SCHEDULE A

SUPPLIER PERSONAL DATA PROCESSING ADDENDUM

This PERSONAL DATA PROCESSING ADDENDUM ("**Addendum**") constitute an agreement between MoneyGram Payment Systems, Inc. ("**Customer**" or "**MoneyGram**") and you ("**you"** or "**Supplier**") related to your provision of Goods and/or Services to Customer.

WHEREAS, under the terms of the Agreement, Supplier may provide Services to Customer which require Supplier to process Customer Personal Data on Supplier's behalf; and,

WHEREAS, the Parties desire to amend and supplement the Agreement with the terms of this Addendum to comply with the CCPA, including, but not limited to, new privacy laws that are enacted from time to time.

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Definition

1.1 "**Controller**" means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

1.2 "**Data Protection Laws**" means personal data protection or privacy laws of any applicable locality, state, territory or country, including but not limited to the California Consumer Privacy Act of 2018 (the "**CCPA**").

1.3 "**Data Subject**" means any natural person, including, but not limited to a consumer, who is the subject of Personal Data, and as applicable, resident of a locality, state, territory or jurisdiction that is covered by an applicable Data Protection Law.

1.4 "**Personal Data**" means any data that identifies, relates to, is capable of being associated with, or could reasonably be linked to an identified or identifiable natural person or household. An identifiable natural person or household is one that can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person or household.

1.5 "**Processing, Processes, Processed or Process**" means any operation or set of operations which are performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as, collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available, restricting, erasing, destroying Personal Data.

1.6 **"Processor**" means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of the Controller.

1.7 **"Security Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored

or otherwise processed.

1.8 **"Subprocessor**" means any third party, including, but not limited to, subcontractor, service provider, or contractor, appointed by or on behalf of Supplier to Process Customer Personal Data, that does not collect Personal Data from the Data Subject or act as a contracted Processor on behalf of the Customer.

2. Personal Data Processing

2.1 As between Customer and Supplier, Customer is the Controller of all Personal Data Processed under the Agreement on behalf of Customer, while Supplier is the Processor of all Personal Data Processed under the Agreement on behalf of Customer.

2.2 Each of the Parties will comply with the applicable Data Protection Laws, including, but not limited to, the CCPA in Processing of Personal Data under the Agreement.

2.2 Each of the Parties will, upon the request of the other Party, comply with the other Party's request to enter into any further amendments to the Agreement to the extent reasonably necessary to comply with the applicable Data Protection Laws.

3. Supplier Obligations

3.1 To the extent that Supplier receives Personal Data for Processing on behalf of Customer pursuant to the Agreement, Supplier shall:

3.1.1 be a "service provider" to Customer as defined under the CCPA, or any other applicable Data Protection Law even if different designation is given; and shall not retain, use, share, transfer, give access to or disclose Customer Personal Data without the Customer's written consent, for any purpose other than for the specific purpose of performing the Services as provided under the Agreement or as otherwise permitted by the CCPA, or Applicable Data Protection Laws;

3.1.2 not retain, use, share, transfer, give access to or disclose Personal Data for any "commercial purpose" as defined in the CCPA or under any other applicable Data Protection Laws, other than providing the Services under the Agreement;

3.1.3 not "sell," as defined in CCPA, or any other applicable Data Protection Laws, Personal Data;

3.1.4 in the case of receiving any complaint, notice, or communication from a Data Subject or any other entity, relating directly or indirectly Supplier's processing of Personal Data or potential failure to comply with any applicable Data Protection Laws, to the extent permitted by law, promptly forward the complaint, notice, or communication to privacyprogramoffice@moneygram.com and provide reasonable cooperation and assistance in relation to the same;

3.1.5 promptly, but in no event more than seven (7) days of receipt, comply with Customer's written instructions associated with responding to a Data Subject's request to exercise his or her privacy rights with respect to his or her Personal Data pursuant to applicable Data Protection Laws;

3.1.6 in case Supplier is required to disclose Personal Data by court order, subpoena, or other governmental requirement or authority, or by law or regulation, provided that such disclosure is permitted by applicable Data Protection Laws (a "**Compulsory Request**"), Supplier shall promptly inform the Customer of such requirement to disclose Personal Data before processing the Compulsory Request, unless applicable law prohibits such disclosure;

3.1.7 if Supplier authorizes any Subprocessor to process Customer Personal Data, Supplier shall enter into contractual provisions obligating such Subprocessor, to the same obligations that Supplier has under this Addendum, the Agreement and applicable Data Protection Laws; and

3.1.8 Supplier hereby certifies that it understands and is willing to abide by the restrictions set forth in the Agreement, this Addendum and applicable Data Protection Laws with respect to the Processing of Personal Data under the Agreement.

4. Data Security

4.1 Supplier shall implement appropriate technical and organizational measures to protect Customer Personal Data from unauthorized access, disclosure, destruction, alteration, accidental loss, misuse, or damage and shall ensure that all such safeguards comply with applicable Data Protection Laws, as well as the terms and conditions of this Addendum and the Agreement.

4.2 Supplier shall notify Customer of a Security Breach without undue delay, but no later than seventy-two (**72**) business hours after Supplier becomes aware of a Security Breach. Immediately following Supplier notification to Customer of a Security Breach, the Parties shall in good faith coordinate with each other to investigate the Security Breach.

5. Customer Audits. Supplier will make available to Customer all information necessary to demonstrate compliance with the obligations in this Addendum and the applicable Data Protection Laws. If applicable, Supplier will permit Customer and its third-party representatives (subject to applicable confidentiality obligations) to audit Supplier's compliance with its obligations under this Addendum and will give Customer and its third-party representatives all necessary assistance to conduct such audits.

6. Indemnification. Supplier will indemnify and hold harmless Customer for all claims and proceedings and all liability, loss, costs, fine and expenses (including reasonable legal fees) incurred by Customer arising from or in connection with (i) unauthorized Processing of Customer Personal Data by the Supplier or its Subprocessors; (ii) Supplier's failure to comply with its obligations under this Addendum, or (iii) a Security Breach.

7. Return or Destruction of Personal Data. Unless otherwise agreed to the contrary, Supplier will, at the request of Customer or within sixty (**60**) days of the expiration or termination of the Agreement, destroy or deliver to Customer (and shall cause its Subprocessors to destroy or deliver) all materials containing Customer Personal Data, together with any and all copies thereof (excluding archived or other copies that are not readily retrievable and are scheduled for deletion pursuant to an established Supplier retention schedule, which shall be provided to Customer and provided such scheduled deletion subsequently takes place). Notwithstanding the forgoing, subject to the obligations herein, Supplier may retain one archived copy of any information that it is required by law to retain, but only for the period necessary to comply with such requirement.

8. **Conflict of Language**. In the event that language in the Agreement conflicts or is deemed to conflict with the language in this Addendum, the Parties agree that the language in this Addendum shall supersede and control as to the subject matter hereof unless there are sector-specific privacy laws that apply to the Agreement or Supplier, in which case, such privacy laws shall prevail.

9. **Survival.** This Addendum shall survive the termination of the Agreement.

IN WITNESS WHEREOF, the Parties, through their authorized representatives, have executed this Addendum as of the date written below.

MONEYGRAM PAYMENT SYSTEMS, INC.	**[SUPPLIER]**
_____	_____
Signature	Signature
_____	_____
By: Name	By: Name
_____	_____
Its: Title	Its: Title
_____	_____
Date:	Date: