Last Modified: June 20, 2023

Need a signed copy? Click here

Need a Japanese Translation Click here

DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Schedules, ("**DPA**") is an addendum to and forms part of the Master Subscription Agreement (or other such titled written or electronic agreement addressing the same subject matter) for the purchase of the Hosted Service (the "**Principal Agreement**") to reflect the parties' agreement with regard to the Processing of Personal Data.

In the course of providing the Hosted Service to Customer pursuant to the Principal Agreement, BlackLine may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data, each acting reasonably and in good faith.

Any inquiry regarding the Processing of Personal Data under this DPA can be referred to BlackLine's Data Protection Officer at data.protection.officer@blackline.com.

THIS DPA IS INCORPORATED BY REFERENCE:

1. This DPA consists of two parts: the main body of the DPA, and Schedules 1, 2, 3, 4 and 5.

2. The terms of this DPA are incorporated by reference into the Principal Agreement. Except as otherwise expressly provided in the Principal Agreement, this DPA is effective and will become legally binding as of the effective date of the Principal Agreement.

3. To the extent Personal Data from the European Economic Area (EEA), the United Kingdom or Switzerland are Processed by BlackLine, Customer's acceptance of the Principal Agreement, and Customer's execution of an Order Form, shall be deemed to constitute acceptance of the applicable Transfer Mechanism (as defined below, for example, the Standard Contractual Clauses) and such Transfer Mechanism will be incorporated by reference into this DPA.

4. The name of the data exporter on page 11 (Schedule 2) and page 17 (Schedule 4) will be Customer, as defined in this DPA, and the contact person of the data exporter will be the Customer's license administrator as set out on the BlackLine Order Form.

HOW THIS DPA APPLIES:

If the Customer entity entering into this DPA is a party to the Principal Agreement, then this DPA is an addendum to and forms a part of the Principal Agreement. In such case, the BlackLine entity that is party to the Principal Agreement is party to this DPA.

If the Customer entity entering into this DPA is not a party to a BlackLine Order Form and the Principal Agreement, this DPA is not valid and is not legally binding. Such entity should request that the Customer entity who is a party to the Principal Agreement executes this DPA.

If the Customer entity entering into this DPA is not a party to a BlackLine Order Form and a Principal Agreement directly with BlackLine but is instead a customer indirectly via an authorized reseller or partner of BlackLine's Hosted Service, this DPA is not valid and is not legally binding. Such entity should contact the authorized reseller or partner to discuss whether any amendment to its agreement with that reseller may be required.

Data Processing Terms

1. Definitions

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity, or the right to direct the affairs of a subject entity.

"**Applicable Law**" shall mean all regional, national and international applicable laws, orders, statutes, codes, regulations, ordinances, decrees, rules, subordinate legislation, treaties, directives, bylaws, standards or other requirements with similar effect of any governmental or regulatory authority, which apply to Customer or BlackLine in the circumstances governed by this DPA, including Data Protection Laws.

"**BlackLine**" means the BlackLine entity which is a party to this DPA, as specified in the section "HOW THIS DPA APPLIES" above, being BlackLine Systems, Inc., a company incorporated in California, US; BlackLine K.K., a company incorporated in Japan; or as applicable.

"**Customer**" shall mean the entity entering into this DPA that is a party to the Principal Agreement.

"**Customer Data**" means what is defined in the Principal Agreement as "Customer Data", provided that such data is electronic data and information submitted by or for Customer to the Hosted Service.

"**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data.

"**Data Breach**" means the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer's Personal Data transmitted, stored or otherwise Processed by BlackLine or its Sub-processors.

"**Data Protection Laws**" means all laws and regulations (including, without limitation, European Data Protection Laws), which are applicable to BlackLine's or a Sub-processor's Processing of Personal Data under the Principal Agreement.

"**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates.

"**Europe**" means the European Union ("**EU**"), the European Economic Area and/or their member states ("**EEA**"), Switzerland and the United Kingdom ("**UK**").

"**European Data**" means Personal Data that is subject to the protection of European Data Protection Laws.

"**European Data Protection Laws**" means Data Protection Laws applicable in Europe, including, without limitation: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("**GDPR**"); (ii) applicable national implementations of the GDPR; (iii) the Swiss Federal Act on Data Protection of 19 June 1992 ("**FADP**"); and (iv) the United Kingdom Data Protection Act 2018 and the GDPR as saved into the United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

"Hosted Service" shall mean BlackLine's online products reflected on an Order Form (as defined in the Principal Agreement) accessed at a web site designated by BlackLine, or ancillary services rendered to Customer by BlackLine, to which Customer is being granted access under the Principal Agreement.

"**Personal Data**" means any information relating to an identified or identifiable natural person contained within Customer Data, to the extent such information is protected under Data Protection Laws and Processed by BlackLine or a Sub-processor under the Principal Agreement. An identifiable natural person is one who can be identified, directly or indirectly, in particular 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.

"**Processing**" (or "**Processed**" or "**Process**") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" means the entity which Processes Personal Data on behalf of the Controller.

"**Sub-processor**" shall mean any third-party Processor engaged by BlackLine to Process Personal Data in order to provide the Hosted Service under the Principal Agreement.

"**Supervisory Authority**" means (a) an independent public authority which is established by an EU member state pursuant to the GDPR, (b) for the United Kingdom, the Information Commissioner's Office, or (c) other independent competent public authority established or recognized under Data Protection Laws.

"**Worker**" shall mean any employee, staff member, agency worker or other full time or temporary, paid or unpaid person working for BlackLine.

2. Introduction

2.1. This DPA governs the manner in which Personal Data shall be Processed. BlackLine is the Processor of Personal Data and Customer is the Controller of Personal Data under this DPA and the Principal Agreement.

2.2. The Hosted Service is provided by BlackLine under a Software as a Service (SaaS) model, namely, Customer brings its own data and largely controls the upload and handles directly the use of Customer Data that has been uploaded into the Hosted Service. Customer agrees and understands that BlackLine will not monitor Customer Data or Customer's use of any such Customer Data, unless Customer submits an explicit written request to BlackLine to access Customer Data. In any other case, only Customer knows which data comprise the Customer Data. It is therefore the sole responsibility and liability of Customer to ensure that Customer Data is collected and transmitted to BlackLine in compliance with applicable Data Protection Laws and, in particular, to have a legal basis for Processing and to properly inform Data Subjects of the collection and Processing of their Personal Data. Customer will, in its use of the Hosted Service, Process Personal Data in accordance with the requirements of Data Protection Laws.

2.3. The subject-matter of Processing of Personal Data, the duration of the Processing of Personal Data, the nature and purpose of the Processing of Personal Data, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 2 to this DPA.

3. General Personal Data Obligations

3.1. The parties shall comply with the terms of this DPA, and each party is responsible for compliance with its respective obligations under applicable Data Protection Laws.

3.2. BlackLine shall Process Personal Data on behalf of Customer only in accordance with this DPA and documented instructions received from Customer. Customer hereby instructs BlackLine to Process Personal Data: (i) in accordance with the Principal Agreement and applicable Order Form(s), including to provide, support, maintain and improve the Hosted Service; (ii) to comply with documented reasonable instructions received from Customer (e.g., via email) where such instructions are consistent with the terms of the Principal Agreement; and (iii) where required by Applicable Law. Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. BlackLine shall notify Customer about any instruction from Customer which, in BlackLine's opinion, infringes Data Protection Laws.

3.3. If BlackLine is legally required to Process Personal Data otherwise than as instructed by Customer, it shall inform Customer before such Processing occurs, unless the law requiring such Processing prohibits BlackLine from informing Customer on an important ground of public interest, in which case it shall notify Customer as soon as that law permits it to do so.

3.4. Additional instructions outside the scope of this DPA (if any) shall require prior written agreement between BlackLine and Customer, including agreement on any additional fees payable by Customer to BlackLine for carrying out such instructions.

3.5. BlackLine Workers: (i) who have access to Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (ii) shall Process Personal Data only as instructed to by Customer, unless otherwise required to do so by Data Protection Laws; and (iii) shall be provided training as necessary from time to time with respect to BlackLine's obligations under this DPA and under Data Protection Laws.

3.6. BlackLine will not publish, disclose, divulge or otherwise permit third parties to access any Personal Data, except, in each case, in accordance with the Principal Agreement and this DPA (including as necessary to maintain and provide the Hosted Service and to Sub-processors in accordance with this DPA), with Customer's consent or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order).

3.7. Upon Customer's request, BlackLine shall provide Customer with reasonable cooperation and assistance needed to fulfil Customer's obligation under Data Protection Laws to carry out a data protection impact assessment related to Customer's use of the Hosted Service or with any prior consultation that Customer is legally required to make under Data Protection Laws in respect of Personal Data, taking into account the nature of the Processing and to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to BlackLine.

3.8. Upon Customer's written request, BlackLine will provide reasonable assistance to Customer in the event of an investigation by or request from any regulator, including a Supervisory Authority, or similar authority, if and to the extent that such investigation or request relates to Personal Data. BlackLine will take steps reasonably requested by Customer to assist Customer in complying with any obligations in connection with such an investigation or request.

4. Sub-processors

4.1. Customer agrees that BlackLine may use Sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services. BlackLine's website (currently posted at https://www.blackline.com/legal/subprocessors/) lists Sub-processors that are currently engaged by BlackLine to carry out Processing activities on Personal Data on behalf of Customer. BlackLine shall inform Customer in writing of any intended changes to that list through the addition or replacement of Sub-processors at least thirty (30) days in advance, thereby giving Customer sufficient time to be able to object to such changes prior to the engagement of the Sub-processor(s). If, within 30 days of receipt of that notice, Customer notifies BlackLine in writing of any reasonable objections to the proposed appointment based on reasonable grounds relating to data protection or Data Protection Laws, the parties shall negotiate in good faith a mutually acceptable alternative. If no such alternative is agreed within two months of the objection, Customer may terminate the applicable Order Form(s) with respect only to the Hosted Service which cannot be provided by BlackLine without the use of the objected-to new Sub-processor by providing written notice to BlackLine, with any such termination to be effective upon the conclusion of the then current billing cycle as set forth in the applicable Order Form(s).

4.2. Where BlackLine engages a Sub-processor to carry out specific Processing activities (on behalf of Customer), it shall do so by way of a written contract that provides for substantially similar data protection obligations as those binding BlackLine under this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Hosted Service provided by such Sub-processor. BlackLine conducts appropriate due diligence on its Sub-processors.

4.3. BlackLine shall remain fully responsible to Customer for the performance of the Sub-processor's obligations under its contract with BlackLine and for any acts or omissions of the Sub-processors that cause BlackLine to breach any of BlackLine's obligations under this DPA.

5. Data Transfers

5.1. Where Personal Data is transferred from Europe to a country outside of Europe, the parties acknowledge that steps must be taken to ensure that such data transfers comply with European Data Protection Laws. The parties

acknowledge that similar obligations can apply for international transfers of Personal Data from a non-European country and shall in good faith take the steps required where necessary under Data Protection Laws to ensure the transfer complies with Data Protection Laws.

5.2. To the extent Customer's use of the Hosted Service requires an onward transfer mechanism to lawfully transfer European Data from Europe to BlackLine or a Sub-processor located outside of Europe, the terms set forth in Schedule 1 (Europe Specific Provisions) of this DPA will apply to the Processing of European Data.

5.3. Customer Data is hosted in the region Customer requests at the time the Principal Agreement is signed. BlackLine will not host Customer Data in a different region, except with Customer's prior authorization, as necessary to provide the Hosted Service initiated by Customer or as necessary to comply with the law or binding order of a governmental body. BlackLine and its Sub-processors may Process Customer Data from outside the hosting region in accordance with the Principal Agreement and this DPA. Any such cross-border Processing is hereby authorized by the Customer, provided it is in compliance with Data Protection Laws.

6. Notification of Access Requests and Complaints

6.1. BlackLine shall, to the extent legally permitted, promptly notify Customer of any Data Protection Communication it receives. "**Data Protection Communication**" shall mean (i) any request received directly by a party from a Data Subject to exercise the Data Subject's rights under Data Protection Laws (e.g., right of access or have copies of Personal Data, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or its right not to be subject to an automated individual decision making pertaining to his or her Personal Data); or (ii) any complaint or allegation made to a party relating to Personal Data, either from a Data Subject, a Supervisory Authority or other third party.

6.2. BlackLine shall not respond to a Data Protection Communication it receives, unless BlackLine is authorized to do so by Customer or BlackLine is legally compelled to respond.

6.3. Where BlackLine is compelled to respond to a Data Protection Communication, unless prohibited by law, it shall permit Customer to make representations and/or participate in the response process to ensure compliance with Data Protection Laws.

6.4. Customer is responsible for responding to a Data Protection Communication received directly by Customer by using its own access to the relevant Personal Data. If Customer is unable to access the relevant Personal Data after reasonable efforts, BlackLine will, at Customer's request, provide reasonable assistance to Customer in responding to any such Data Protection Communication directly received by Customer to the extent the response to such Data Protection Communication is required under Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from BlackLine's provision of such assistance.

7. Data Security Requirements

7.1. BlackLine shall, with regard to the state of the art and costs of implementation as well as taking into account the nature, scope, context and purposes of the Processing and the risk of varying likelihood and severity for the rights and freedoms of individuals, implement, maintain and comply with comprehensive information and network security programs, practices and procedures that govern the Hosted Service to ensure a level of security appropriate to the risk.

7.2. In assessing the appropriate level of security, BlackLine shall take into account the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise Processed.

7.3. BlackLine implements appropriate technical and organizational measures for the protection of Personal Data as detailed in Schedule 2.

8. Data Breach

8.1. BlackLine shall notify Customer without undue delay after becoming aware of a Data Breach. In the event of a Data Breach, BlackLine shall provide Customer with all reasonable assistance in investigating and mitigating the adverse effects of any such Data Breach. BlackLine will also provide all reasonable assistance to Customer to enable

Customer to comply with its obligations under Data Protection Laws to notify the competent Supervisory Authority and the affected Data Subjects, taking into account the nature of Processing and the information available to BlackLine.

8.2. Unless legally required by Data Protection Laws, BlackLine will not disclose Customer's identity in any communication about the Data Breach to any third party without obtaining Customer's prior written consent.

9. Certification and Audits

9.1. BlackLine is certified under ISO 27001 and attested to SSAE 18 / ISAE 3402 audit standards and agrees to maintain an information security program for the Hosted Service that complies with the ISO 27001 standards or such other alternative standards that are substantially equivalent to these standards for the establishment, implementation, control and improvement of BlackLine security standards.

9.2. BlackLine uses external auditors to validate the adequacy of its security standards and controls. Audit activities: (i) will be performed at least annually; (ii) will be performed according to ISO 27001 / SSAE 18 / ISAE 3402 standards or such other alternative standards that are substantially equivalent to ISO 27001; (iii) will be performed by independent third-party security professionals at BlackLine's selection and expense; and (iv) will result in the generation of an audit report, which will be deemed BlackLine's confidential information.

9.3. At Customer's written request, BlackLine will provide Customer with a confidential report summarizing the records set forth in Section 9.2 above so that Customer can reasonably verify BlackLine's compliance with its obligations under this DPA.

9.4. Customer may audit BlackLine's compliance with its obligations under this DPA up to once per year; additionally, to the extent required by Data Protection Laws, including where mandated by Customer's Supervisory Authority, Customer or Customer's Supervisory Authority may perform more frequent audits of the procedures relevant to the protection of Customer's Personal Data (collectively, "**Customer Audit**"). BlackLine will contribute to such Customer Audits by providing Customer or Customer's Supervisory Authority with the information and assistance reasonably necessary to conduct the Customer Audit, including any relevant records of Processing activities applicable to the Hosted Service ordered by Customer.

9.5. If a third party is to conduct the Customer Audit, the third party must be mutually agreed to by Customer and BlackLine (except if such third party is a competent Supervisory Authority). BlackLine will not unreasonably withhold its consent to a third-party auditor requested by Customer. The third party must execute a written confidentiality agreement acceptable to BlackLine or otherwise be bound by a statutory confidentiality obligation before conducting the Customer Audit.

9.6. To request a Customer Audit, Customer must submit a detailed proposed audit plan to BlackLine at least four weeks in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. BlackLine will review the proposed audit plan and provide Customer with any concerns or questions (for example, any request for information that could compromise BlackLine security, privacy, employment or other relevant policies). BlackLine will work cooperatively with Customer to agree on a final audit plan. Before the commencement of any Customer Audit, Customer and BlackLine shall mutually agree upon the scope, timing, and duration of the Customer Audit.

9.7. If the requested audit scope is addressed in a SSAE 18/ISAE 3402, ISO or similar audit report or certification issued by a qualified third party auditor within the prior twelve months and BlackLine provides such report or certification to Customer confirming there are no known material changes in the controls audited, Customer agrees to accept the findings presented in the third party audit report or certification in lieu of requesting an audit of the same controls covered by the report or certification.

9.8. The Customer Audit must be conducted during regular business hours at the applicable facility, subject to the agreed final audit plan and BlackLine's health, safety, security or other relevant policies, and may not unreasonably interfere with BlackLine's business activities or operations. Nothing in this Section 9 shall require BlackLine to breach its obligations under Applicable Law or breach its confidentiality, security or privacy obligations to any customers, employees or third parties.

9.9. Customer will provide BlackLine any audit reports generated in connection with any Customer Audit, unless prohibited by Applicable Law or otherwise instructed by a Supervisory Authority. Customer may use the audit reports only for the purposes of meeting Customer's regulatory audit requirements and/or confirming compliance with the requirements of this DPA. The audit reports are Confidential Information of the parties under the terms of the Principal Agreement.

9.10. Any Customer Audits are at Customer's expense. The parties will negotiate in good faith with respect to any charges or fees that may be incurred by BlackLine to provide assistance with a Customer Audit that requires the use of resources different from or in addition to those required for the provision of the Hosted Service. Before the commencement of a Customer Audit, Customer and BlackLine shall mutually agree upon the reimbursement rate for which Customer shall be responsible for any time expended for any such Customer Audit. All reimbursement rates shall be reasonable, taking into account the resources expended by BlackLine.

10. Return and Deletion of Personal Data

BlackLine will delete or return all Customer Data, including Personal Data, on termination or expiration of the Principal Agreement in accordance with the Principal Agreement. Until all Personal Data is deleted or returned, BlackLine shall continue to ensure compliance with this DPA. If Applicable Law prohibits the return or deletion of Personal Data, BlackLine will continue to ensure compliance with this DPA and will only Process Personal Data to the extent and for as long as required under Applicable Law.

11. Requests for Personal Data from Governmental Bodies

11.1. If BlackLine receives a valid and binding order ("**Request**") from any governmental body ("**Requesting Party**") for disclosure of Personal Data, BlackLine will, to the extent permitted by Applicable Law, use every reasonable effort to redirect the Requesting Party to request Personal Data directly from Customer. As part of this effort, BlackLine may provide Customer's basic contact information to the Requesting Party.

11.2. If compelled to disclose Personal Data to a Requesting Party, BlackLine will give Customer reasonable notice of the Request to allow Customer to seek a protective order or other appropriate remedy, unless BlackLine is legally prohibited from doing so. If BlackLine is prohibited from notifying Customer about the Request, BlackLine will (a) use all reasonable and lawful efforts to obtain a waiver of prohibition, to allow BlackLine to communicate as much information to Customer as soon as possible; and (b) to the extent permitted by Applicable Law, challenge any overbroad or inappropriate Request (including where such Request conflicts with the law of Europe).

11.3. If, after exhausting the steps described above in this Section, BlackLine remains compelled to disclose Personal Data to a Requesting Party, BlackLine will disclose only the minimum amount of Personal Data necessary to satisfy the Request.

11.4. Nothing in this Section restricts Customer's Data Subjects from exercising their rights under the GDPR, including their rights to compensation from BlackLine for material or non-material damage under, and in accordance with, Article 82 of the GDPR.

12. Liability

Each party and each of their affiliates' liability, taken in aggregate, arising out of or related to this DPA, will be subject to the limitations and exclusions of liability set out in the Principal Agreement and any reference in such section to the liability of a party means aggregate liability of that party and all of its affiliates under the Principal Agreement (including this DPA).

13. Miscellaneous

13.1. In the event of any conflict or inconsistencies between the provisions of this DPA and the Principal Agreement, the provisions of this DPA shall prevail.

13.2. This DPA will remain in effect until, and will automatically expire upon, return or deletion of all Personal Data by BlackLine and any applicable Sub-processors.

13.3. If any provision of this DPA is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this DPA, and all provisions not affected by such invalidity or unenforceability will remain in full force and effect.

13.4. The section "HOW THIS DPA APPLIES" above specifies which BlackLine entity is party to this DPA. Where a Transfer Mechanism applies, BlackLine Systems, Inc. is the party to the Transfer Mechanism (including the Standard Contractual Clauses). Where the BlackLine entity that is a party to this DPA is not BlackLine Systems, Inc., that BlackLine entity is carrying out the obligations of the data importer on behalf of BlackLine Systems, Inc. Such other BlackLine entities are not a party to the Transfer Mechanism or this DPA (only the BlackLine entity specified in the section "HOW THIS DPA APPLIES" above is a party to this DPA).

Schedule 1 – Europe Specific Provisions

This Schedule 1 is supplemental to the DPA and sets out the terms that apply to the extent that Customer's use of the Hosted Service requires an onward transfer mechanism to lawfully transfer European Data from Europe to BlackLine or a Sub-Processor in a country located outside of Europe that does not ensure an adequate level of data protection within the meaning of European Data Protection Laws.

A. Definitions

1. "**2021 EU SCCs**" means the Standard Contractual Clauses sections I, II, III and IV (as applicable) to the extent they reference Module Two (Controller-to-Processor) for the transfer of Personal Data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, as currently set out at https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf, subject to the terms in this Schedule 1.

2. "**UK International Data Transfer Addendum**" or "**UK IDTA**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the United Kingdom Information Commissioner under section 119A(1) of the Data Protection Act 2018, Version B1.0, in force 21 March 2022, as currently set out at https://ico.org.uk/media/fororganisations/documents/4019539/international-data-transfer-addendum.pdf, subject to Schedule 1 and Schedule 4.

3. "**Swiss SCCs**" means the 2021 EU SCCs, as amended by the Swiss Addendum in Schedule 3, subject to the terms in this Schedule 1.

4. "**Transfer Mechanism**" means, depending on the circumstances unique to Customer, any of the following: (a) the 2021 EU SCCs, (b) the Swiss SCCs, and/or (c) the UK IDTA.

B. Transfer Mechanisms for European Data Transfers

1. **2021 EU SCCs**. The 2021 EU SCCs will apply to European Data that is transferred from the EEA to any country or recipient outside the EEA that is not recognized by the European Commission as providing an adequate level of protection for European Data. For European Data transfers from the EEA that are subject to the 2021 EU SCCs, the 2021 EU SCCs will be deemed entered into (and incorporated into this DPA by this reference).

2. **UK International Data Transfer Addendum**. The UK IDTA will apply to European Data that is transferred from the UK to any country or recipient outside the UK that is not recognized by the competent UK regulatory authority or governmental body for the UK as providing an adequate level of protection for European Data. For European Data transfers from the UK that are subject to the UK IDTA, the UK IDTA will be deemed entered into (and incorporated into this DPA by this reference).

3. **Swiss SCCs.** The Swiss SCCs will apply to European Data that is transferred from Switzerland to any country or recipient outside Switzerland that is not recognized by the competent authority for Switzerland as providing an adequate level of protection for European Data. For European Data transfers from Switzerland that are subject to the Swiss SCCs, and pursuant to the statement issued 27 August 2021 by the FADP, the Swiss SCCs will be deemed entered into (and incorporated into this DPA by this reference).

4. **Invalid Transfer Mechanism**. In the event that a Transfer Mechanism is no longer a valid mechanism for transfer of European Data, the parties shall, as required by European Data Protection Laws, negotiate in good faith a mutually acceptable alternative, valid mechanism.

5. **Notice & Conflicts**. Any notice to be given under a Transfer Mechanism will be made in accordance with this DPA and the Principal Agreement. In the event of any conflict or inconsistency between the body of this DPA and a Transfer Mechanism, the Transfer Mechanism shall prevail.

C. Terms for the 2021 EU SCCs

1. **Docking Clause.** In Clause 7 of the 2021 EU SCCs, the optional docking clause will apply.

2. **Redress**. In Clause 11 of the 2021 EU SCCs, the optional language will not apply.

3. **Supervision**. Where Customer is the data exporter, the supervisory authority shall be the competent supervisory authority that has supervision over the Customer in accordance with Schedule 2 of this DPA.

4. **Governing Law**. In Clause 17 (Option 1), the 2021 EU SCCs will be governed by the law of the Netherlands.

5. **Jurisdiction**. In Clause 18(b) of the 2021 EU SCCs, disputes will be resolved before the courts of the Netherlands.

6. **Annex I and II.** See Schedule 2 for the information in Annex I and Annex II of the 2021 EU SCCs.

7. **Instructions**. This DPA and the Principal Agreement are Customer's complete and final documented instructions to BlackLine for the Processing of Personal Data. Any additional or alternate instructions must be consistent with the terms of this DPA and the Principal Agreement. For the purposes of Clause 8.1(a) of the 2021 EU SCCs, the instructions by Customer to Process Personal Data are set out in this DPA and the Principal Agreement and include onward transfers to a third party located outside Europe for the purpose of the performance of the Hosted Service in accordance with this DPA and the Principal Agreement.

8. **New Sub-processors and List of current Sub-processors**. Option 2 under Clause 9 shall apply. For the purposes of Clause 9(a), BlackLine has Customer's general authorization to engage Sub-processors in accordance with this DPA. BlackLine shall make available to Customer the current list of Sub-processors in accordance with this DPA. Pursuant to Clause 9(a), Customer acknowledges and expressly agrees that BlackLine may engage new Sub-processors as described in this DPA. BlackLine shall inform Customer of any changes to Sub-processors following the procedure provided for in this DPA.

9. **Copies of Sub-processor Agreements**. The parties agree that the copies of the Sub-processor agreements that must be provided by BlackLine to Customer pursuant to Clause 9(c) of the 2021 EU SCCs may have all commercial information, or clauses unrelated to the 2021 EU SCCs or their equivalent, removed by BlackLine beforehand; and, that such copies will be provided by BlackLine, in a manner to be determined in its discretion, only upon written request by Customer.

10. **Audits and Certifications**. The parties agree that the audits described in Clause 8.9 of the 2021 EU SCCs shall be carried out in accordance with this DPA.

11. **Certification of Deletion**. The parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 and 16(d) of the 2021 EU SCCs shall be provided by BlackLine to Customer only upon Customer's written request.

12. **Security of Processing**. For the purposes of Clause 8.6(a) of the 2021 EU SCCs, Customer is solely responsible for making an independent determination as to whether the technical and organizational measures set forth in this DPA meet Customer's requirements and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing of its Personal Data as well as the risks to individuals) the security measures and policies implemented and maintained by BlackLine provide a level of security appropriate to the risk with respect to its Personal Data. For the purposes of Clause 8.6(c) of the 2021 EU SCCs, Personal Data breaches will be handled in accordance with this DPA.

13. **Notification of Government Access Requests**. For the purposes of Clause 15(1)(a) of the 2021 EU SCCs, BlackLine shall notify Customer (only) and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary.

Schedule 2 – 2021 EU SCCs Annexes

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: Customer, as defined above in this DPA

Address: Customer's address, as set out in the BlackLine Order Form

Contact person's name, position and contact details: The Customer contact details of its license administrator, as set out in the BlackLine Order Form

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with the provision of the Hosted Service and Customer's use of the Hosted Service under the Principal Agreement

Role: Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: BlackLine Systems, Inc.

Address: 21300 Victory Blvd., 12th Floor, Woodland Hills, CA 91367, USA

Contact person's name, position and contact details: Data Protection Officer. Tel.: 1-877-777-7750. E-mail: data.protection.officer@blackline.com

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with the provision of the Hosted Service and Customer's use of the Hosted Service under the Principal Agreement. BlackLine provides cloud-based accounts receivable, intercompany financial management, account reconciliation and financial close accounting software, which may involve Processing Personal Data provided by the data exporter in accordance with the terms of the Principal Agreement.

Role: Processor

B. DESCRIPTION OF TRANSFER

DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter may submit Personal Data to the Hosted Service provided by data importer, the extent of which is determined and controlled by data exporter. Such data may include Personal Data relating to data exporters' employees, clients, contractors, business partners or other individuals whose Personal Data is stored in the Hosted Service.

Categories of personal data transferred

Data exporter may submit Personal Data to the Hosted Service provided by data importer, the extent of which is determined and controlled by data exporter. Such data may include the following categories of Personal Data:

- First and last name
- Title, position, employer
- Contact details (company, email, phone, physical business address)
- Invoice data

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.

- None. The parties do not anticipate the transfer of sensitive data.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- Continuous basis given the use of the Hosted Service as determined by the data exporter

Nature of the processing

- Processing of Personal Data in connection with the provision of the Hosted Service and Customer's use of the Hosted Service under the Principal Agreement.

Purpose(s) of the data transfer and further processing

- The data importer is Processing Personal Data for the purpose of providing, supporting, maintaining and improving the Hosted Service (in accordance with the DPA)
- Data importer will Process Personal Data in accordance with the Principal Agreement and where required by Applicable Law
- Data importer will Process Personal Data to comply with other documented reasonable instructions received by data exporter (e.g., via email) where such instructions are consistent with the terms of the DPA and the Principal Agreement.

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

- Data importer will generally Process Personal Data for the duration of the Principal Agreement, unless otherwise agreed upon in writing.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

- As per the "*purpose(s) of the data transfer and further processing*" section above, the Sub-processor will Process Personal Data as necessary to provide the Hosted Service and perform the services pursuant to the Principal Agreement.
- Subject to the terms of the DPA, the Sub-processor will Process Personal Data for the duration of the Principal Agreement, unless otherwise agreed in writing.
- Data importer may transfer Personal Data to its Sub-processors in accordance with the DPA.
- For clarity, there are no specific restrictions when the Data Import may transfer Personal Data other than those set forth in the DPA.
- The subject matter, nature and location of the Processing of Personal Data by Sub-processors is listed on BlackLine's website at the following link: https://www.blackline.com/legal/subprocessors.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

a) Where the data exporter is established in an EU Member State, the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

b) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679, the supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established shall act as competent supervisory authority.

c) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) shall act as competent supervisory authority.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the data importer(s) (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

Overview of the technical and organisational measures to be taken by the data importer.

Physical Access Control

Measures to ensure that only those explicitly authorized will have physical access to systems used to process Personal Data.

- security guards, doormen
- keys and corresponding documentation
- electronic access control system
- video surveillance
- security checks for any external companies/services
- security checks for visitors
- security guidelines for utilization of mobile devices

System Access Control

Measures to prevent data processing systems from being used without authorization:

- password guidelines (e.g., digits/special characters, min. length, expiration, uniqueness)
- multi-factor authentication
- automatic log-out or password-protected screensaver after certain period without user activity
- access authentication rules

- firewall, anti-virus protection
- intrusion detection/intrusion prevention
- logging of access
- securing external interfaces

Data Access Control

Measures to ensure that those authorized to use data processing systems have access only to those data they are authorized to access, and that Personal Data cannot be read, copied, altered or removed without authorization during processing, use and after:

- access control (access rights limited by profiles and roles)
- documentation of access rights
- approval and assignment of access rights through authorized personnel only

Data Transfer Control

Measures to ensure that Personal Data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred Personal Data using data transmission facilities:

- transport encryption
- encryption of physical data carriers

Data Entry Control

Measures to ensure that it is possible to check and ascertain whether Personal Data have been entered into, altered or removed from data processing systems and if so, by whom:

- documenting/logging of physical access
- logging of system access (*e.g.*, login name, IP address)
- logging of individual actions
- other event logging (*e.g.*, intrusion and hacking attempts, unsuccessful login attempts)

Availability Control

Measures to ensure that Personal Data are protected against accidental destruction or loss:

- backup in separate location and regular tests of recovery procedures
- business continuity/disaster recovery
- uninterruptable power supply (UPS)
- anti-theft measures
- fire protection (early-warning-fire-detection, extinguishing system)
- water protection
- redundant air conditioning system

Separation of Data

Measures to ensure that data collected for different purposes can be processed separately:

- clear physical and/or logical separation of data from data of other Controllers
- physical and/or logically separated systems for development and production environments
- pseudonymisation of data, where appropriate

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.

As per Section 4 (Sub-processors) in the DPA above, a Sub-processor's technical and organizational measures will be substantially similar to the data importer's technical and organizational measures set forth above in this Annex II with respect to the protection of Personal Data to the extent applicable to the nature of the Hosted Service provided by the Sub-processor.

Schedule 3 – Swiss Addendum

This Schedule 3 ("**Swiss Addendum**") shall apply only if BlackLine, in the performance of the Hosted Service, transfers European Data from Switzerland to a country that has not been recognized by the relevant authorities as providing an adequate level of protection of European Data, to the extent such transfers are subject to the Swiss Data Protection Laws, pursuant to the statement issued 27 August 2021 by the FADP.

1. Interpretation of this Addendum

1.1. Where this Swiss Addendum uses terms that are defined in the Clauses, those terms shall have the same meaning as in the 2021 EU SCCs. In addition, the following terms have the following meanings:

This Swiss Addendum	This Swiss Addendum to the 2021 EU SCCs
Clauses	The 2021 EU SCCs
FADP	The Swiss Federal Act on Data Protection of 19 June 1992

1.2. This Swiss Addendum shall be read and interpreted in the light of the provisions of the FADP, and so that it fulfils the intention for it to provide the appropriate safeguards as required by Article 46 GDPR.

1.3. This Swiss Addendum shall not be interpreted in a way that conflicts with rights and obligations provided for in the FADP.

1.4. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, reenacted and/or replaced after this Swiss Addendum has been entered into.

1.5. This Swiss Addendum shall remain in force until the entry of a revised FADP.

2. Hierarchy

In the event of a conflict or inconsistency between this Swiss Addendum and the provisions of the Clauses or other related agreements between the parties, existing at the time this Addendum is agreed or entered into thereafter, the provisions which provide the most protection to Data Subjects shall prevail.

3. Incorporation of the Clauses

3.1. In relation to any processing of personal data subject to Swiss Data Protection Law, this Swiss Addendum amends the Clauses to the extent necessary so they operate:

a. for transfers made by the data exporter to the data importer, to the extent that the FADP applies to the data exporter's processing when making that transfer; and

b. to provide appropriate safeguards for the transfers in accordance with the FADP.

3.2. The amendments to the Clauses as required by Section 3.1 above, include (without limitation):

a. Clause 6 Description of the transfer(s) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred are those specified in Annex I.B where the FADP applies to the data exporter's processing when making that transfer."

b. References to "*Regulation (EU) 2016/679*" or "*that Regulation*" or "*GDPR*" are replaced by "*the FADP*" and references to specific Article(s) of "*Regulation (EU) 2016/679*" or "*GDPR*" are replaced with the equivalent Article or Section of the FADP.

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

d. References to the "*European Union*", "*Union*", "*EU*", "*EEA*", "*EU Member State*", "*Member State of the EU*", "*Member State of the EEA*" and "*member state*" are all replaced with the "*Switzerland*".

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

f. Clause 17 is replaced to state "*These Clauses are governed by the laws of Switzerland*".

g. Clause 18 is replaced to state:

"*Any dispute arising from these Clauses shall be resolved by the courts of Switzerland. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of Switzerland. The parties agree to submit themselves to the jurisdiction of such courts*."

h. The footnotes to the Clauses do not form part of the Swiss Addendum.

Schedule 4 - UK Addendum

This Schedule 4 ("**UK Addendum**") shall apply only if BlackLine, in the performance of the Hosted Service, transfers European Data from the United Kingdom to a country that has not been recognized by the relevant authorities as providing an adequate level of protection of European Data, to the extent such transfers are subject to UK Data Protection Laws.

Table 1: Parties

Start date	Effective date of the DPA to which this Schedule is attached.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: BlackLine Customer, as set out on the applicable BlackLine Order Form Trading name (if different):_____ Main address (if a company registered address): As set out on the applicable BlackLine Order Form Official registration number (if any) (company number or similar identifier): _____	Full legal name: BlackLine Systems, Inc. Trading name (if different): BlackLine Main address (if a company registered address): 21300 Victory Blvd., 12th Floor, Woodland Hills, CA 91367, USA Official registration number (if any) (company number or similar identifier):
Key Contact	Customer's license administrator as set out on the BlackLine Order Form.	Full Name: Job Title: Data Protection Officer Contact details including email: Tel.: 1-877-777-7750. E-mail: data.protection.officer@blackline.com

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: See effective date of the DPA to which this Schedule is attached. Reference (if any): N/A Other identifier (if any): 2021 EU SCCs as defined in Schedule 1 of the DPA

		Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:				
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	N/A	N/A	N/A	N/A	N/A	N/A
2	N/A	N/A	N/A	N/A	N/A	N/A
3	N/A	N/A	N/A	N/A	N/A	N/A
4	N/A	N/A	N/A	N/A	N/A	N/A

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex IA: List of Parties: See Schedule 2, Annex IA to this DPA.
Annex IB: Description of Transfer: See Schedule 2, Annex IB to this DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Schedule 2, Annex II to this DPA.
Annex III: List of Sub-processors (Modules 2 and 3 only): Annex III not applicable

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19. ☒ Importer ☒ Exporter ☐ neither Party

Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses, is incorporated by reference herein.

Schedule 5 – U.S. Specific Provisions

This Schedule 5 ("**U.S. Addendum**") shall apply solely to the extent that BlackLine, in the provision of the Hosted Service to Customer, Processes Consumer Personal Information.

The terms used in this U.S. Addendum shall have the meanings set forth in this U.S. Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the DPA. The terms and conditions of this U.S. Addendum are in addition to those of the DPA, thus both the DPA and this U.S. Addendum shall apply; provided, however, that in the event of a conflict between the terms and conditions of the DPA and those of this U.S. Addendum, this Addendum shall prevail.

1. **Definitions**.

    a) "**CCPA**" means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.

    b) "**Consumer Personal Information**" means any information that relates to an individual that falls within the definition of "personal information", "personal data" or other comparable term as defined by U.S. Data Protection Laws, to the extent such information is protected under U.S. Data Protection Laws and contained within Customer Data.

    c) "**CPA**" means the Colorado Privacy Act, together with all implementing regulations.

    d) "**CTDPA**" means the Connecticut Act Concerning Data Privacy and Online Monitoring.

    e) "**UCPA**" means the Utah Consumer Privacy Act.

    f) "**U.S. Data Protection Laws**" means all state and federal data privacy regulations of the United States of America (including, without limitation, the CCPA, VCDPA, CPA, CTDPA and UCPA), which are applicable to BlackLine's or a Sub-processor's Processing of Consumer Personal Information under the Principal Agreement.

    g) "**VCDPA**" means the Virginia Consumer Data Protection Act.

    h) For the purposes of this U.S. Addendum only, "**Controller**", "**Processor**", "**Service Provider**", "**Processor**", "**Sell**", "**Share**", "**Business**,", "**Business Purpose**", "**Commercial Purpose**", "**Consumer**" and "**Processing**" shall have the meanings given to these terms in U.S. Data Protection Laws.

2. **Roles of the Parties**. The parties agree that for the purposes of U.S. Data Protection Laws, BlackLine acts as a Service Provider or Processor for Consumer Personal Information with respect to the provision of the Hosted Service under the Principal Agreement.

3. **Definitions in the DPA.**

    a) The definition of "Data Protection Laws" in the DPA includes "U.S. Data Protection Laws" as defined in this U.S. Addendum.

    b) The definition of "Personal Data" in the DPA includes "Consumer Personal Information."

    c) The definition of "Data Subject" in the DPA includes "Consumer."

    d) The definition of "Controller" in the DPA includes "Business."

    e) The definition of "Processor" in the DPA includes "Service Provider."

    f) The definition of "Processing" in the DPA includes "Processing" as defined in U.S. Data Protection Laws.

4. **Data Processing Terms**. By executing the Principal Agreement:

   a) BlackLine will comply with all obligations applicable to it as a Service Provider or Processor under U.S. Data Protection Laws. BlackLine will provide Consumer Personal Information with the same level of privacy protection as is required by U.S. Data Protection Laws.

   b) BlackLine will not Sell or Share Consumer Personal Information.

   c) BlackLine will not retain, use, or disclose Consumer Personal Information for any purpose other than for the Business Purposes specified in the DPA and the Principal Agreement, including retaining, using, or disclosing Consumer Personal Information for a Commercial Purpose other than the Business Purposes specified in the DPA and the Principal Agreement, or as otherwise permitted by Applicable Law.

   d) BlackLine will not retain, use, or disclose Consumer Personal Information outside of the direct business relationship between BlackLine and Customer, unless otherwise permitted by Applicable Law.

   e) Except as otherwise permitted by Applicable Law, BlackLine will not combine Consumer Personal Information with other personal information that it receives from other sources, including the information collected from BlackLine's independent interaction with a Consumer. This does not include combining Consumer Personal Information in the context of the business purpose of providing the Hosted Service.

   f) BlackLine will ensure that it has a written agreement in place with all Sub-processors which contains obligations on the Sub-processor which are no less protective of Consumer Personal Information than the obligations on BlackLine under this U.S. Addendum.

   g) If BlackLine makes a determination that it can no longer meet its obligations under this U.S. Addendum, it shall notify Customer of that determination within the time period required under U.S. Data Protection Laws and cease the Processing of Consumer Personal Information or take other reasonable and appropriate steps to remediate.

   h) Customer has the right to take reasonable and appropriate steps in accordance with the DPA and the Principal Agreement (e.g., Section 9 – Certification and Audits) to help ensure that BlackLine uses Consumer Personal Information in a manner consistent with Customer's obligations under U.S. Data Protection Laws.

   i) Upon notice, Customer will have the right to take reasonable and appropriate steps in accordance with the DPA and Principal Agreement to stop and remediate unauthorized use of Consumer Personal Information.

   j) BlackLine certifies that it has read and understands this U.S. Addendum and will abide by it.

   k) Customer is responsible for ensuring that it has complied, and will continue to comply, with the requirements of U.S. Data Protection Laws in its use of the Hosted Service and its own Processing of Consumer Personal Information.

   l) Customer specifically acknowledges that its use of the Hosted Service will not violate the rights of any Consumer that has opted-out from Sales, Sharing or other disclosures of Consumer Personal Information, to the extent applicable under U.S. Data Protection Laws.