WALMART INFORMATION SECURITY ADDENDUM

Walmart Inc. ("Walmart") and You ("Seller") (each a "Party" and collectively the "Parties") have entered into the Comprehensive Walmart Marketplace Program Retailer Agreement ("Agreement"). This Information Security Addendum ("Addendum") sets forth the Parties' mutual understanding relating to the privacy and security of Walmart Confidential Information and Walmart Systems. Exhibit A sets out in more detail: (i) instructions pertaining to Seller's Processing; (ii) the duration of the Processing; (iii) the nature and purpose of the Processing; and (iv) the types of Personal Information Processed and categories of data subjects involved.

1. Definitions. All terms used in this Addendum shall have the meaning specified in the Agreement, unless otherwise defined herein. For the purposes of this Addendum, the terms are defined as follows:

    a. "Walmart Confidential Information": (i) all information received by Seller from Walmart or a Walmart Affiliate, or collected or generated directly by Seller on Walmart's behalf in connection with the Services, that should reasonably be considered confidential under the circumstances, notwithstanding whether it was identified as such at the time of disclosure; (ii) all information identified as confidential to which Seller has access in connection with the subject matter of the Agreement, whether before or after the Effective Date of the Agreement; and (iii) the Agreement. Walmart Confidential Information shall include, without limitation: (A) all trade secrets; (B) existing or contemplated products, services, designs, technology, processes, technical data, engineering, techniques, methodologies, and concepts and any information related thereto; and (C) information relating to business plans, sales, or marketing methods and customer lists or requirements. Walmart Confidential Information includes Personal Information.

    b. "Personal Information": information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with particular persons or households, including but not limited to information derived from such information that is used to create inferences or profiles of such persons or households. Personal Information includes "sensitive personal information," "sensitive personal data," and similar terms as defined by Laws (as defined below).

    c. "Walmart System": any physical or technical system owned, leased, licensed, or operated by Walmart or its Affiliates, whether on premises or hosted by a third party, which Processes Walmart Confidential Information and is accessed by Seller in the course of performing the Services.

    d. "Services": services provided by Seller to Walmart in accordance with the Agreement.

    e. "Data Incident": any actual or suspected unauthorized or accidental access to or loss, use, disclosure, modification, destruction, acquisition, or Processing of any Walmart Confidential Information.

    f. "Process" and "Processing": any operation or set of operations which is performed on Walmart Confidential Information, whether by manual or automated means, such as collecting, recording, using, storing, retaining, altering, modifying, analyzing, retrieving, disclosing, disseminating, renting, selling, sharing, combining, reconfiguring, restricting, de-identifying, aggregating, deleting, disposing of, or destroying Walmart Confidential Information, and similar terms as defined by Laws.

    g. "Business Purpose," "Sell," and "Share" have the meanings ascribed to them in the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020), Cal. Civ. Code § 1798.100

et seq., and its implementing regulations, including any amendments thereto (collectively, the "CCPA/CPRA").

2. Compliance with Laws. During the term of the Agreement, Seller will: (i) comply, at its own cost and expense, with current and new laws, regulations, governmental requirements, and industry standards applicable to Seller's Processing of Walmart Confidential Information (collectively, "Laws"); and (ii) provide at least the same level of privacy protection as required by Laws. Should a disagreement arise as to the interpretation of any requirement of the Laws, Walmart's interpretation shall govern. If Seller is unable to comply with any new Laws, Walmart may, in its sole discretion, terminate the Agreement upon notice to Seller.

3. Information Security Program. Seller agrees to establish and maintain, in writing, an information security and privacy program consistent with this Addendum and Laws ("Information Security Program"). The Information Security Program shall include appropriate physical, technical, and administrative safeguards, including any safeguards and controls agreed to by the Parties, in writing, sufficient to protect Walmart Systems and Walmart Confidential Information from unauthorized or unlawful destruction, loss, alteration, disclosure, or access.

   The Information Security Program shall follow the NIST Cybersecurity Framework (CSF), NIST SP:800-53, ISO 27001 (including 27002 controls), or substantially similar standards applicable to Seller's industry. Seller's program shall also follow the PCI-DSS (wherever Seller processes PCI data for Walmart).

4. Security Certification. Seller shall maintain a certification or third-party assessment of compliance with the security standards identified in Section 3 of this Addendum provided by a qualified, independent third-party. Such certifications shall be provided to Walmart upon request.

5. Workforce. Seller shall ensure that each person authorized to Process Walmart Confidential Information on Seller's behalf is subject to a duty of confidentiality with respect to such information.

6. Information Security Contact. Seller's primary information security contact is the Seller contact on file with Walmart. Seller agrees to promptly notify Walmart of any changes to this information.

7. Restriction of Use of Walmart Confidential Information. Seller acknowledges and agrees that Seller is authorized to Process Walmart Confidential Information only on behalf of, and in accordance with, the instructions of Walmart, and consistent with any data subject's exercise of rights as provided herein. Seller shall not: (i) Sell or Share Walmart Confidential Information; (ii) Process Walmart Confidential Information for any purpose other than for the limited Business Purpose of providing the Services specified in the Agreement and Exhibit A to the Addendum; (iii) retain, use, or disclose Walmart Confidential Information outside of the direct business relationship between Walmart and Seller; (iv) combine Walmart Confidential Information with Personal Information that Seller receives from, or on behalf of, another person or persons, or collects from its own interactions with an individual; or (v) use Walmart Confidential Information to create any derivative work or product for the benefit of Seller or any other party without Walmart's express, written authorization. Any unauthorized Processing of Walmart Confidential Information, or any Processing of Walmart Confidential Information in a manner not consistent with Walmart's obligations under Laws, shall constitute a material breach of the Agreement and, as a result, Walmart may, in its sole discretion, immediately suspend or terminate Seller's Processing of Walmart Confidential Information and access to Walmart Systems. Seller certifies that it understands the restrictions set forth in this section and will comply with them.

8. Audit. Seller shall monitor and, at regular intervals consistent with industry best practices, test and evaluate the effectiveness of its Information Security Program and Seller's compliance with the terms of the Addendum. Seller shall evaluate and promptly adjust its practices with regards to compliance with the Addendum, including its Information Security Program, in light of the results of the testing and monitoring, any material changes to its operations or business arrangements, or any other facts or circumstances that Seller knows or reasonably should know may have a material impact on the use or security of Walmart Confidential Information or Systems,

or Seller's compliance with the terms of the Addendum. Seller shall promptly provide Walmart with notice of any issues that are likely to adversely impact Walmart Confidential Information or Walmart Systems that are identified through any assessment or review of Seller's systems or Information Security Program performed by Seller or a third party (including those identified by Seller's clients). Notice of these issues may be provided in the form of a written summary. Seller shall keep Walmart timely informed of its remediation efforts to address these issues.

Walmart shall have the right to monitor Seller's compliance with the Agreement. Upon Walmart's request, Seller shall make available to Walmart information necessary to demonstrate compliance with the obligations set forth in this Addendum. Walmart may, in its discretion, periodically inspect and audit Seller's compliance with this Addendum, including Seller's Information Security Program and any facilities or systems used by Seller to provide the Services. Such inspections and audits may, at Walmart's option, be conducted on-site, or through surveys and interviews by Walmart personnel or Walmart's contracted third- party assessors who are required to agree to confidentiality terms. Onsite inspections and audits will be conducted during Seller's ordinary office hours upon reasonable prior written notice by Walmart and shall be subject to Seller's reasonable security restrictions (*e.g.*, sign-in requirements, badge requirements, escort requirements).

9. Breach Notification and Investigation. Seller shall notify Walmart's Emergency Operations Center: (i) by telephone at 479. 277.1001 within twenty-four (24) hours of any Data Incident; and (ii) in writing, within forty-eight (48) hours to its Chief Information Security Officer at WalmartInfoSec@walmart.com. The written notices described in (ii) shall summarize, in reasonable detail, the nature and scope of the Data Incident (including a description of all impacted Walmart Confidential Information and Walmart Systems to the extent known at that time) and the corrective action already taken or planned by Seller. The notice shall be timely supplemented to the level of detail reasonably requested by Walmart, inclusive of relevant investigative or forensic reports.

   Seller shall promptly, at its own cost and expense, take all reasonable and necessary actions to end the Data Incident, mitigate its impact, and prevent recurrence. Seller shall cooperate with Walmart in the investigation of the Data Incident and shall promptly respond to Walmart's reasonable inquiries about the Data Incident. In the event of a Data Incident, Walmart may, in its sole discretion, immediately suspend or terminate Seller's access to Walmart Confidential Information and Walmart Systems.

   Seller shall assist Walmart with determining whether to provide notice of the Data Incident to any person, governmental entity, the media, or other party, and preparing the content of any such notice. Walmart will make the final determination as to: (i) whether notice will be provided and to whom; (ii) the content of the notice; and (iii) which Party will be the signatory to the notice. Unless prohibited by Laws, Seller shall promptly notify Walmart of any investigations by a governmental, regulatory, or self-regulatory body into Seller's information use, privacy, or information security practices or a Data Incident, which reasonably may involve or relate to Walmart Confidential Information in Seller's possession, custody or control.

   Seller shall pay all expenses and costs (including but not limited to, assessments, fines, losses, penalties, settlements, costs of investigating and responding to any Data Incident, costs of notifying and providing affected individuals with at least one (1) year of credit monitoring and fraud prevention services, and attorneys' fees, including attorneys' fees incurred in enforcing this provision) arising out of or related to Seller's use of Walmart Confidential Information not in accordance with this Addendum, any Data Incident, or any breach by Seller of this Addendum.

10. Seller Assistance. Seller shall assist Walmart in complying with its obligations under Laws, including without limitation, Walmart's obligations to: (i) respond to data subjects' requests (as further detailed below); (2) implement appropriate data security measures (as further detailed in Section 3 of this Addendum); and (3) conduct and document data protection assessments, including providing information necessary to Walmart to conduct such assessments. To the extent that Laws require Walmart to comply with requests from individuals, including requests to access, delete, modify, or restrict the Processing of their Personal Information, Seller shall: (i) no more than thirty (30) days from Seller's receipt of Walmart's written instruction, provide any assistance

that Walmart reasonably deems necessary to fulfill such requests at Seller's own cost and expense; (ii) promptly notify Walmart of any such requests directed to Seller; and (iii) only Process Personal Information consistent with Walmart's direction regarding any data subject request, whether directed to Walmart or Seller. Such assistance shall be delivered through appropriate technical and organizational measures, taking into account the nature of the Processing. Seller shall certify, in writing, its compliance with such instructions. To the extent Seller directly interacts with Walmart customers, employees, contractors, service providers, or other individuals while acting on behalf of Walmart, Seller agrees to provide Walmart with any assistance Walmart reasonably deems necessary to fulfill applicable legal obligations to provide such individuals with notice of Processing activities.

11. Subcontractors. Seller shall notify Walmart and provide Walmart with an opportunity to object if Seller engages another party to assist in Processing Walmart Confidential Information. Seller shall contractually require all Sellers, contractors, or other agents of Seller engaged to perform the Services or to otherwise Process Walmart Confidential Information to do so under terms and conditions at least as protective of Walmart Confidential Information as this Addendum and in compliance with Laws. Seller shall make commercially reasonable efforts to monitor and enforce such contractual requirements, and shall be responsible to Walmart for all acts or omissions of its subcontractors and agents with respect to their access to and use of Walmart Confidential Information and Walmart Systems.

12. Cross-Border Transfers. Walmart Confidential Information may not be Processed outside the country in which Seller receives it without prior written approval from Walmart, inclusive of transfers to subcontractors or agents. Seller shall cooperate with Walmart in complying with all Laws regulating the cross-border transfer of information, and the Parties shall negotiate, in good faith, such additional agreements, terms, and conditions Seller may be required by such Laws to effectuate such transfers.

13. Deletion of Data. At Walmart's direction at any time, and in any event upon termination or expiration of this Agreement, Seller will, and will cause its Sellers, contractors, and other agents to, immediately cease use of the Walmart Confidential Information and return the same to Walmart and then destroy any and all residual copies of Walmart Confidential Information (in whole or part), whether in hard copy or electronic format. Seller will ensure that Walmart Confidential Information is destroyed securely and in accordance with Laws. As requested, Seller will certify its compliance with these procedures.

    Notwithstanding the foregoing, Seller will be permitted to retain: (i) Walmart Confidential Information for a longer period if such retention is strictly necessary to meet Seller's legal compliance obligations; and (ii) Walmart Confidential Information in backup media. Retention of Walmart Confidential Information pursuant to (i) and (ii) shall be pursuant to Seller's fully implemented and documented records management program, provided that such retention shall not be indefinite and shall not exceed industry standards. In addition, Walmart Confidential Information so retained shall not be used for any other purpose and such Walmart Confidential Information shall be otherwise maintained in accordance with this Addendum.

14. Indemnification. No limitation of liability provisions, if any, in the Agreement (or any other agreement between the parties) shall apply to any breach of this Addendum by Seller. Notwithstanding anything in the Agreement to the contrary, Seller shall indemnify, hold harmless, and defend Walmart (including its affiliates) from all suits, claims, demands, proceedings, and other actions brought by a third party arising out of or related to Seller's Processing of Walmart Confidential Information not in accordance with this Addendum, any Data Incident, or any breach by Seller of this Addendum.

15. Information Security-Related Termination Rights. In addition to any other termination rights under the Agreement, Walmart shall have the right to terminate the Agreement immediately if Seller materially breaches any provision of this Addendum.

16. Statement of Compliance. Seller shall provide Walmart with prompt written notice if at any time it determines it is not, or will not be, in full compliance with any requirements of this Addendum. Seller shall certify compliance with this Addendum from time-to-time or as may be reasonably requested by Walmart.

17. Survival; Severability. This Addendum shall survive termination of the Agreement. The invalidity or unenforceability of a portion of this Addendum shall not affect the validity or enforceability of the remainder hereof.

Exhibit A – Details of Processing

Walmart's instructions to Seller regarding the Processing of Personal Information are contained in the Agreement, this Addendum (including Exhibit A – Details of Processing), and any additional written agreement or documentation through which Walmart instructs Seller to perform specific Processing of Personal Information.

The details of the Processing of Personal Information carried out by Seller are as follows:

Nature, purpose and duration of Processing

Seller Processes Personal Information on behalf of Walmart for the following Business Purpose pursuant to the Agreement: performing services on behalf of Walmart, including fulfilling Walmart.com customer orders through the Walmart Marketplace Program.

The duration of the Processing is equal to the duration of the Agreement, or until otherwise instructed by Walmart.

Categories of data subjects to whom the Personal Information relates:

The Processing of Personal Information may concern the following categories of individuals: (check all that may apply):
[_] employees (associates)
[_] job applicants
[ ] contractors
[_] vendors
[x] consumers
[x] customers
[_] other (specify where possible):

Types of Personal Information to be Processed:

The Processing may concern the following types of Personal Information (check all that may apply):

[x] contact details (email, phone, address)
[_] device identifiers (IP address, MAC address, MAID, device ID)
[_] education and resume details
[_] training or performance-related data
[_] financial, economic, and insurance data
[_] billing and payment information
[_] digital, device, and social identifiers or digital profiles
[_] login credentials (username and password)
[_] any other categories of Personal Information (specify): [_____]

The Processing also may concern any other categories of Personal Information made available by Walmart, or otherwise obtained by Seller, in connection with the Agreement.

Seller also may also Process some of the following special categories of Personal Information (check all that may apply):

[x] none
[_] racial or ethnic origin
[_] political opinions
[_] religious or philosophical beliefs
[_] trade union membership

[_] genetic data
[_] biometric data
[_] data concerning health
[_] sex life or sexual orientation
[_] citizenship, citizenship status, or immigration status
[_] government-issued identifiers (e.g., SSNs, driver's license numbers, passport numbers, other national identification numbers)
[_] precise geolocation data
[_] personal information about a known child under the age of majority under applicable law
[_] financial account login credentials
[_] financial account number, or payment card number, in combination with any password, code or other credential that provides access to a financial account