SPADE'

DATA PROCESSING AGREEMENT

This Data Processing Agreement (this "**DPA**") forms an integral part of the Master Services and API License Agreement ("**Agreement**") between Spade and Client. Capitalized terms used but not defined in this DPA will have the meanings set forth in the Agreement. In the event of any conflict among the terms set forth in this DPA or the Agreement, the terms of this DPA shall prevail to the extent of such conflict.

1. DATA PROCESSING, SUBJECT MATTER, AND ROLES

1.1. Data Processing. In the course of providing the Services to Client pursuant to the Agreement, Spade may Process Client Data that constitutes "personal data", "personal information", "personally identifiable information", or an analogous term under any applicable law ("**Personal Data**"). The Parties agree to comply with this DPA and all privacy and data protection laws applicable to the Processing of Personal Data under the Agreement, including, as applicable, those of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom, and the United States ("**Data Protection Laws**").

1.2. Subject Matter. The subject matter, nature, and purpose of the Processing of Personal Data, the types of Personal Data, and the categories of "**Data Subjects**" (as such term is defined under applicable Data Protection Laws) are set out in **Schedule I**, which is an integral part of this DPA.

1.3. Roles. Client is a "**Controller**" or "**Business**" (as such terms are defined under applicable Data Protection Law) and appoints Spade as a "**Processor**" or "**Service Provider**" (as such terms are defined under applicable Data Protection Law) on behalf of Client. Client is responsible for compliance with the requirements of Data Protection Law applicable to Controllers and Businesses.

2. PROCESSING INSTRUCTIONS.

Spade shall Process Personal Data on behalf of and only in accordance with Client's documented instructions for the following purposes: (a) Processing in accordance with this DPA, the Agreement, or the Order Form; (b) Processing initiated by Client in its use of the Services; and (c) Processing to comply with other reasonable documented instructions provided by Client (e.g., via email) where such instructions are consistent with the terms of this DPA or the Agreement.

3. PERSONNEL.

Spade will ensure that all personnel authorized to Process Personal Data are subject to an obligation of confidentiality.

4. CCPA LIMITATIONS ON PROCESSING.

Except as permitted by applicable Data Protection Law, the Agreement, the Order Form, or this DPA, Spade will not (a) retain, use, or disclose Personal Data for any purpose other than for the specific purposes of performing the Services or in accordance with Client's documented instructions (including as set forth in the Agreement), (b) retain, use, or disclose Personal Data outside of the direct business relationship between the Parties, (c) combine Personal Data with "**Personal Information**" (as such term is defined under the CCPA) obtained from, or on behalf of, sources other than Client, or (d) "**Sell**" or "**Share**" (as such terms are defined under the CCPA) Personal Data.

5. SECURITY AND SECURITY INCIDENT.

5.1. **Security**. Spade will implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risks presented by the Processing of Personal Data and the Services ("**Security Measures**"), including the measures set forth in Schedule I. The Security Measures are subject to technical progress and development, and Spade may update the Security Measures, provided that any updates shall not materially diminish the overall security of Personal Data or the Services.

5.2. **Security Incident**. Spade will notify Client without undue delay and within twenty-four (24) hours of becoming aware of any actual or reasonably suspected unauthorized access to, or other Processing of, Personal Data in its possession or control ("**Security Incident**"). If Spade's notification of a Security Incident is delayed, it will be accompanied by reasons for the delay.

6. **SUBPROCESSING**.

6.1. **Subprocessors**. Client hereby authorizes Spade to engage any Processor that processes Personal Data on behalf of Spade ("**Subprocessor**"). A list of Spade's current Subprocessors is available at the Spade Trust Center.

6.2. **Subprocessor Agreements**. Spade has entered into a written agreement with each Subprocessors containing, in substance, data protection obligations no less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Subprocessors.

6.3. **Subprocessor Changes**. Spade will notify Client prior to any intended change to Subprocessors. Client may object to Spade's use of a new Subprocessor within thirty (30) days of receipt of Spade's notice of the intended change of Subprocessor based on reasonable grounds that the appointment of such Subprocessor will result in a material violation of Data Protection Law by providing written notice to Spade detailing the grounds of such objection. Spade will use reasonable efforts to make available to Client a change in the Services or recommend a commercially reasonable change to Client's configuration or use of the Services to avoid the Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening Client. If Spade is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Client may terminate the relevant parts of the Services which cannot be provided by Spade without the use of the objected-to new Subprocessor by providing written notice to Spade and Spade will refund Client any prepaid fees covering the remainder of the Term following the effective date of termination with respect to such terminated Services.

7. **ASSISTANCE**.

7.1. **DSR**. Client is responsible for responding to and complying with data subject requests ("**DSRs**"). The Services include controls that Client may use to assist it to respond to DSRs. If Client is unable to respond to DSRs using such controls, Spade will, taking into account the nature of the Processing and the information available to Spade, provide commercially reasonable assistance to Client designed to satisfy Client's obligations to comply with Data Subject and "**Consumer**" (as such term is defined under applicable Data Protection Laws) requests. To the extent legally permitted, Client shall be responsible for any costs and expenses arising from Spade's provision of such assistance.

7.2. **Other Assistance**. Spade will, taking into account the nature of the Processing and the information available to Spade, provide commercially reasonable assistance to Client designed to satisfy Client's obligations under Data Protection Law, including in connection with implementing appropriate technical and organizational measures, reply to inquiries, complaints, investigations, and inquiries, conduct data protection impact assessments, conduct data protection assessments, and conduct prior consultations with regulators. To the extent legally permitted, Client shall be responsible for any costs and expenses arising from Spade's provision of such assistance.

8. AUDIT.

Upon Client's written request, Spade will provide Client access to reasonably requested documentation designed to demonstrate Spade's compliance with its obligations under this DPA in the form of the relevant audit report or certifications listed in the Security Addendum ("**Audit Report**"). If the Audit Report reveals any breach of this DPA or violation of Data Protection Law by Spade, Client may request and conduct, at Client's sole expense, a reasonable audit of Spade's applicable controls and compliance with this DPA (an "**Audit**"), provided (a) such Audit is conducted by Client or a third-party auditor designated by Client and reasonably acceptable to Spade that has executed an appropriate confidentiality agreement with Spade, (b) such Audit is conducted during reasonable times and of reasonable scope and duration in accordance with mutually agreed upon terms between Client and Spade, (c) a similar Audit has not already been conducted less than twelve (12) months prior, unless it is required by a "**Supervisory Authority**" (as such term is defined under applicable Data Protection Laws) or other regulatory authority responsible for the enforcement of Data Protection Law, and (d) such Audit does not involve any Spade's production systems or environments. Client may use the results of an Audit only for the purposes of meeting Client's regulatory audit requirements or confirming compliance with the requirements of the DPA.

9. INTERNATIONAL DATA TRANSFERS

9.1. European Data Transfers. Spade will obtain Client's specific prior written authorization for any transfer of Personal Data subject to European Data Protection Law that is not subject to an adequacy decision by the European Commission ("**International Data Transfer**"). Client hereby authorizes Spade to conduct International Data Transfers outside the European Economic Area ("**EEA**") or Switzerland:

- to any country subject to a valid adequacy decision of the European Commission;
- on the basis of an organization's binding corporate rules approved by EEA Supervisory Authorities; and
- to any data importer with whom Spade has entered into the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council as amended or replaced from time to time ("**SCCs**").

9.2. European Transfer Mechanisms. Client and Spade conclude Module 2 (Controller-to-Processor) of the SCCs and, to the extent Client is a Processor on behalf of a Third-Party Controller, Module 3 (Processor-to-Subprocessor) of the SCCs, which are hereby incorporated and completed as follows: the "data exporter" is Client; the "data importer" is Spade; the optional docking clause in Clause 7 is implemented; Option 1 of Clause 9(a) is implemented and the time period therein is specified in Section 6.3 above; the optional redress clause in Clause 11(a) is struck; Option 1 in Clause 17 is implemented and the governing law is the law of Ireland; the courts in Clause 18(b) are the Courts of Ireland; Annexes I and II to the SCCs are Schedule I to this DPA. For International Data Transfers from Switzerland, Data Subjects who have their habitual residence in Switzerland may bring claims under the SCCs before the courts of Switzerland.

9.3. UK Data Transfers. Client hereby authorizes Spade to perform International Data Transfers outside the UK subject to the requirements:

- to any country subject to a valid adequacy decision issued by the UK Government;
- on the basis of an organization's binding corporate rules approved by the UK Information Commissioner; and
- to any data importer with whom Spade has entered into the addendum to the SCCs issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022) ("**UK Addendum**") or other standard contractual clauses issued by the UK Information Commissioner, as appropriate.

9.4. UK Transfer Mechanism. Client and Spade conclude the UK Addendum which is hereby incorporated and applies to International Data Transfers outside the UK. Part 1 of the UK Addendum is completed as follows: (a) in Table 1, the "Exporter" is Client and the "Importer" is Spade, their details are set forth in this DPA and the Agreement; (b) in Table 2, the first option is selected and the "Approved EU SCCs" are the SCCs referred to in Section 9.2 of this DPA; (c) in Table 3, Annexes 1 (A and B), II, and III to the "Approved EU SCCs" are Schedule I to this DPA; and (d) in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

9.5. Other Transfer Mechanisms. If Spade's compliance with Data Protection Law applicable to International Data Transfers is affected by circumstances outside of Spade's control, including if a legal instrument for International Data Transfers is invalidated, amended, or replaced, then Client and Spade will work together in good faith to reasonably resolve such non-compliance. In the event that additional, replacement or alternative standard contractual clauses or UK standard contractual clauses are approved by Supervisory Authorities, Spade reserves the right to amend the Agreement and this DPA by adding to or replacing, the standard contractual clauses or UK standard contractual clauses that form part of it at the date of signature in order to ensure continued compliance with Data Protection Law.

10. RETURN AND DELETION.

Upon Client's written request, Spade will delete or return Personal Data within thirty (30) days, provided that Spade may retain Personal Data if required by law or in standard backups that remain subject to this DPA's protections.

CLIENT	**SPADE DATA, INC.**
By:	By:
Name:	Name: _____
Title:	Title: _____

Schedule I

DESCRIPTION OF THE TRANSFER

A. LIST OF PARTIES

Data exporter:

- **Name:** Client
- **Activities relevant to the data transferred under these Clauses:** Client receives Spade's Services as described in the Agreement and Client provides Personal Data to Spade in that context.
- **Role (controller/processor):** Controller

Data importer:

- **Name:** Spade Data, Inc.
- **Activities relevant to the data transferred under these Clauses:** Spade provides its Services to Client as described in the Agreement and Processes Personal Data on behalf of Client in that context.
- **Role (controller/processor):** Processor on behalf of Client

B. CATEGORIES OF DATA SUBJECTS WHOSE PERSONAL DATA IS TRANSFERRED

Data subjects include individuals about whom Personal Data is provided to Spade via transaction data (by or at the direction of Client), which shall include: consumers, customers, cardholders, account holders, and other individuals whose personal data is included in transaction records and Client Data.

C. CATEGORIES OF PERSONAL DATA TRANSFERRED

The types of Personal Data are determined and controlled by Client in its sole discretion, and may include transaction data elements such as: transaction descriptors and amounts, truncated payment card identifiers, merchant information, timestamps, location data, and pseudonymous user and account identifiers processed in the course of the Services.

D. SENSITIVE DATA TRANSFERRED (IF APPLICABLE)

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 specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: N/A.

E. FREQUENCY OF THE TRANSFER

The frequency of the International Data Transfer (e.g. whether the Personal Data is transferred on a one-off or continuous basis): On a continuous basis.

F. NATURE OF THE PROCESSING

The Personal Data will be processed and transferred as described in the Agreement.

G. PURPOSE(S) OF THE INTERNATIONAL DATA TRANSFER AND FURTHER PROCESSING

The Personal Data will be transferred and further processed for the provision of the Services as described in the Agreement.

H. DURATION OF PROCESSING

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: Personal Data will be retained for as long as necessary taking into account the purpose of the Processing, and in compliance with applicable laws, including laws on the statute of limitations and Data Protection Law.

I. SUB-PROCESSOR TRANSFERS

For International Data Transfer to (Sub)Processors, also specify subject matter, nature and duration of the Processing: For the subject matter and nature of the Processing, reference is made to the Agreement, the Agreement, and this DPA. The Processing will take place for the duration of the Agreement.

J. COMPETENT SUPERVISORY AUTHORITY

The competent authority for the Processing of Personal Data relating to Data Subjects located in the EEA is the Supervisory Authority of Ireland.

The competent authority for the Processing of Personal Data relating to Data Subjects located in the UK is the UK Information Commissioner.

The competent authority for the Processing of Personal Data relating to Data Subjects located in Switzerland is the Swiss Federal Data Protection and Information Commissioner.

K. TECHNICAL AND ORGANIZATIONAL MEASURES

Spade will implement security safeguards designed to protect the security, confidentiality and integrity of Personal Data in accordance with SOC 2 Type II, ISO 27001, or a substantially similar standard, and as described at https://spade.com/security.