law:

(a) Merchant Personal Data is provided by or on behalf of Merchant, as independent controller, to BlueSnap; and

(b) BlueSnap, as independent controller, receives and processes Merchant Personal Data including for the purposes of (1) setting up and administering Merchant's account; (2) performing merchant underwriting; (3) conducting checks and reviews relating to KYC, anti-money laundering, identity, credit status, reference, financial status, beneficial interests, location, tax status and other related matters; (4) monitoring and preventing fraudulent transactions, and (5) BlueSnap's compliance with BlueSnap's legal and regulatory obligations relating to the collection, processing, storing or retention of Merchant Personal Data following a transaction.

2.2 The subject matter, duration, nature and purpose of the processing, and type of personal data and categories of data subject processed by BlueSnap as the Merchant's processor in accordance with clause 2.1(i)(c) is set out in Appendix 1.

3. Data Processing Role (CCPA).

3.1 With respect to the processing of personal information within the material and territorial scope of the CCPA:

(i) BlueSnap acts as service provider and certifies that it understands and shall comply with such contractual restrictions as may have been set by Merchant in writing;

(ii) without derogation from such contractual restrictions, BlueSnap acknowledges and confirms that it does not receive any personal information as consideration for any services or other items that BlueSnap provides to Merchant under the Agreement;

(iii) BlueSnap shall not have, derive, or exercise any rights or benefits regarding personal information processed on Merchant's behalf, and may use and disclose personal information solely for the purposes for which such personal information was provided to it, as stipulated in the Agreement and this DPA;

(iv) BlueSnap certifies that it understands the rules, requirements and definitions of the CCPA and agrees to refrain from selling (as such term is defined in the CCPA) any personal information processed under this Agreement, and to refrain from taking any action that would cause any transfer of personal information to or from BlueSnap under the Agreement or this DPA to qualify as "selling" such personal information under the CCPA;

(v) for the purposes of the CCPA, BlueSnap receives Customer Personal Data and Merchant Personal Data from Merchant pursuant to a business purpose, in accordance with and to fulfill its obligations under its Agreement with Merchant and in accordance with other lawful and reasonable instructions as may be provided by Merchant from time to time; and

(vi) BlueSnap agrees that it will not sell, access, disclose or use Merchant Personal Data and/or Customer Personal Data except as necessary to fulfill its obligations to Merchant under the Agreement or as necessary to carry out Merchant's lawful and reasonable instructions to BlueSnap

4. **Compliance with laws**.

4.1 Each party will comply with all laws, rules, and regulations applicable to it and binding on it in the performance of this DPA, including all Privacy Laws.

4.2 The Merchant is responsible for reviewing the information available from BlueSnap relating to the BlueSnap Services and data security and making an independent determination as to whether the BlueSnap Services meet its requirements and legal obligations as well as its obligations under this Agreement.

4.3 Merchant is solely responsible for complying with its obligations as independent controller under European Privacy Laws in relation to Customer Personal Data and Merchant Personal Data, including the requirement to have a valid legal basis for the provision of the personal data to BlueSnap (including obtaining consent from data subjects, if applicable), to comply with data subject requests under the GDPR and to provide the relevant data subjects with the information (including any data privacy notices) required under Article 13 or 14 GDPR with regard to the provision of their personal data to BlueSnap for the purposes set out in clause 2.1. Merchant shall provide all such data subjects with a link to BlueSnap's privacy policy (available at https://home.bluesnap.com/privacy-policy) or other information sufficient to ensure BlueSnap's compliance, to the extent it is a controller, with its obligations under Article 14 GDPR.

4.4 The Merchant shall ensure that the processing by BlueSnap of the Customer Personal Data as processor or otherwise in accordance with its instructions and the Merchant Personal Data does not cause or result in BlueSnap or the Merchant breaching any laws, rules or regulations (including Privacy Laws).

5. **BlueSnap Processing Obligations**.

5.1 BlueSnap shall, to the extent it acts as processor of Merchant in the processing of Customer Personal Data in accordance with clause 2.1(i)(c):

(i) only process Customer Personal Data on behalf of Merchant and in accordance with Merchant's written instructions set out in the Agreement and this DPA, unless required to do otherwise by applicable law to which BlueSnap is subject; in such a case, BlueSnap shall inform the Merchant of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(ii) ensure that persons authorised by BlueSnap to process Customer Personal Data are subject to a binding duty of confidentiality;

(iii) take steps to ensure that any natural person acting under BlueSnap's authority who has access to Customer Personal Data does not process them except on instructions from BlueSnap, unless he or she is required to do so by applicable law.

(iv) implement the technical and organisational security measures set out in Appendix I in respect of the Customer Personal Data;

(v) provide reasonable assistance, at Merchant's expense, to Merchant to assist the Merchant complying with its obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to BlueSnap;

(vi) upon request by Merchant and at its expenses, provide reasonable assistance to Merchant, by appropriate technical and organisational measures, insofar as this is reasonably possible, to assist Merchant in the fulfilment of its obligations to respond to requests for exercising data subject rights under Chapter III of the GDPR, taking into account the nature of the processing;

(vii) subject to reasonable notice, enable Merchant to access and review up-to-date security certifications, attestations, reports or extracts of them from independent bodies relating to compliance with the security requirements of this DPA and, if necessary, make available other information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR;

(viii) provide Merchant an opportunity to conduct a security audit of BlueSnap's security program and systems and procedures that are applicable to the services provided by BlueSnap to Merchant subject to BlueSnap's confidentiality agreement. Audits will occur at most annually or following notice of a Personal Data Breach. Alternatively, Merchant may request in writing a copy of the most recent audit of such services conducted on behalf of BlueSnap by an independent third party security professional at Merchant's selection and expense. Merchant shall promptly provide a copy of such audit report to BlueSnap without charge. If any such audit reveals any vulnerability, BlueSnap shall take reasonable steps to correct such vulnerability at its sole cost and expense;

(ix) to the extent required to notify Merchant of a Personal Data Breach under Privacy Laws, notify Merchant of any Personal Data Breach within 48 hours of discovery and provide Merchant with the information set out in Article 33(3) GDPR – where it is not possible to provide the information at the same time, BlueSnap may provide it in phases without undue further delay; and

(x) subject to BlueSnap's rights and obligations under this Agreement (including this DPA), at Merchant's choice, delete or return all Customer Personal Data, and delete existing copies held by BlueSnap, unless BlueSnap is required or authorised by applicable law (e.g. for the establishment, exercise or defence of legal claims, until time barred) to store Customer Personal Data for a longer period (provided that any deletion will take place as soon as reasonably practical based upon BlueSnap's next deletion run which is normally every thirty days, and may be implemented by rendering the Customer Personal Data no longer personal data).

5.2 All documentation provided by BlueSnap, including any response to a security or other questionnaire, is BlueSnap's confidential information.

6. **Sub-processing**.

6.1 Merchant confirms that BlueSnap has a general authorisation to use Sub-processors in the performance of the BlueSnap Services. BlueSnap maintains an up-to-date list of its Sub-processors used for processing under this Agreement at https://home.bluesnap.com/legal/BlueSnapDPASubprocessors.

6.2 Merchant must subscribe to receive notifications of additional or changes to Sub-processors by emailing DPAList@bluesnap.com with a request to subscribe to the DPA Sub-processor list. BlueSnap shall notify Merchant of any additions or changes of Sub-processors within 7 days prior to such changes taking effect by email to the email which Merchant subscribed by emailing DPAList@bluesnap.com. Merchant shall have the opportunity to object to the engagement of new Sub-processors within 30 days of the issue of such notice. The objection must be based on reasonable legitimate grounds such as where the Sub-processor presents significant data protection risks for the protection of Customer Personal Data. If the parties are unable to resolve such objection, then either party may terminate the Agreement on providing 30 days' written notice without penalty.

6.3 BlueSnap will enter into a written agreement with each Sub-processor that imposes on that Sub-processor the same obligations, in functional terms, as those imposed on BlueSnap under this DPA. If a Sub-processor fails to fulfill its data protection obligations under that agreement, BlueSnap will remain liable to you for the acts and omissions of its Sub-processor to the same extent BlueSnap would be liable if performing the relevant services directly under this DPA.

7. **Liability**.

Nothing in the Agreement shall relieve BlueSnap or Merchant of their respective individual responsibilities and liabilities under Privacy Law. BlueSnap's liability under or in connection with this DPA, including under the SCCs, is subject to the exclusions and limitations on liability contained in the Agreement. In no event does BlueSnap limit or exclude its liability towards data subjects or competent data protection authorities in respect of this DPA or SCCs.

8. **Cross-Border Transfers of Merchant Personal Data and Customer Data .**

8.1 Merchant acknowledges that BlueSnap may transfer or onward transfer Merchant Personal Data and Customer Personal Data to a country not recognised under European Privacy Laws as having an adequate level of protection pursuant to Standard Contractual Clauses or using another means recognised by European Privacy Laws.

8.2 Subject to clause 8.3, BlueSnap and the Merchant agree with each other to be bound by, observe, comply with and perform the Standard Contractual Clauses (as though the Merchant is the data exporter and BlueSnap is the data importer) in respect of Merchant Restricted Transfers as if the Standard Contractual Clauses were set out in, and incorporated into, this DPA. For this purpose, and without limiting or affecting the foregoing:

(i) with respect to Merchant Restricted Transfers of Customer Personal Data and Merchant Personal Data which constitute, in accordance with clause 2 of this DPA, a transfer by the Merchant as controller to BlueSnap as controller, module one of the Standard Contractual Clauses apply;

(ii) with respect to Merchant Restricted Transfers of Customer Personal Data which constitute, in accordance with clause 2 of this DPA, a transfer by the Merchant as controller to BlueSnap as processor, module two of the Standard Contractual Clauses apply; and

(iii) the Merchant and BlueSnap are deemed to have signed Annex I of the Standard Contractual Clauses on the occurrence of a Merchant Restricted Transfer by the Merchant.

8.3 The Standard Contractual Clauses shall not apply as between Merchant and BlueSnap to the extent BlueSnap has adopted an alternative recognised compliance standard for the lawful transfer of European Personal Data outside the European Economic Area, EU and/or UK in accordance with applicable European Privacy Law, such as Binding Corporate Rules or a valid successor to the Privacy Shield framework.

8.4 BlueSnap and Merchant agree at the request of either of them to confirm that the Standard Contractual Clauses are binding upon it and/or to execute a copy of the Standard Contractual Clauses to confirm their binding nature.

8.5 If the Merchant and BlueSnap previously entered into:

(i) the European Commission standard contractual clauses adopted under Decision 2001/497/EC or Decision 2010/87/EU, the Merchant and BlueSnap agree that such standard contractual clauses are hereby terminated with respect to European Personal Data and that any European Personal Data previously transferred under such standard contractual clauses does not have to be returned or deleted due to their termination but instead shall be deemed to have been transferred prospectively under the Standard Contractual Clauses (but without limiting or affecting any accrued rights, obligations, liabilities or obligations that survive the termination); and

(ii) the EU SCCs in respect of Merchant Restricted Transfers made by the Merchant to BlueSnap in respect of European Personal Data, to the extent European Privacy Laws of the UK applied to the Merchant's processing when making that transfer ("**UK Personal Data**"), the Merchant and BlueSnap agree that such EU SCCs are hereby terminated with respect only to UK Personal Data and that any UK Personal Data previously transferred under such EU SCCs does not have to be returned or deleted due to their termination in such respect but instead shall be deemed to have been transferred under the UK SCCs (but without limiting or affecting any accrued rights, obligations, liabilities or obligations that survive the termination in such respect).

8.6 BlueSnap Inc. continues to comply with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred to the United States pursuant to Privacy Shield. BlueSnap Inc. has certified that it adheres to the Privacy Shield Principles with respect to such data but does not rely on Privacy Shield as a method of transferring personal data to third countries under European Data Protection Laws. BlueSnap, upon request by Merchant and at its expense, will, taking into account the nature of the processing, assist Merchant, in Merchant's capacity as controller, in responding to individuals exercising their rights under the Privacy Shield Principles.

9. **Jurisdiction and Law**. The parties to this DPA submit to the choice of jurisdiction and choice of law stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity. This does not limit or affect the governing law or jurisdiction of the Standard Contractual Clauses.

10. **Variations**. BlueSnap may propose variations to this DPA which it reasonably considers to be necessary to address the requirements of any relevant Privacy Law including new laws, rules and regulations that may be promulgated in the future.

11. **Severance**. Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

12. **Equivalent Provisions**. References in this DPA to a provision of the GDPR includes, to the extent the processing of European Personal Data is subject to European Privacy Laws other than the GDPR, the equivalent provision under that other applicable European Privacy Law.

Appendix 1

SECTION A:

A. List of Parties

Data exporter: Merchant.

Activities relevant to processing: Operating as a merchant.

Role: controller

Data importer: BlueSnap. BlueSnap's name, address and contact details are as set out in the Agreement.

Activities relevant to processing: Provision of the services under the Agreement.

- With respect to module 1 (where applicable in accordance with clause 8.2(i) of the DPA), this includes underwriting and due diligence reviews of merchants in accordance with payment/financial industry standard legal requirements, and securing financial records of transactions and the other activities described in clause 2 of the DPA for which BlueSnap is a controller.

- With respect to module 2 (where applicable in accordance with clause 8.2(ii)of the DPA), this includes the processing of online payment transactions in order to provide safe secure payment services to merchants, market place vendors and their customers and the other activities described in clause 2 of the DPA for which BlueSnap is a processor.

Role:

- controller (where module 1 applies in accordance with clause 8.2(i) of the DPA)

- processor (where module 2 applies in accordance with clause 8.2(ii) of the DPA)

B. Description of Transfer

Categories of Data Subject:

- With respect to module 1 (where applicable in accordance with clause 8.2(i) of the DPA): Customers of Merchant and personnel of Merchant.

- With respect to module 2 (where applicable in accordance with clause 8.2(ii) of the DPA): Customers of Merchant.

Categories / Type of Personal Data:
With respect to module 1 (where applicable in accordance with clause 8.2(i) of the DPA):

- Other data: ID documents, passport data, financial records, security certificates, professional qualifications, bank/credit/personal references, background and credit checks, required to conduct merchant due diligence.

With respect to module 2 (where applicable in accordance with clause 8.2(ii)of the DPA):

- Contact details (name, address, e-mail address, phone and fax contact details and associated local time zone information), and other data points required by payment card networks to fulfil a transaction;

- IT systems information (user ID and password, computer name, domain name, IP address, location, and software usage pattern tracking information i.e. cookies); and

- Where applicable financial, payment data such as card numbers

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose

limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).
With respect to module 1 (where applicable in accordance with clause 8.2(i) of the DPA):

- Due diligence checks are periodic. Transaction fraud checks generally take place each time there is a transaction.

With respect to module 2 (where applicable in accordance with clause 8.2(ii) of the DPA):

- Payment transactions are continuing.

Nature of the Processing
With respect to module 1 (where applicable in accordance with clause 8.2(i)of the DPA):

- The personal data will be subject to storage, audit and review by payment processors, acquirers, Card Associations and regulatory authorities and any other activities described in clause 2 of the DPA for which BlueSnap is a controller. Transaction fraud checks are undertaken for all card transactions.

With respect to module 2 (where applicable in accordance with clause 8.2(ii) of the DPA):

- The personal data transferred will be subject to the processing operations in order for the BlueSnap to provide the services requested by the Merchant and any other activities described in clause 2 of the DPA for which BlueSnap is a processor. This includes payment processing.

Purpose(s) of the data transfer and further processing:
With respect to module 1 (where applicable in accordance with clause 8.2(i) of the DPA):

- The purpose of the data transfer and further processing is so that BlueSnap can conduct transaction records, fraud and money laundering prevention services and other activities described in clause 2.1 of the DPA for which BlueSnap is a controller.

With respect to module 2 (where applicable in accordance with clause 8.2(ii) of the DPA):

- The purpose of the data transfer and further processing is so that BlueSnap can as requested by the Merchant from time to time, perform payment transaction fulfilment and other activities described in clause 2.1 of the DPA for which BlueSnap is a processor.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
With respect to module 1 and 2 (where applicable in accordance with clauses 8.2(i) and 8.2(ii) respectively of the DPA):

- The maximum data retention periods are determined by the DPA, as updated from time to time, and applicable data retention policies of BlueSnap and law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing.
With respect to module 2 (where applicable in accordance with clause 8.2(ii) of the DPA):

- **Subject matter of Processing:** See purpose and nature above.

- **Nature of Processing:** See nature above.

- **Duration of Processing:**
The processing of the personal data shall take place as long as the Agreement remains in force. BlueSnap will retain the personal data as per the data retention period(s) described above, under the heading "The

period for which the personal data will be retained or, if that is not possible, the criteria used to determine that period".

Persons or Parties Exposed to Merchant Personal Data:

Merchant's and BlueSnap's personnel, employees, contractors

C. Competent Supervisory Authority

Identify the competent supervisory authority/ies in accordance with Clause 13:
With respect to module 1 and 2 (where applicable in accordance with clauses 8.2(i) and 8.2(ii) respectively of the DPA):

- See the definition of the applicable Standard Contractual Clauses in the DPA.

SECTION B:

Technical and organizational security measures including technical and organisational measures to ensure the security of the data

Description of the technical and organisational measures implemented by BlueSnap (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

With respect to module 1 and 2 (where applicable in accordance with clauses 8.2(i) and 8.2(ii) respectively of the DPA):

BlueSnap maintains an information security program focused on the security and integrity of personal data. BlueSnap's information security program includes administrative, technical and operational controls appropriate for the size of its business, the types of information it processes and the relative level of risk such information poses.

1. Personnel Security.

(a) As part of the hiring process, all employees undergo criminal background (US) and reference checks, sign NDAs committing them to protecting confidential information (including Customer Personal Data), agree to reasonable use policies for personal data, and sign off on the BlueSnap Information Security Policy

(b) During employment, continued security awareness training and education are provided annually.

(c) Following any severing of the work relationship, the employee must surrender all assets and all access is revoked.

2. Physical Security and Hosting Environment

(a) All personal data is secured and access is limited to only the systems and employees that need access to facilitate providing services to the customer.

(b) The production servers are hosted at SSAE 16-audited facilities. Visual confirmation and strict sign-in procedures are executed by trained security personnel that have passed criminal background checks. Data center access is also restricted with key cards, photo ID verification and is staffed 24/7/365. The site is also monitored and recorded via color, high-resolution digital video cameras. Neither the lessor of the servers nor the facility managers have login access to the servers.

(c) All BlueSnap offices including the corporate headquarters in Waltham are protected by badge access and staffed by security personnel 24/7.

3. Application Security and Access Control

(a) System Administration: All access is authenticated via userID/password, sensitive systems/services are also protected with an additional 2FA authentication. All access is logged and those logs are replicated and preserved.

(b) Personal data

i. Employees that need to access personal data to do their jobs may only do so under the following conditions:

1. There is no other way accomplish the task

2. Only the minimal amount of data required is accessed

3. Any captured information is destroyed once no longer needed

ii. Access is granted on a per-user basis, based on job role and requirements, and only to the appropriate level of personal data in accordance with least privilege. User authentication is controlled using multiple security factors including username, password, and 2 Factor authentication. Passwords are safeguarded and never stored in plain text, either at rest or in transit.

(c) Source code static scanning is performed on the application source code

(d) Web Application Firewall is deployed in Production to defend against application attacks

4. Information Security / Incident Management

(a) For Production systems, the operating system is Linux with all ports but 443 are closed to the internet at large. Critical patches are automatically applied while high and medium severity patches are applied monthly and quarterly.

(b) Vulnerability digests are monitored daily for new issues in any software BlueSnap relies on.

(c) Surfaces are minimized by locking down all ports accessible outside of the private network.

(d) In the event of an incident, there is an on-call engineer at all times. The process for triage, escalation, and communication are clear and documented internally.

(e) BlueSnap maintains security incident management policies and procedures.

(f) In addition, periodic penetration tests are performed against the Production and Corporate environment to minimize the risk of exposure. Internal security reviews are conducted for all new features. A particular emphasis is placed on the OWASP Top 10.

5. Data Protection and Encryption

(a) Https is required for all access to production services and applications that have access to Customer Personal Data

(b) All PII and Card data in Production is encrypted at rest

(c) Hard drives are encrypted on all endpoints

6. Corporate Infrastructure Security

(a) Anti-Virus/Anti-Malware: All workstations are equipped with centrally-managed anti-malware and anti-virus software

(b) DDOS mitigation is setup “always-on” for our services in Production

(c) Next Generation Security agent is deployed on every desktop/laptop

(d) Anti-phishing and anti-malware email filter is applied and all emails are filter

(e) Data Leak Protection software is applied on every desktop

(f) Wireless Networks: Wi-Fi networks is completely segregated from the corporate network.

(g) Automatic Updates: All Windows workstations are configured using Active Directory based Group Policies to automatically download and install security and related updates released by Microsoft.

(h) User Account Password Complexity: Passwords used for common login services such as Active Directory and Google Apps for Work are required to meet complexity requirements, where available, required to be changed on a regular basis.

(i) An Intrusion Prevention System is deployed in production and corporate networks

(j) Host Intrusion Detection Software is deployed on every production server to alert on system file changes

(k) Data Leak protection is deployed in email and SharePoint sites

(l) 2 Factor Authentication is deployed to protect every sensitive server/IT asset

(m) The Production network is segmented into VLANs for further isolation and protection of data and servers

(n) A Security information and event management system (SIEM) is deployed to monitor and manage security events across the organization

(o) BlueSnap is level 1 PCI compliant which requires the following:

i. Annual Report on Compliance (“ROC”) by Qualified Security Assessor (“QSA”)

ii. Annual onsite audit and assessment by the QSA

iii. Quarterly network scan by an Approved Scan Vendor (“ASV”)

iv. Proper encryption of card data at rest and in transmission

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

With respect to module 2 (where applicable in accordance with clause 8.2(ii) of the DPA):

- The scope and the extent of the assistance to be provided by BlueSnap in accordance with Clause 10(b) shall be such as is necessary to enable BlueSnap to comply with its obligations of assistance with respect to data subjects rights owed to Merchant under the DPA.

Appendix 2

Swiss Addendum to the EU Commission Standard Contractual Clauses

Interpretation of this Addendum

1. In this Appendix, terms used in the DPA have the same meaning in this Addendum. In addition, the following terms have the following meanings:

This Addendum	This Appendix
Swiss Data Protection Laws	All European Privacy Laws in Switzerland, including the FADP.
FADP	The Federal Act on Data Protection of 19 June 1992 (SR 235.1; FADP) and the revised version of the Federal Act of Data Protection of 25 September 2020, scheduled to come into force on 1 January 2023 (the "Revised FADP"), including any further revisions or updates from time to time.

2. This Addendum shall be read and interpreted in the light of the provisions of Swiss Data Protection Laws.

3. This Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in Swiss Data Protection Laws.

Hierarchy

4. In the event of a conflict or inconsistency between this Addendum and the provisions of the EU SCCs or other related agreements between the parties, the provisions which provide the most protection to data subjects shall prevail.

Incorporation of the Clauses

5. This Addendum amends the EU SCCs which are deemed to be amended to the extent necessary so they operate:

   a. for transfers made by the Merchant to BlueSnap, to the extent that Swiss Data Protection Laws apply to the Merchant's processing when making that transfer; and

   b. to provide appropriate safeguards for the transfers in accordance with Article 6 of the FADP (or Article 16 of the Revised FADP).

6. The amendments required by paragraph 6 above comprise:

   a. references to the "EU SCCs" means the EU SCCs as amended by this Addendum;

   b. references to "Regulation (EU) 2016/679" or "that Regulation" are replaced by "Swiss Data Protection Laws" and references to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of Swiss Data Protection Laws.

   c. references to Regulation (EU) 2018/1725 are removed;

   d. references to the "Union", "EU" and "EU Member State" shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland)

   e. Clause 13(a) and Part C of Annex II are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner;

   f. references to 'personal data' extends to data of legal entities until the entry into force of the Revised FADP.