Customer DPA 2024v1

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the Spiff Master Subscription Agreement and accompanying Sales Order(s) (collectively, the "**Agreement**") entered into between Customer and Spiff (each, a "**Party**" and, collectively, the "**Parties**"). In the event of a conflict between the terms of this Addendum and the Agreement, the terms of this Addendum will prevail.

1. **General Processing Obligations and Descriptions.**
   1.1. **Roles of the Parties**. In connection with the Permitted Processing, Spiff is the Data Processor, and Customer is the Data Controller. Spiff will Process Personal Data only as necessary to achieve the Purposes and as otherwise permitted by this Addendum, or as instructed in writing from time to time by Customer (collectively, the "**Permitted Processing**"). The Parties agree that this Addendum, including specifically the terms of this section, constitute the documented instructions of the Data Controller described in Article 28 of the GDPR or the UK GDPR, as applicable, and/or the contract referred to in Sections 1798.100(d) and 1798.140(ag) of the CCPA / CPRA, as applicable. Spiff shall inform Customer if, in Spiff's opinion, any aspect of the Permitted Processing violates applicable Data Protection Law, or if Spiff makes a determination that Spiff is unable to follow Customer's instructions for the Processing of Personal Data. If under Data Protection Laws an Affiliate of Customer is considered the Data Controller (either alone or jointly with the Customer) with respect to certain Personal Data, Customer represents and warrants to Spiff that Customer is authorized: (a) to give the instructions to Spiff and otherwise act on behalf of such Affiliate in relation to such Personal Data as described in this Addendum and (b) to bind the Affiliate to this Addendum.
   1.2. **Subject Matter**. Spiff and Customer enter into this Addendum to establish their respective rights and obligations with regard to Processing of Personal Data in connection with the Products and Services provided under the Agreement.
   1.3. **Purpose of Processing**. Customer is disclosing Personal Data to Spiff, and Spiff is conducting the Permitted Processing, for the limited and specified business purpose of Spiff providing the Products and Services to Customer and otherwise performing its obligations under the Agreement (including this Addendum) (the "**Purposes**"). Spiff may also Process the Personal Data if required to comply with applicable law, provided that, if permitted under such law, Spiff provides Customer with advance written notice of such Processing. Spiff acknowledges and agrees that it may not: (a) sell or share (as each term is defined in the CCPA / CPRA) the Personal Data; (b) retain, use, or disclose the Personal Data for any purpose other than the business purposes specified herein or, without limiting Spiff's rights under Section 1.5, outside of the direct business relationship between Customer and Spiff; or (c) unless otherwise permitted under applicable Data Protection Law, combine the Personal Data received from Customer with personal data received or collected from or on behalf of a third party or in its own interaction with a Data Subject.
   1.4. **Nature of Processing**. Spiff shall, through the Products and Services, receive, store, and perform other Processing activities on the Personal Data as required to fulfill the Purposes. Such Processing shall take place in the United States and other non-EU+ Territories, subject to the Parties' compliance with Section 5.
   1.5. **Sub-processors**. Customer acknowledges and expressly agrees that Spiff may engage third-party Sub-processors in connection with the provision of the Products and Services. Spiff shall ensure that all such Sub-processors are subject to terms consistent with those set forth in this Addendum. A list of Sub-processors engaged by Spiff in connection with the provision of the Products and Services can be found at the end of this Addendum and may be updated via email notification or via a webpage link to be provided to Customer. If such webpage ceases to be maintained, Spiff shall make available to Customer from time to time at its reasonable request a current list of Sub-processors for the respective Products and Services.
   1.6. **Personal Data and Data Subjects**. Spiff is Processing Personal Data of Customer's sales employees and personnel who are compensated on a commission basis as well as Customer's authorized Users of the Products and Services. This Personal Data includes Personal Data within the categories of identifiers, commercial information, professional or employment-related information, Internet and other electronic network activity information, audio data, and inferences drawn from the foregoing.
   1.7. **Duration of Processing**. Spiff will Process the Personal Data for so long as it is providing the Products and Services to Customer. Within 45 days after the conclusion of such provision (including, for clarity, the termination or expiration of the Agreement), Spiff shall delete all Personal Data, provided that Spiff may retain such copies of Personal Data as are required to comply with applicable law. At Customer's written election, Spiff shall also, prior to so deleting, return to Customer all Personal Data then in Spiff's possession, custody, or control.
   1.8. **Compliance with Data Protection Laws**. Each Party shall Process Personal Data in accordance with the requirements of applicable Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data, including specifically providing sufficient information to enable transparent Processing and, if applicable, obtaining free and informed consent to the Processing contemplated under the Agreement and this Addendum.

2. **Spiff Assistance to Customer.**
   2.1. **Data Subject Rights**. Spiff shall, to the extent legally permitted, promptly notify Customer if Spiff receives a request from a Data Subject to exercise the Data Subject's rights granted under applicable Data Protection Law (each such request being a "**Data Subject Request**"). Taking into account the nature of the Processing, Spiff shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Products and Services, does not have the ability to address a Data Subject Request, Spiff shall upon Customer's request provide commercially reasonable

efforts to assist Customer in responding to such Data Subject Request, to the extent Spiff is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws. Unless prohibited under applicable law, Customer shall be responsible for any costs arising from Spiff's provision of such assistance.

2.2. **Data Protection Impact Assessments and Prior Consultations**. Taking into account the nature of the Processing and information available to Spiff, Spiff shall assist Customer with Customer's conduct of a data protection impact assessment and, if necessary, any prior consultations with Governmental Authorities arising out of any such assessment.

2.3. **Audits and Inspections, Records**. Spiff shall, at Customer's reasonable request and sole cost and expense, make available all information reasonably necessary to demonstrate Spiff's compliance with this Addendum and otherwise contribute to audits and inspections carried out by or on behalf of Customer (including any such inspection by a Governmental Authority following a Security Incident). To the fullest extent possible, Customer shall: (i) give Spiff reasonable prior notice of any such audit; (ii) undertake such audit no more than once per calendar year, except for good cause shown; and (iii) conduct or cause to be conducted such audit in a manner designed to minimize disruption of Spiff's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Agreement.

3. **Security Requirements.**

3.1. **Spiff Security Measures**. Spiff shall maintain commercially reasonable technical and organizational measures designed to protect the security, confidentiality, and integrity of Personal Data. Spiff will not materially decrease the overall security of the Products and Services during the term of the Agreement.

3.2. **Confidentiality**. As between the Parties, Personal Data shall be considered the confidential information of Customer in accordance with the Agreement. Notwithstanding the foregoing, nothing set forth herein or in the Agreement shall prevent Spiff from using data regarding Customer's and its Users' use of the Products and Services in an aggregate and anonymized manner, including to compile statistical and performance information related to the use, provision and operation of the Products and Services. Without limiting the foregoing or anything else in this Addendum or the Agreement, Spiff shall ensure that access to Personal Data is limited to the Authorized Personnel and that such Authorized Personnel are subject to binding obligations of confidentiality (whether contractual, statutory, or otherwise) consistent with those set forth in the Agreement.

3.3. **Customer Security Measures**. The security requirements do not limit Customer's responsibility for implementing and maintaining appropriate technical and organizational measures to protect the Personal Data and otherwise using the Products and Services consistent with the Agreement and in a secure manner.

4. **Personal Data Breach Procedures.**

4.1. **Notification**. Spiff shall notify Customer without undue delay after becoming aware of any Security Incident.

4.2. **Mitigation**. Spiff shall (a) make reasonable efforts to identify the cause of such Security Incident; (b) take those steps as Spiff deems necessary and reasonable in order to remediate the cause of such a Security Incident to the extent the remediation is within Spiff's reasonable control; and (c) provide timely information and cooperation as Customer may reasonably require and request in writing to fulfill Customer's data breach reporting obligations under the Data Protection Laws. Spiff may withhold information that it deems confidential or over which it intends to assert attorney-client or similar privilege or protection.

4.3. **Disclosure**. Unless otherwise required by applicable law, Spiff shall not disclose to third parties any information about a Security Incident involving Personal Data without prior written and express permission from Customer for such disclosure; provided, however, nothing herein should be construed to prevent Spiff from publicly acknowledging or disclosing the occurrence of a Security Incident, provided Spiff does not identify Customer in the applicable communication to third parties. Notwithstanding the foregoing, Spiff agrees that Customer has the sole right to determine whether legal notification of a breach of Personal Data shall be provided to individuals, Governmental Authorities, or other third parties, as well as the contents of such notification.

5. **Certain Cross-Border Data Transfers.**

5.1. **Location of Processing**. Customer acknowledges that Spiff will Process Personal Data outside of the European Economic Area (the "**EEA**"), the United Kingdom, and Switzerland (collectively, the "**EU+ Territories**") and may engage Sub-processors that Process Personal Data outside the EU+ Territories. Customer expressly agrees to such Processing and to the transfer of Personal Data from within the EU+ Territories to jurisdictions outside of the EU+ Territories, including to countries not recognized by the European Commission or other applicable Government Authority as providing an adequate level of protection for Personal Data (as described in Article 45 of the GDPR, the UK GDPR, or the FADP, as applicable). Each such transfer shall be subject to the Standard Contractual Clauses.

5.2. **Standard Contractual Clauses**.

(i) The Standard Contractual Clauses apply only to Personal Data that is transferred from the EEA, the United Kingdom (subject to the UK Addendum), Switzerland (subject to Section 5.2(iv) below), or any other jurisdiction that recognizes the Standard Contractual Clauses as a lawful transfer mechanism, either directly or via onward transfer, to any country or recipient: (a) not recognized by the European Commission or other applicable Government Authority as providing an adequate level of protection for Personal Data (as described in Article 45 of the GDPR, the UK GDPR, or the FADP, as applicable) and (b) not covered by a suitable framework recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data. The Standard Contractual Clauses (including, if applicable, the UK Addendum and/or the modifications pursuant to Section 5.2(iv) below) are hereby incorporated by reference with

respect to each applicable transfer.

(ii) To the extent the Parties rely on the Standard Contractual Clauses (with or without the UK Addendum and/or the modifications pursuant to Section 5.2(iv) below), by executing this Addendum, the Parties are deemed to be signing the Standard Contractual Clauses, including Annex I.A thereto and, if applicable, the UK Addendum and/or the modifications pursuant to Section 5.2(iv) below. The Standard Contractual Clauses are deemed completed as follows:

- Customer is the data exporter, Spiff is the data importer, and their respective contact information is set forth in Exhibit A (Sections 1 and 2, respectively) to this Addendum.
- Module Two (Transfer Controller to Processor) applies to transfers occurring pursuant to this Addendum.
- Clause 7 (Optional Docking Clause) does not apply.
- Clause 8.9 (Documentation and Compliance): the Parties agree that audits and requests for audits pursuant to Clause 8.9 shall be done in accordance with Section 2.3 of this Addendum.
- Clause 9(a) (Use of Sub-processors): the Parties elect Option 2 (General Written Authorisation) with a 10-day notice period. The data exporter consents to the data importer's engagement of Sub-processor(s) in accordance with Section 1.5 of this Addendum.
- Clause 11(a) (Redress): the optional section does not apply.
- Clause 17 (Governing Law): the Parties elect Option 1 and agree that the Standard Contractual Clauses shall be governed by the laws of Ireland.
- Clause 18(b) (Choice of Forum and Jurisdiction): the Parties agree that any dispute arising from the Standard Contractual Clauses shall be resolved by the courts of Ireland.
- Exhibit A (Section 3) to this Addendum will apply to Annex 1.
- Exhibit A (Section 4) to this Addendum will apply to Annex 2.

(iii) Ex-UK Transfers. In addition to the Standard Contractual Clauses, as completed pursuant to Section 5.3(ii), Personal Data transfers from the United Kingdom to a country or recipient described in Section 5.3(i) shall be governed by the UK Addendum, completed as follows:

- For the purposes of Table 1 of the UK Addendum, the parties' details and contact information are set forth in Sections 1 and 2 of Exhibit A to this Addendum, and the start date shall be deemed the same date as the Standard Contractual Clauses.
- For the purposes of Table 2 of the UK Addendum, the version of the Standard Contractual Clauses to which the UK Addendum applies is Module Two (Transfer Controller to Processor), and Section 5.3(ii) describes the selection of applicable optional provisions.
- For the purposes of Table 3 of the UK Addendum, the list of parties and description of the transfer are as set out Sections 1 through 3 of Exhibit A of this Addendum, Spiff's technical and organisational measures are set forth in Section 4 of Exhibit A, and the list of Spiff's sub-processors shall be provided pursuant to Section 1.5 of this Addendum.
- For the purposes of Table 4 of the UK Addendum, neither party will be entitled to terminate the UK Addendum in accordance with clause 19 of Part 2: Mandatory Clauses thereof.

(iv) Ex-Switzerland Transfers. In addition to the Standard Contractual Clauses, as completed pursuant to Section 5.3(ii), Personal Data transfers from Switzerland to a country or recipient described in Section 5.3(i) shall be governed by the Standard Contractual Clauses, modified as follows:

- The parties adopt the GDPR standard for all data transfers.
- For competent supervisory authority under Clause 13, the parties choose the supervisory authority identified in Section 3 of Appendix A insofar as the data transfer is governed by the GDPR and the Federal Data Protection and Information Commissioner insofar as the data transfer is governed by the FADP.
- The term "member state" in the Standard Contractual Clauses shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18 c.
- The Standard Contractual Clauses also protect the data of legal entities to the extent set forth in the FADP until the entry of the force of the revised FADP on 1 January 2023.

5.3. **Conflict**. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

6. **Liability.** Each Party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the "**Limitation of Liability**" section of the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party and all of its Affiliates under the Agreement and this Addendum taken together.

7. **Definitions.** Capitalized terms used but not defined in this Addendum have the meanings given in the Agreement. Additionally, the following definitions apply to this Addendum:

7.1. "**Authorized Personnel**" means Spiff's employees, subcontractors, or independent contractors who have a need to know or otherwise access Personal Data to enable Spiff to perform its obligations under the Agreement.

7.2. "**Data Controller**" means the natural or legal person, public authority, agency, or any other body which alone or jointly with

others determines the purposes and means of the Processing of Personal Data. To the extent Processing hereunder is subject to the CCPA / CPRA, "Data Controller" shall have equivalent meaning to the term "business" as defined in the CCPA / CPRA.

7.3. "**Data Processor**" means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of the Data Controller. To the extent Processing hereunder is subject to the CCPA / CPRA, "Data Processor" shall have equivalent meaning to the term "service provider" as defined in the CCPA / CPRA.

7.4. "**Data Protection Laws**" means, as in effect from time to time, the laws and regulations, including laws and regulations of the United States, European Union, the European Economic Area and their member states, Switzerland, and the United Kingdom, applicable to the Processing of Personal Data under the Agreement. With respect to Processing within its respective scope, Data Protection Laws include specifically Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "**GDPR**"); with respect to the United Kingdom, the GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and the United Kingdom Data Protection Act 2018; with respect to Switzerland, the Federal Act on Data Protection of 19 June 1992, as revised effective 1 January 2023 (the "**FADP**"); and with respect to California, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (together, the "**CCPA / CPRA**").

7.5. "**Data Subject**" means the identified or identifiable natural person to whom Personal Data relates. To the extent Processing hereunder is subject to the CCPA / CPRA, "Data Subject" shall have equivalent meaning to the term "consumer" as defined in the CCPA / CPRA.

7.6. "**Governmental Authority**" means any federal, state, local or foreign government or political subdivision thereof, or any agency or instrumentality of such government or political subdivision, or any quasi-governmental authority (to the extent that the rules, regulations or orders of such organization or authority have the force of law), or any arbitrator, court or tribunal of competent jurisdiction, in each case, to the extent such Governmental Authority has jurisdiction and authority over the applicable person, entity or subject matter.

7.7. "**Process**" or "**Processing**" means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, compilation, use, disclosure, duplication, organization, storage, alteration, transmission, combination, redaction, erasure, or destruction.

7.8. "**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

7.9. "**Standard Contractual Clauses**" means the standard contractual clauses as set forth in the Annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021D0914&qid=1623192961660), completed as described in this Addendum. Upon effectiveness (as determined by the European Commission) of any amendments or replacements, the 2021 Standard Contractual Clauses shall be deemed to include such amendments and/or replacements to the extent applicable to the activities described in this Addendum.

7.10. "**Sub-processor**" means any further Data Processor engaged by Spiff in its capacity as Data Processor under this Addendum. To the extent Processing hereunder is subject to the CCPA / CPRA, "Sub-processor" shall refer to any service provider (as defined in the CCPA / CPRA) engaged by Spiff to assist in providing the Products and Services to Customer.

7.11. "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, template version B1.0, issued by the UK's Information Commissioner's Office and laid before Parliament under Section 119A(1) of the Data Protection Act 2018 on 2 February 2022, and entering into force on 21 March 2022.

Exhibit A

Processing Information

1. Data Exporter Information

Name of Data Exporter: **Customer***

Role: Controller

*The identity and associated contact information for Customer is as specified in the applicable Agreement.

The data exporter is a customer of the data importer. The data exporter is sending data to Spiff, and Spiff will use that data to track all information related to commission calculations for the customer.

2. Data Importer Information

Name of Data Importer: **Spiff, Inc.**

Address: c/o Salesforce, Inc., 415 Mission St. 3rd Floor
San Francisco, CA 94105

e-mail: legal.notifications@spiff.com

Data Importer's Representative in the EU:
Osano International Compliance Service Limited
ATTN: 2SGH
3 Dublin Landings
North Wall Quay
Dublin 1
D01C4E0

Data Importer's Representative in the UK:
Osano UK Compliance LTD
ATTN: 2SGH
42-46 Fountain Street
Belfast
Antrim
Northern Ireland
BT1 - 5EF

Role: Processor

The data importer is a service provider to the data exporter. Spiff imports data primarily via authorized API calls to "connected" systems such as Salesforce, data sent in via web hooks, and manually uploaded data via Spiff's Excel-based import/export tool. Business Users at Customer can configure the logical rules of their commission plans via Spiff's online UX leveraging the imported data and logical rules to drive commission calculations. Spiff uses and tracks all information related to commission calculations for individuals. We generally track connected systems information and some additional Spiff-specific calculations. We use these calculations to derive commission calculations for each User each commission period.

3. Details of Processing

Categories of data subjects whose personal data is transferred:

Individuals compensated by the data exporter (in whole or in part) on a commission basis, typically employees and contractors of the data exporter, and the data exporter's authorized Users of the data importer's products and services.

Categories of personal data transferred:

Identifiers: Names, title, and contact information for Users
Professional-related information such as: Commission calculations, quotas, performance metrics and trends, and CRM deal and User information

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:

N/A

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

Continuous

Nature of the processing:

Spiff takes imported data and runs it through a set of rule-based manipulations to arrive at commission calculations for all of Customer's commissioned employees. Customer will help to set up and define those rules and may at times change them. Spiff software will make this process relatively straightforward so that even Customer business Users will be able to make changes to the commission calculations over time.

Purpose(s) of the data transfer and further processing

Spiff is transferring the data to enable processing activities required to provide its products and services to the data exporter. Such processing may need to occur in jurisdictions outside of the EEA.

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

The personal data will be retained for so long as the data importer provides to the data exporter products or services requiring processing of the personal data. Personal data may be retained beyond such period only to the extent the data importer determines it is necessary to do so to comply with applicable legal obligations.

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

Transfers to sub-processors shall be made only to the extent the sub-processors provide services to the data importer that require processing of personal data. The subject matter, nature, and duration of the processing will all be as required for the applicable sub-processor to provide its services to the data importer.

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

- 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.
- 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 the competent supervisory authority.
- 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: Data Protection Commission (DPC) Ireland shall act as the competent supervisory authority.
- Where the data exporter is established in the United Kingdom or falls within the territorial scope of application of UK Data

Protection Laws and Regulations, the Information Commissioner's Office shall act as the competent supervisory authority.

- Where the data exporter is established in Switzerland or falls within the territorial scope of application of Swiss Data Protection Laws and Regulations, the Swiss Federal Data Protection and Information Commissioner shall act as competent supervisory authority insofar as the relevant data transfer is governed by Swiss Data Protection Laws and Regulations.

4. Data Importer's Technical and Organisational Measures

Spiff will maintain commercially reasonable appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Products and Services. Spiff will not materially decrease the overall security of the Products and Services during a subscription term.

Sub-processors

Subprocessor	Country	Service
Atlassian Corporation Plc	USA	Project management
Clari, Inc.	USA	Revenue operations
Datadog, Inc.	USA	Monitoring
Dovetail Research Pty. Ltd.	USA	Customer research
Dropbox, Inc.	USA	Comp plan approvals (signatures)
Fivetran Inc.	USA	Customer application interaction
Flatfile, Inc.	USA	Data importing
Fullstory, Inc.	USA	Customer experience analytics
Goldcast Inc.	USA	Communication
Gong.io Inc	USA	Communication
Google, LLC	USA	Cloud-based computing, data hosting services, customer support tickets, Looker BI reporting, AI functionality
Honeybadger Industries LLC	USA	Error monitoring
Khoros, LLC	USA	Customer engagement
Loom, Inc.	USA	Communication
Mango Technologies, Inc. (ClickUp)	USA	Project management
Microsoft Corporation	USA	Document sharing
Pendo.io, Inc.	USA	Product analytics
Qualtrics, LLC	USA	Client relationship management, data importing
Salesforce, Inc.	USA	Customer support tickets
SendGrid, Inc.	USA	Email delivery
Slack Technologies, Inc.	USA	Communication
Vitally, Inc.	USA	Client relationship management
Workato, Inc.	USA	Data connectivity
WorkRamp, Inc.	USA	Learning management
Zoom Video Communications, Inc.	USA	Communication