Ironclad, Inc.
71 Stevenson St. #600
San Francisco, CA 94105

This “**Order Form**” and “**Enterprise Services Agreement**” is entered into as of the Effective Date by and between Ironclad and Customer. The Order Form is subject to and incorporates by reference the Enterprise Services Agreement attached hereto. The Parties have caused this Order Form to be signed as of the Effective Date by their duly authorized representatives.

LLC (d/b/a Mailchimp)
Ironclad, Inc.

Customer: The Rocket Science Group

Signature: Signature:

Jason Boehmig

Name: Name: Koleen Henson

CEO

Senior Corporate Counsel

Title: Title:

07 / 29 / 2021

Date: Date:

07 / 29 / 2021

ENTERPRISE SERVICES AGREEMENT

1. DEFINITIONS

1.1 “**Affiliate**” means a legal entity that controls, is controlled by, or is under common control with a party, where “control” is defined as owning more than 50% of the voting shares of such entity.

1.2 “**Agreement**” means this Enterprise Services Agreement and each Order Form(s).

1.3 “**Authorized User**” means an employee or contractor of Customer or its Affiliates that Customer has registered to access and use the Enterprise Services.

1.4 “**Confidential Information**” means any business or technical information disclosed by one party to the other party, including Customer Data provided that it is identified as confidential at the time of disclosure or under the circumstances, a person exercising reasonable businessjudgment would understand to be confidential or proprietary.

1.5 “**Customer Data**” means the data and information input or uploaded into the Enterprise Services by Customer or Authorized Users.

1.6 “**Enterprise Services**” means the cloudbased web platform delivered and accessible through the Site that provides contract management and workflowrelated services (the “**Digital Contracting Services**”), and/or the cloudbased web platform delivered and accessible through Ironclad’s website located at: https://app.pactsafe.com that provides contract acceptance, clickwrap, and legal termmanagementrelated services (the "**Acceptance Services**"), and the services performed by Ironclad to configure and rollout the Enterprise Services to Customer and Authorized Users, as described in an applicable Order Form.

1.7 "**Order Form**" means the document that Customer uses to order the Enterprise Services that is signed by both Customer and Ironclad.

1.8 "**Intellectual Property Rights**" means patent rights(including, without limitation, patent applications and disclosures), copyrights, trade secrets, moral rights, knowhow, and any other intellectual property rightsrecognized in any country or jurisdiction.

1.9 "**Site**" means Ironclad's website located at: https://www.ironcladapp.com.

2. ENTERPRISE SERVICES

2.1 **Enterprise Services.** Customer and its Authorized Users may access and use the Enterprise Services solely for Customer's internal business purposes in accordance with the Agreement.

2.2 **Cooperation and Assistance**. Customer will cooperate with Ironclad in good faith and provide to Ironclad the information and personnel that Ironclad reasonably requests and requires to provide the Enterprise Services. Customer, at its option, may utilize certain thirdparty software and services with the Enterprise Services and is responsible for acquiring and maintaining all such thirdparty software and services required to access, use, or integrate with the Enterprise Services, including all costs related to the foregoing.

2.3 **Authorized Users**. Customer will keep its user IDs and password for the Enterprise Services confidential and will be responsible for all actions taken under an Authorized User's account, except, for the avoidance of doubt, those taken by Ironclad which are not at the direction of Customer. Customer will comply with all applicable laws, rules and regulations in connection with its use of the Enterprise Services. Customer will promptly notify Ironclad of any suspected violation of this Agreement by an Authorized User and will cooperate with Ironclad to address the suspected violation. Ironclad may suspend or terminate any Authorized User's access to the Enterprise Services upon notice to Customer in the event that Ironclad reasonably determines that such Authorized User violated this Agreement.

2.4 **Restrictions.** Customer will not allow anyone other than Authorized Users to access or use the Enterprise Services from Customer's accounts. Customer will not and will ensure that its Authorized Users do not: (i) attempt to interfere with or disrupt the Enterprise Services (or any related systems or networks) or use the Enterprise Services other than directly for Customer's benefit; (ii) copy, modify or distribute any portion of the Enterprise Services; (iii) rent, lease, or resell the Enterprise Services; or (iv) transfer any of its rights hereunder. In addition, Customer will not reverse engineer or access the Enterprise Services in order to build a competitive product or service.

2.5 **Customer Data.** Customer is responsible for obtaining any necessary right and licenses for use of the Customer Data by Customer and Ironclad as contemplated in this Agreement. Customer agreesthat it hasthe legal right and authority to access, use and disclose to Ironclad any Customer Data. Customer authorizes Ironclad to access, process, and use the Customer Data as necessary to perform and fulfill its obligations hereunder. The Enterprise Services includes functionality that permits Customer to download certain Customer Data as an archive file consisting of individual files in an industry standard data file format. In the unlikely scenario that any Customer Data is lost or corrupted, Ironclad will use commercially reasonable efforts to restore such Customer Data. Customer acknowledges that, while Ironclad maintains a copy of Customer Data for the provision and performance of the Enterprise Services, the files and documents that Customer uploads to the Enterprise Services are stored in Customer's chosen thirdparty cloud storage provider. AS SUCH, IRONCLAD'S EFFORTS TO RESTORE LOST OR CORRUPTED CUSTOMER DATA PURSUANT TO THIS SECTION SHALL CONSTITUTE IRONCLAD'S SOLE AND EXCLUSIVE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY IN THE EVENT OF ANY LOSS OR CORRUPTION OF CUSTOMER DATA. Customer will use commercially reasonable efforts to maintain backup copies of its thencurrent Customer Data. Ironclad will process and maintain Customer Data consistent with the Data Processing Addendum, which is attached at Exhibit B and hereby incorporated by reference.

2.6 **Information Security**. Ironclad will use commercially reasonable technical and organizational measures designed to prevent unauthorized access, use, alteration or disclosure of the Enterprise Services or Customer Data. Ironclad, however, will have no responsibility for errors in transmission, unauthorized thirdparty access (unless resulting, directly or indirectly, from Ironclad's failure to satisfy its obligations under this **Section 2.6**) or other causes beyond

Ironclad's control.

2.7 **Usage Data.** Ironclad may collect and analyze data and other information relating to the provision, use and performance of the Enterprise Services and related systems and technologies therefrom ("**Usage Data**") in order to improve and enhance the Enterprise Services. Insights drawn from Usage Data may be disclosed to Customer and other users of the Enterprise Services in connection with their respective use of the Enterprise Services. For clarification, if Ironclad discloses insights drawn from Usage Data, then all Usage Data in such disclosures will be anonymized and aggregated, will not identify Customer or a Customer's users, and will not be disclosed in a manner that would permit a third party to determine Customer's or Customer's users' identity.

2.8 **Electronic Signatures.** Customer acknowledges and agrees that: (i) as between Ironclad and Customer, Customer has exclusive control and responsibility for the content, quality, and format of any documents used with the Enterprise Services; (ii) certain types of documents, agreements, or contracts may be excluded from general electronic signature laws (such as wills, trusts, court orders, or family law matters), or may have specific regulations that are applicable to them; and, (iii) Customer is solely responsible for ensuring that the documents, agreements or contracts it uses with the Enterprise Services are appropriate for electronic signatures, and Ironclad is not responsible or liable for any such determination or use; (iv) Consumer protection laws or regulations may impose specific requirements for electronic transactions involving consumers, Customer is solely responsible for ensuring it complies with all such laws/regulations, and Ironclad has no obligationsto make such determination or assist with fulfilling any requirements therein; (v) Ironclad is not responsible for determining how long any contracts, documents, or other records are required to be retained orstored under any applicable laws; and (vi) Ironclad is notresponsible for or liable to produce any of Customer's contracts or other documents to any third parties. If Customer is using an API or other service that allows Customer to perform any end user/participant/signer authentication, then Customer is solely responsible and liable for such authentication.

3. FEES; EXPENSES; TAXES

3.1 **Fees**. Customer will pay to Ironclad the Fees in accordance with the terms set forth in the applicable Order Form(s) and this **Section 3**.

3.2 **Invoices; Payment**. Unless otherwise set forth in an Order Form, Ironclad will invoice Customer annually in advance for the Enterprise Services and each invoice will be due and payable within thirty (30) days of receipt by Customer. All payment obligations are noncancellable, and other than as provided in the Agreement, all amounts paid are non refundable. Ironclad will be entitled, in itssole discretion, to withhold performance and discontinue Customer's access to the Enterprise Services until all undisputed amounts past due are paid in full.

3.3 **Taxes**. All Fees and other amounts stated or referred to in this Agreement are exclusive of all taxes, duties, levies, tariffs, and other governmental charges (collectively, "**Taxes**"). Customer will be responsible for payment of all Taxes and any related interest and/or penalties resulting from any payments made hereunder, other than any taxes based on Ironclad's net income.

4. PROPRIETARY RIGHTS.

4.1 Customer owns and retains: (i) the Customer Data and (ii) Customer's name, logo and other trademarks, and (iii) all Intellectual Property Rights in and to any of the foregoing.

4.2 Ironclad owns and retains: (i) the Enterprise Services, and all improvements, enhancements or modifications made by any party; (ii) the Usage Data; (iii) any software, applications, inventions or other technology developed by Ironclad in connection with providing the Enterprise Services; (iv) Ironclad's name, logo, and other trademarks; and (v) all Intellectual Property Rights in and to any of the foregoing.

5. CONFIDENTIALITY

5.1 **Use and Nondisclosure**. A receiving party will not use the disclosing party's Confidential Information except as necessary under this Agreement and will not disclose Confidential Information to any third party except: (a) to those of its employees and subcontractors who have a business need to know such Confidential Information; provided that each such employee and subcontractor is bound to confidentiality restrictions consistent with the terms set forth in this Agreement or (b) as further described in the Data Processing Addendum. Each receiving party will protect the disclosing party's Confidential Information from unauthorized use and disclosure using efforts equivalent to the efforts that the receiving party uses with respect to its own confidential information and in no event less than a reasonable standard of care. The provisions of this **Section 5.1** will remain in effect during the Term and for a period of three (3) years after the expiration or termination thereof, except with regard to trade secrets of the disclosing party, which will be held in confidence for as long as such information remains a trade secret.

5.2 **Exclusions**. The obligations and restrictions set forth in **Section 5.1** will not apply to any information that: (i) is or becomes generally known to the public through no fault of or breach of this Agreement by the receiving party; (ii) is rightfully known by the receiving party at the time of disclosure; (iii) isindependently developed by the receiving party without access to the disclosing party's Confidential Information; or (iv) the receiving party rightfully obtains from a third party who has the right to disclose such information without breach of any confidentiality obligation to the disclosing party.

5.3 **Permitted Disclosures.** The provisions of this **Section 5** will not restrict either party from disclosing the other party's Confidential Information: (i) pursuant to the order or requirement of a court, administrative agency, or other governmental body; provided that to the extent legally permitted, the party required to make such a disclosure gives reasonable notice to the other party to enable it to contest such order or requirement or limit the scope of such request; (ii) on a confidential basis to its legal or professional financial advisors; (iii) as required under applicable securities regulations.

5.4 **Injunctive Relief**. The receiving party acknowledges that disclosure of Confidential Information could cause substantial harm for which damages alone may not be a sufficient remedy, and therefore that upon any such disclosure by the receiving party, the disclosing party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law.

6. WARRANTY

6.1 **Warranty for Enterprise Services**. Ironclad warrants solely to Customer that the Enterprise Services will materially conform to the description set forth in this Agreement under normal use and circumstances when used consistently with the terms of this Agreement. As Ironclad's sole and exclusive liability and Customer's sole and exclusive remedy for any breach of the warranty set forth in this **Section 6.1** Ironclad will use commercially reasonable efforts to modify the Enterprise Services to correct the nonconformity; provided, however, that if such nonconformity is not cured within fifteen (15) business days of Ironclad'sreceipt of notice of such nonconformity from Customer, Customer may elect to terminate the Agreement. Such termination shall be subject to **Section 7.3**.

6.2 **Disclaimer**. EXCEPT AS EXPRESSLY PROVIDED IN SECTION 6.1, IRONCLAD MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED, IN CONNECTION WITH THIS AGREEMENT OR THE ENTERPRISE SERVICES AND IRONCLAD HEREBY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY, ACCURACY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE OF TRADE. IRONCLAD DISCLAIMS ANY WARRANTY THAT THE ENTERPRISE SERVICES WILL BE ERROR FREE OR UNINTERRUPTED OR THAT ALL ERRORS WILL BE CORRECTED. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED FROM IRONCLAD OR ELSEWHERE SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT. Customer assumes sole responsibility and liability for results obtained from the use of the Enterprise Services and for conclusions drawn from such use. Ironclad will have no liability for any claims, losses, or damages caused by errors or omissions in any Customer Data or other information provided to Ironclad by Customer in connection with the Enterprise Services or any actions taken by Ironclad at Customer's direction. Ironclad will have no liability for any claims, losses or damages arising out of or in connection with Customer's or any Authorized User's use of any thirdparty products,services, software or web sites that are accessed via links from within the Enterprise Services.

7. TERM AND TERMINATION

7.1 **Term.** This Agreement will commence on the Effective Date and continue for the period specified in the Order Form (the "Term"), unless terminated earlier as provided in this Agreement. Thereafter, the Agreement shall automatically renew for subsequent oneyear periods (the "Renewal Term"), unless either party notifies the other in writing of its intent not to renew at least sixty (60) days prior to the end of the thencurrent term. If a party provides timely notice of its intent not to renew the Agreement, the Agreement shall expire at the end of the thencurrent Term. Unless otherwise set forth in an Order Form, Ironclad may modify the applicable fees upon prior written notice to Customer, provided that the modified fees will not apply until the next Renewal Term.

7.2 **Termination for Cause.** Either party may terminate this Agreement upon written notice if the other party breaches any material terms of this Agreement and fails to correct the breach within thirty (30) days following written notice from the nonbreaching specifying the breach.

7.3 **Rights and Obligations Upon Expiration or Termination**. Upon expiration or termination of this Agreement, Customer's and Authorized Users' right to access and use the Enterprise Services will immediately terminate and each will immediately cease all use of the Enterprise Services, and in the event of termination by Customer under **Section 6.1** or **7.2**, Ironclad shall refund to Customer a prorata portion of the Fees paid for the remaining portion of the Term after the date of termination. Upon expiration or termination of this Agreement, Ironclad will deliver a thencurrent export of the Customer Data to Customer.

7.4 **Survival.** The rights and obligations of Ironclad and Customer contained in **Sections 2.7** (Usage Data), **3** (Fees; Expenses; Taxes), **4** (Proprietary Rights), **5** (Confidentiality), **7.3** (Rights and Obligations Upon Expiration or Termination), **7.4** (Survival), **8** (Indemnification), **9** (Limitation of Liability), and **10** (General) will survive any expiration or termination of this Agreement.

8. INDEMNIFICATION

8.1 **Indemnification by Ironclad.** Ironclad will defend Customer, its Affiliates, and each of their respective officers, directors, employees, agents and representatives ("**Customer Indemnitees**"), from and against any suit or action brought by a thirdparty against Customer: (a) alleging that the Enterprise Services, as provided by Ironclad and when used by Customer pursuant to this Agreement, infringes any Intellectual Property Right of a third party (the "**IP Indemnity**"); or (b) resulting from unauthorized disclosure and misuse of Customer Data directly resulting from Ironclad's breach of its obligations under Section 2.5 (Customer Data) (the "**Data Indemnity**"). Ironclad shall indemnify and hold harmless Customer Indemnitees from and against any damages, costs, liabilities, fines, penalties and expenses (including reasonable attorneys' fees) arising out of or resulting from such claim, provided that: (i) Customer provides Ironclad with prompt written notice of such claim; (ii) Customer provides reasonable cooperation to Ironclad, at Ironclad's expense, in the defense and settlement of such claim; and (iii) Ironclad has sole authority to defend or settle such claim, provided that it may not settle any claim in a manner that imposes any liability upon Customer without Customer's prior written consent.

8.2 **Injunctions**. If Customer's use of the Enterprise Services is, or in Ironclad's opinion is likely to be, enjoined due to the type of claim specified in **Section 8.1(a)**, then Ironclad may at its sole option and expense: (i) replace or modify the Enterprise Services to make them noninfringing and of equivalent functionality; (ii) procure for Customer the right to continue using the Enterprise Services under the terms of this Agreement; or (iii) if Ironclad is unable to accomplish either (i) or (ii) despite using its commercially reasonable efforts, terminate Customer'srights and Ironclad's obligation under this Agreement with respect to such Enterprise Services and refund to Customer a prorata portion of the Fees paid for the remaining portion of the Term during which Customer would have had access to the Enterprise Services.

8.3 **Exclusions**. Notwithstanding the terms of **Section 8.1**, Ironclad will have no liability for any infringement or misappropriation claim of any kind to the extent that it results from: (i) the combination, operation or use of the Enterprise Services with equipment, devices, software or data (including without limitation Customer Data) not supplied by Ironclad, if a claim would not have occurred but for such combination, operation or use; or (ii) Customer's or an Authorized User's use of the Enterprise Services other than in accordance with this Agreement.

8.4 **Sole Remedy**. THE FOREGOING STATES IRONCLAD'S AND ITS LICENSORS' SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY ALLEGED OR ACTUAL INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS BY THE ENTERPRISE SERVICES.

8.5 **Indemnification by Customer**. Customer will defend Ironclad, its Affiliates, and each of their respective officers, directors, employees, agents and representatives ("**Ironclad Indemnitees**") from and against any action or suit brought against Ironclad by a third party based on a claim that the Customer Data infringes any Intellectual Property Rights of a third party. Customer will indemnify and hold harmless Ironclad Indemnitees from and against any damages, costs, liabilities, fines, penalties and expenses (including reasonable attorneys' fees) arising out of or resulting from such claim, provided that (i) Ironclad provides Customer with prompt written notice of such claim; (ii) Ironclad provides reasonable cooperation to Customer, at Customer's expense, in the defense and settlement of such claim; and (iii) Customer has sole authority to defend or settle such claim, provided that it may not settle any claim in a manner that imposes any liability upon Ironclad without Ironclad's prior written consent.

9. LIMITATION OF LIABILITY.

9.1 Exclusion of Damages. To the fullest extent permitted by law, except for Excluded Claims (as defined below in Section 9.3 and for which there will be no cap on liability), neither Customer (and its Affiliates) nor Ironclad, and its Affiliates and suppliers, will be liable under this Agreement for (i) indirect, special, incidental, consequential, exemplary, or punitive damages; or (ii) loss of use, data, business, revenues, or profits (in each case whether

direct or indirect), even if the party knew or should have known that such damages were possible and even if a remedy fails of its essential purpose.

9.2 **Total Liability. To the fullest extent permitted by law, except for Excluded Claims (for which there shall be no cap on liability) or Special Claims (which are subject to the Enhanced Liability Cap set forth in Section 9.4), neither party's aggregate liability under this Agreement will exceed the greater of $100,000 or the amount paid by Customer to Ironclad during the twelve months prior to the event giving rise to liability.**

9.3 **Excluded Claims.** "**Excluded Claims**" means: (i) any intentional misconduct or gross negligence by either party; (ii) any amounts payable to third parties pursuant to Ironclad's IP Indemnity obligations under Section 8.1(a); or (iii) any amounts payable to third parties pursuant to Customer's indemnification obligations under Section 8.5 (Indemnification by Customer).

9.4 **Special Claims**. "**Special Claims**" means(i) any breach by Ironclad of Section 2.5 (Customer Data) or 5 (Confidentiality) resulting in unauthorized disclosure and misuse of Customer Data or Confidential Information; (ii) any amounts payable to third parties pursuant to Ironclad's Data Indemnity obligations under Section 8.1(b); or (iii) Ironclad's liability arising under or in connection with the DPA . For any and all Special Claims, Ironclad's aggregate liability shall be subject to an enhanced liability cap not to exceed the greater of either (i) three times (3x) **the amount paid by Customer to Ironclad during the twelve months prior to the event giving rise to liability** or (ii) $2,500,000 (the "**Enhanced Liability Cap**").

10. GENERAL

10.1 **Governing Law.** This Agreement will be governed by the laws of the State of California, without regard to its conflict of law provisions. Any legal action or proceeding relating to this Agreement will be brought exclusively in the state or federal courts located in San Francisco, CA. Ironclad and Customer hereby agree to submit to the jurisdiction of, and agree that venue is proper in, those courts in any such legal action or proceeding.

10.2 **Order of Preference**. In the event of a conflict between the Enterprise Services Agreement and Order Form, the order of preference will be the Enterprise Services Agreement, then the Order Form, unless the Special Contractual Terms section of the Order Form clearly specifies the section of the Enterprise Services Agreement to be modified.

10.3 **Waiver**. The waiver by either party of any default or breach of this Agreement will not constitute a waiver of any other or subsequent default or breach. No waiver of any provision of this Agreement will be effective unless it is in writing and signed by the party granting the waiver.

10.4 **Notices**. Notices will be sent to the addresses set forth in the Order Form. The notices will be deemed to have been given upon: (i) the date actually delivered in person; (ii) the day after the date sent by overnight courier; (iii) three (3) days following the date such notice was mailed by first class mail; or (iv) the same day sent by email to legal@ironcladapp.com.

10.5 **Severability**. In the event any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions of this Agreement will remain in full force and effect.

10.6 **Force Majeure**. Neither party will be liable hereunder by reason of any failure or delay in the performance of its obligations hereunder (except for the payment of money owed) on account of events beyond the reasonable control of such party, which may include without limitation denialofservice attacks, strikes, shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes and material shortages, internet connectivity.

10.7 **Relationship Between the Parties**. Nothing in this Agreement will be construed to create a partnership, joint venture or agency relationship between the parties.

10.8 **Assignment**. Neither party may assign its rights or obligations under this Agreement without the other party's prior written consent. Notwithstanding the foregoing, either party may assign its rights and obligations under this Agreement to an Affiliate as part of a reorganization, or to a purchaser of its business entity or substantially all of its assets or business to which rights and obligations pertain without the other party's consent, provided that: (a) the purchaser is not insolvent or otherwise unable to pay its debts as they become due; (b) the purchaser is not a competitor of the other party; and (c) any assignee is bound hereby. Other than the foregoing, any attempt by either party to transfer its rights or obligations under this Agreement will be void.

10.9 **Entire Agreement**. This Agreement (including any Exhibits hereto) constitutes the complete and exclusive agreement between the parties concerning its subject matter and supersedes all prior or contemporaneous agreements or understandings, written or oral, concerning the subject matter of this Agreement. This Agreement may not be modified or amended except in a writing signed by a duly authorized representative of each party.

10.10 **No ThirdParty Beneficiaries.** This Agreement is intended for the sole and exclusive benefit of the signatories and is not intended to benefit any third party. Only the parties to this Agreement may enforce it.

Doc ID: 03b94585cf04063478fb323c4a1700f0636ce22b

IRONCLAD SERVICE LEVEL AGREEMENT &
TECHNICAL SUPPORT SCHEDULE

Exhibit A

This Ironclad Service Level Agreement (“SLA”) & Technical Support Schedule (“TSS”) shall be governed by and incorporated by reference into the Enterprise Services Agreement and the Applicable Order Form (“Agreement”) entered into between the parties. All capitalized terms contained but not defined herein shall have the meaning ascribed to them in the Agreement.

A. Digital Contracting Services Service Level Agreement. This Section A shall apply solely to Digital Contracting Services. 1.

Defined Terms.

a. “Emergency Maintenance” means maintenance performed to fix critical functionality, vulnerabilities, or material defects that may substantially impair the usability or performance of the Services.

b. “Excused Maintenance” means Emergency Maintenance and Scheduled Maintenance.

c. “Request” means a request issued by an Authorized User to access the Enterprise Services which is received by the Enterprise Services.

d. “Scheduled Availability Time” means twentyfour (24) hours a day, seven (7) days a week, excluding: (i) Excused Maintenance, (ii) any downtime due to defects caused by Customer, one of its vendors, third party connections, utilities, or equipment, or caused by other forces beyond the reasonable control of Ironclad (such as denial of Enterprise Services attacks, internet or thirdparty Enterprise Services outages or outages with respect to Customer’s network or internet access).

e. “Scheduled Maintenance” is any system maintenance performed during the Maintenance Window. The

Maintenance Window is available at https://status.ironcladapp.com/.

f. "Service Credits" are credits for which Customer may be eligible if Ironclad fails to meet the Target Uptime. Service Credits are provided in the form of a number of credited days of Enterprise Services, for the period of time covered by the invoice to which the Service Credit is applied. The availability of the Enterprise Services per calendar month and corresponding Service Credits are set forth in the table below.

Availability Per Calendar Month	**Service Credit**
< 99.7% >= 99.0%	.5% of the Annual Subscription Fee
< 99.0% >= 95.0%	1% of the Annual Subscription Fee
< 95.0%	1.5% of the Annual Subscription Fee

g. "Service Credit Request" means a request to Ironclad at support@ironcladapp.com stating that Customer believes that Ironclad has failed to meet the SLA.

2. Target Uptime. During the Term of the Agreement, Ironclad will use all commercially reasonable efforts to make the Enterprise Services available and operational to Customer for 99.7% of the Scheduled Availability Time (the "Target Uptime"). If Ironclad does not meet the Target Uptime, and if Customer meets its obligations below, Customer will be eligible to receive the applicable Service Credits.

3. Service Credits. To receive a Service Credit, Customer must: (i) issue a Service Credit Request within 7 days of the day in which Customer believes Ironclad's failure to meet the Target Uptime occurred; and (ii) not be past due on any payments owed to Ironclad when it issues a Service Credit Request. Promptly after receipt a Service Credit Request, Ironclad will investigate the request and notify Customer that either: (i) no Service Credit is due and state the basis of this determination; or (ii) a Service Credit is due. If Ironclad determines a Service Credit is due, then Ironclad will apply the applicable Service Credits to Customer's account for future fees due. Service Credits have no cash value and are Customer's sole and exclusive remedy for any failure by Ironclad to meet the Target Uptime.

B. Acceptance Services Service Level Agreement. This Section B shall apply solely to Acceptance Services. 1. Defined

Terms.

a. "Activity API" means the portions of the Acceptance Services that programmatically display contracts inside of a web page or mobile app, retrieve acceptance data for individual users, and send acceptance of contracts.

b. "Emergency Maintenance" means maintenance performed to fix critical functionality, vulnerabilities, or material defects that may substantially impair the usability or performance of the Acceptance Services.

c. "Excused Maintenance" means Emergency Maintenance and Scheduled Maintenance.

d. "REST API" means the portions of the Acceptance Services that are accessed programmatically for integrations into third party applications.

e. “Scheduled Availability Time” means twentyfour (24) hours a day, seven (7) days a week, excluding: (i) Excused Maintenance, (ii) any downtime due to defects caused by Customer, one of its vendors, third party connections, utilities, or equipment, or caused by other forces beyond the reasonable control of Ironclad (such as denial of service attacks, internet or thirdparty service outages or outages with respect to Customer’s network or internet access).

f. “Scheduled Maintenance” is any system maintenance performed during a Maintenance Window. The Maintenance Window, if one isscheduled, will be available at https://status.pactsafe.com/ at least two weeks prior to the Maintenance Window.

g. “Service Credits” are credits for which Customer may be eligible if Ironclad fails to meet the Target Uptime. The availability of the Acceptance Services per calendar month and corresponding Service Credits are set forth in the table below.

Availability Per Calendar Month	**Service Credit**
< 99.5% >= 99.0%	1% of the Annual Subscription Fee
< 99.0% >= 95.0%	2% of the Annual Subscription Fee
< 95.0%	3% of the Annual Subscription Fee

h. “Service Credit Request” means a request to Ironclad at support@ironcladhq.com stating that Customer believes that Ironclad has failed to meet the Target Uptime.

i. “Application User Interface” means the dashboard portion of the Acceptance Services accessed via the Internet through a web browser to create and publish contracts, download electronic records of acceptance, and send contracts.

2. Target Uptime. During the Term of the Agreement, Ironclad will use all commercially reasonable efforts to make the Application User Interface, REST API, and Activity API available and operational to the Customer for 99.5% of the Scheduled Availability Time (the “Target Uptime”), as tracked by each such measure on https://status.pactsafe.com/. If Ironclad does not meet the Target Uptime as to any of the three measures, and if Customer meets its obligations below, Customer will be eligible to receive the applicable Service Credits.

3. Service Credits. To receive a Service Credit, Customer must: (i) issue a Service Credit Request within 7 days of the last day of the month in which Customer believes Ironclad’s failure to meet the Target Uptime occurred; and (ii) not be past due on any payments owed to Ironclad when Customer issues a Service Credit Request. Promptly after receipt of a Service Credit Request, Ironclad will investigate the request and notify Customer that either: (i) a Service Credit is due; or (ii) no Service Credit is due and state the basis of this determination. If Ironclad determines a Service Credit is due, then Ironclad will apply the applicable Service Credits to Customer’s account for future fees due. Service Credits have no cash value and are Customer's sole and exclusive remedy for any failure by Ironclad to meet the Target Uptime.

C. Ironclad Technical Support Schedule.

1. Maintenance. Ironclad will make available to Customer all generally available updates and bug fixes to the Enterprise Services. Ironclad will take commercially reasonable efforts to perform Scheduled Maintenance during offpeak business hours, made available at https://status.ironcladapp.com/ .

2. Support. Ironclad is available to receive Enterprise Services support inquiries via email (support@ironcladapp.com). Ironclad's support hours are 08:00 AM to 8:00 PM Eastern Standard Time Monday through Friday (excluding standard U.S. holidays) for technical information, technical advice and technical consultation regarding Customer's use of the Enterprise Services.

3. Help Center Access. Customer shall have 24x7 access to our online Help Center (https://support.ironcladapp.com) for any best practices, integration instructions, or product questions.

4. Email & Web Form Cases. Customer shall have the ability to submit support requests 24x7 through email (support@ironcladapp.com) or the web form accessible via Ironclad website or Help Center (https://support.ironcladapp.com).

Doc ID: 03b94585cf04063478fb323c4a1700f0636ce22b

DATA PROCESSING ADDENDUM

Exhibit B

This Vendor Data Processing Agreement ("**DPA**") is entered into between The Rocket Science Group LLC d/b/a Mailchimp ("**Mailchimp**") on behalf of itself and its Affiliates and Ironclad, Inc. ("**Vendor**") and shall be effective on the date both parties execute this DPA ("**Effective Date**"). For the purposes of this DPA only, and except where indicated otherwise, the term "Mailchimp" shall include The Rocket Science Group LLC and/or its Affiliates.

Recitals

Vendor has entered into one or more purchase orders, contracts and/or agreements with Mailchimp (the "**Contract(s)**") pursuant to which the Vendor has agreed to provide certain services to Mailchimp as more particularly described in the Contract(s)

(“**Services**”).

In providing the Services, Vendor may Process data, including Personal Data controlled by Mailchimp and/or its customers, contacts or partners.

As part of its privacy notices and its contractual arrangements, Mailchimp has provided certain assurances to its customers, candidates, contacts, employees, and/or partners (as applicable) to ensure the appropriate protection of their data, including Personal Data, when Mailchimp engages thirdparty vendors. Mailchimp’s engagement of Vendor is conditioned upon Vendor’s agreement to the terms and conditions of this DPA.

Agreement

1. Definitions

“**Affiliate**” means any entity that is directly or indirectly controlled by, controlling or under common control with an entity. “Control” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“**Applicable Privacy Laws**” means all worldwide data protection and privacy laws and regulations applicable to the Personal Data in question, including, where applicable: (i) European Privacy Laws; (ii) all Canadian federal and provincial privacy legislation applicable to Mailchimp and Vendor; and (iii) all laws and regulations of the United States, including the California Consumer Privacy Act of 2018 (California Civil Code §§ 1798.100 et seq. (“**CCPA**”)).

“**Authorized Persons**” means any person who Processes Personal Data on Vendor’s behalf, including Vendor’s employees, officers, partners, principals, contractors, and Subcontractors.

“**Covered Data**” means, in any form or format, all Personal Data and other Confidential Information that is Processed by Vendor or its Subcontractors on behalf of Mailchimp in connection with the Contract(s), whether (i) provided by Mailchimp or any of its Affiliates to an Authorized Person, in connection with the Contract(s), (ii) provided to an Authorized Person by any third party or collected from any third party by an Authorized Person, (iii) created by any Authorized Person under the Contract(s) automatically by any software or systems or through any other means, and (iv) any compiled, summarized, and derivative versions of data or information described in (i)(iii).

“**European Privacy Laws**” means(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 (General Data Protection Regulation) (“**GDPR**”); (ii) the EU ePrivacy Directive (Directive 2002/58/EC); (iii) any national data protection laws made under or pursuant to (i) or (ii); (iv) the Swiss Federal Data Protection Act of 19 June 1992 and its Ordinance; and (v) in respect of the United Kingdom, the Data Protection Act 2018 and any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; in each case, as may be amended, superseded or replaced.

“**Europe**” means, for the purposes of this DPA, the European Economic Area and its Member States, the United Kingdom and Switzerland.

“**Model Clauses**” means the standard contractual clauses for Processors as approved by the European Commission and available at https://ec.europa.eu/info/law/lawtopic/dataprotection/datatransfersoutsideeu/modelcontracts transferpersonaldatathirdcountries_en (as amended, superseded or updated from time to time).

“**Personal Data**” means any data that is protected as “personal data”, “personally identifiable information” or “personal information” under Applicable Privacy Laws.

“**Privacy Shield**” means the EUU.S. and SwissUS Privacy Shield selfcertification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to Decision C(2016)4176 of 12 July 2016 and by the Swiss Federal Council on January 11, 2017 respectively.

"**Security Incident**" means any reasonably suspected or confirmed unauthorized or unlawful breach of security leading to, or reasonably believed to have led to, the theft, accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to any Covered Data.

"**Subcontractor**" means any third party (including any Vendor Affiliates) engaged directly or indirectly by Vendor which Processes any Covered Data. The term "Subcontractor" shall also include any third party appointed by a Subcontractor which Processes any Covered Data.

"**Term**" means (i) the term of the Contract(s) and (ii) any period after the termination or expiry of the Contract(s) during which the Vendor Processes Covered Data, until the Vendor has deleted, destroyed or returned such Covered Data in accordance with the terms of the Contract(s), including this DPA.

The terms "**Controller**," "**data subject**", "**personal data**", "**Processor**," "**Processing**" (or "**Process**"), and "**Supervisory Authority**" shall have the meanings given to them in Applicable Privacy Laws or, if not defined therein, the GDPR. For the avoidance of doubt, the term "Processing" (or "Process") includes retaining, using or disclosing Covered Data. The terms "**Business**", "**personal information**", "**commercial purpose**", and "**Service Provider**" shall have the meanings given to them in the CCPA.

2. Role and Scope of Processing

2.1 Vendor shall Process Covered Data under the Contract(s) only as a Processor or Service Provider (as applicable) acting on behalf of Mailchimp (whether as Controller itself or a Processor or Service Provider acting on behalf of thirdparty Controllers or Businesses, such as Mailchimp customers). Vendor agrees that it will Process Covered Data as described at **Annex A**, which forms an integral part of this DPA.

2.2 Vendor shall at all times Process the Covered Data solely for the purposes of providing the Services to Mailchimp under the Contract(s) and in accordance with Mailchimp's documented instructions (the "**Purpose**"). Without limiting the generality of the foregoing, Vendorshall not: (i) Processthe Covered Data for its own purposes or those of any third party, including Processing the Covered Data for its or a third party's own commercial purposes; (ii) sell or disclose the Covered Data to a third party for monetary or other valuable consideration (including "sell" within the meaning of the CCPA or otherwise); or (iii) Process the Covered Data outside the direct business relationship between Mailchimp and Vendor, except to the extent strictly necessary to provide the Services in accordance with this DPA and the Contract(s).

2.3 Vendor represents, warrants and certifies that it understands and will comply with its obligations under this Section 2 and shall immediately notify Mailchimp in writing, unless prohibited from doing so under Applicable Privacy Laws, if: (i) it becomes aware or believes that any data processing instruction from Mailchimp violates Applicable Privacy Laws; and/or (ii) it is unable to comply with the terms of this DPA for any reason. In the event of any such noncompliance and/or if Mailchimp is aware or has reason to believe that Vendor has breached or will breach its obligations under Applicable Privacy Laws and/or this DPA, but without prejudice to any other right or remedy available to Mailchimp:

(a) Vendor shall work with Mailchimp and promptly take all reasonable and appropriate steps to remediate (if remediable) any such noncompliance; and/or

(b) Mailchimp may elect to suspend or terminate the Processing of Covered Data under the Contract(s) and/or terminate the Contract(s) without any further liability or obligation to Vendor, and Vendor shall refund to Mailchimp any amounts which were paid for work not yet performed under the Contract(s).

2.4 Vendor shall not at any time acquire any ownership, license, rights, title or other interest in or to Covered Data, all of which shall, as between Mailchimp and Vendor, be and remain the proprietary and confidential information of Mailchimp.

2.5 Each Party shall comply with its obligations under Applicable Privacy Laws in respect of any Personal Data it Processes under this DPA.

3. SubProcessing

3.1 Vendor shall not subcontract any Processing of the Covered Data to a Subcontractor without the prior written consent of Mailchimp. Notwithstanding the foregoing, Mailchimp consents to Vendor engaging Subcontractors to Process the Covered Data provided that:

(a) Vendor provides at least 30 days prior written notice to Mailchimp of the engagement of any new Subcontractor (including details of the Processing and location) and Vendor shall update the list of all Subcontractors engaged to Process Covered Data under this DPA at **https://ironcladapp.com/subprocessors/.** Solely for Acceptance Services, Ironclad will also use the following additional Third Parties that Process Customer Personal Data:

Third Party	Processing Activity
Amazon Web Services	Cloud service provider for hosting
MongoDB Atlas	Cloud service provider for database hosting and management
Twilio	Inbound/outbound SMS and mobile messaging provider
Twilio SendGrid	Outbound email service provider
MailChimp	Outbound email service provider
FullStory	Cloud-based customer experience and insight service provider
Intercom	Cloud-based customer support and live chat service provider
Planhat	Cloud-based customer success service provider
Zapier	Cloud-based workflow automation service provider

(b) Vendor imposes the same or substantially similar data protection terms on any Subcontractor it engages as contained in this DPA (including the Model Clauses, where applicable);

(c) Vendor only retains Subcontractors that Vendor can reasonably expect to appropriately protect the privacy, confidentiality and security of Covered Data; and

(d) Vendor remains fully liable for any breach of this DPA or the Contract(s) that is caused by an act, error, or omission of such Subcontractor to the same extent as if Vendor had made such act, error, or omission.

3.2 If Mailchimp objects to the engagement of any Subcontractor, then the parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, and failing any such resolution, Mailchimp may terminate the part of the service performed under the Contract that cannot be performed by Vendor without the use of the objectionable Subcontractor.

4. Cooperation and Individual Rights

4.1 Vendorshall, taking into account the nature of the Processing, reasonably cooperate with Mailchimp to enable Mailchimp (or its thirdparty Controller) to respond to any requests, complaints or other communications from data subjects, consumers, governmental and regulatory or judicial bodies relating to the Processing of Covered Data under the Contract(s), including requests from data subjects seeking to exercise their rights under Applicable Privacy Laws. In the event that any such request, complaint or communication is made directly to Vendor, Vendor shall promptly notify Mailchimp in writing at dpo@mailchimp.com (or such contact notified to Vendor) and shall not respond to such communication without Mailchimp’s express authorization.

4.2 If Vendor becomes aware that any government agency or authority (including law enforcement or national security) requests access to Covered Data (whether on a voluntary basis or through a subpoena or court order), Vendor shall: (i) immediately notify Mailchimp by email; (ii) inform the government agency that Vendor is a processor of the data and is not authorized to disclose the data, and that Vendor will need to immediately notify Mailchimp regarding the request; (iii) attempt to redirect the agency to request the data directly from Mailchimp; (iv) reasonably cooperate with all instructions of Mailchimp, including if Mailchimp (or itsthirdparty Controller) wishesto limit, challenge or protect against disclosure; and (v) not provide access to the data unless and until authorized by Mailchimp in writing. Vendor shall not be required to comply with the obligations under Section 4.2(i) to (v) in full if it is under a legal prohibition or mandatory legal compulsion that prevents it from complying. However, Vendor shall use reasonable and lawful efforts to challenge any such prohibition or compulsion (though Mailchimp acknowledges that such challenge may not always be reasonable or possible in light of the nature, scope, context and purposes of the intended government authority access), and Vendor shall only disclose Covered Data to the extent it is legally required to do so and in accordance with applicable lawful process. In no event shall Vendor knowingly disclose Covered Data in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society.

4.3 Vendor will assist Mailchimp (or its thirdparty Controller) to conduct a data protection impact assessment and, at Mailchimp’sreasonable request, consult with applicable data protection authoritiesin respect of any proposed Processing activity that present a high risk to data subjects.

4.4 Vendor will promptly deal with all inquiries from Mailchimp relating to its Processing of Covered Data under the Contract(s) including making available all information necessary to demonstrate its compliance with Applicable Privacy Laws and this DPA.

5. Security Measures

5.1 Vendor shall ensure that any Authorized Person agrees in writing to protect the confidentiality and security of the Personal Data in accordance with the terms of this DPA, including to ensure that the Authorized Person Processes any Personal Data only for the purpose of delivering the Services under the Contract(s) to Mailchimp. Vendor agrees that Authorized Persons with access to Personal Data: (i) are required to protect and Process all Personal Data in a manner consistent with the terms of the Contract(s) and this DPA; (ii) will receive appropriate training by Vendor regarding the protection of Personal Data prior to receiving accessto Personal Data; and (iii) are restricted in terms of accessto Personal Data based on a “need to know” to provide the Services to Mailchimp.

5.2 Vendor will implement and maintain all reasonable and appropriate technical and organizational security measures to protect from Security Incidents and to preserve the security, integrity and confidentiality of the Personal Data, including (but not limited to) in the event of disruption, disaster or failure of Vendor’s primary systems or operational controls (“**Security Measures**”). Such Security Measures shall have regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, and shall at a minimum, comply with the requirements of Applicable Privacy Laws (including, but not limited to, Article 32 of the GDPR).

5.3 Vendor shall regularly and periodically determine whether upgrades, additions or modifications of applicable controls or Security Measures are required to meet the obligations under this DPA, including upon actual or constructive knowledge of relevant changes in technology and internal and external threats to Personal Data and the Services.

5.4 Without limitation to its other obligations under the Contract(s) and this DPA, Vendor represents, warrants, and covenants that the Security Measures will:

(a) identify appropriately defined organizational roles for security and incident response;

(b) include appropriate controls with respect to organization or person(s) (including Authorized Persons) with access to Personal Data, including background checks, security clearances that assign specific access privileges to individuals, and training regarding the handling of Personal Data;

(c) include an appropriate network security program that includes, without limitation, utilization of encryption when appropriate and, in any case (A) with respect to Personal Data, when transmitted wirelessly or over public networks (e.g., the Internet), when stored on any portable devices or removable media, and/or in any circumstances required under Applicable Privacy Laws; and (B) with respect to Personal Data, when at rest or in those circumstances described in (A); and,

(d) include appropriate controls addressing (A) critical asset identification and asset management; (B) access controls and management; (C) physical and environmental security; (D) communications and operations security and management; (E) systems acquisition, development, and maintenance; (F) thirdparty risk management; (G) configuration and change management for software systems; (H) incident response, planning, and management, including appropriate maintenance, monitoring and analysis of audit logs; and (I) business continuity management and contingency planning/redundancy.

5.5 If Vendor or any Authorized Person is granted accessto or connectsto any computing system, network, platform, facilities or telecommunications or other information system (the "**Systems**") owned, controlled, or operated by or on behalf of Mailchimp or any of its Affiliates, then Vendor and any applicable Authorized Person will be subject to and shall comply with all thencurrent Mailchimp policies, including without limitation, all security, privacy, safety, environmental, information technology, legal and business conduct policies. Any such access or connection to the Systems is strictly for the purpose of Vendor's performance of the Services under and in accordance with the Contract(s). Vendor agrees that Mailchimp may perform periodic network assessments, and should any such assessment reveal inadequate security by Vendor, Mailchimp, in addition to other remedies it may have, may suspend Vendor's access to the Systems until such security issue has been eliminated.

6. Security Incidents

6.1 In the event of a Security Incident, Vendor shall without undue delay (and in no event later than 48 hours of becoming aware of such Security Incident) inform Mailchimp and provide written details of the Security Incident, including the type of data affected and the identity of affected person(s) assoon assuch information becomes known or available to Vendor. Vendor shall keep and maintain a record of every Security Incident and provide a copy of such records to Mailchimp promptly upon request.

6.2 Furthermore, in the event of a Security Incident and without prejudice to any other right or remedy available to Mailchimp, Vendor shall (at its own expense):

(a) provide all timely information and cooperation as Mailchimp may require in order to fulfil Mailchimp's (or the ultimate Controller's) data breach reporting obligations under (and in accordance with the timescales required by) Applicable Privacy Laws. Such information shall include without limitation:

(i) the nature of the Security Incident including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned;

(ii) the name and contact details of the contact point within Vendor (or Vendor's Subcontractors, as applicable) who can provide more information on the Security Incident;

(iii) a description of the likely consequences of the Security Incident; and

(iv) a description of the measures Vendor (or its Subcontractors, as applicable) will take, proposesto take or suggests that Mailchimp takes to address the Security Incident, including, where appropriate to mitigate its possible adverse effects; and

(b) promptly take all such measures and actions as are appropriate and cooperate fully with Mailchimp to prevent, remedy or mitigate the effects of the Security Incident, including at its own expense, and if appropriate, retaining a reputable forensics expert to recommend to Vendor allsteps necessary to stop any ongoing Security Incident, to preserve all records and information related to such activities and to investigate the nature and scope of the Security Incident and shall keep Mailchimp uptodate about all developments in connection with the Security Incident;

(c) at its own expense cooperate with Mailchimp in investigating and responding to the Security Incident, notifying affected individuals and other parties in accordance with applicable law, and seeking injunctive or other equitable relief against any such person or persons who have violated or attempted to violate the security of Personal Data; and

(d) reimburse Mailchimp forthe reasonable costsfor Mailchimp (or the relevant Controller) to send all notifications that are legally required or reasonably necessary. At the written request of Mailchimp, Vendor agrees to provide, at its sole expense, credit monitoring and identity theft protection services to data subjects affected by the Security Incident.

6.3 In the event that applicable law or contract requires that any individuals, organizations, regulators or other parties be notified of a Security Incident, Mailchimp shall determine whether such notice shall come from Mailchimp or Vendor. In any case, the content and provision of any notification, public/regulatory communication or press release concerning the Security Incident shall be solely at Mailchimp's discretion unless otherwise required by applicable law.

7. Security Reports & Inspections

7.1 Vendor shall maintain compliance with security frameworks, including SOC 2 Type II. Upon request, Vendor shall provide copies of relevant audit report summaries and/or other documentation reasonably required by Mailchimp to verify Vendor's compliance with this DPA. Vendor shall also respond to any Mailchimp security questionnaires and meet by teleconference or in person to address any follow up questions.

7.2 While it is the parties' intention ordinarily to rely on Vendor's obligations set forth in Section 7.1 to verify Vendor's compliance with this DPA, Mailchimp (or its appointed representatives) may carry out an inspection of Vendor's records, operations and facilities during normal business hours and subject to reasonable prior notice where Mailchimp considers it necessary or appropriate (for example, without limitation, where Mailchimp has reasonable concerns about Vendor's data protection compliance, following a Security Incident (for which no prior notice will be required), following instruction from the ultimate Controller or a data protection or governmental authority). Mailchimp and Vendor shall mutually agree upon the scope, timing and duration of the audit.

7.3 In the event that any such inspection undertaken pursuant to this Section 7 reveals that Vendor is noncompliant with its obligations under this DPA or Applicable Privacy Laws, Vendor shall promptly bring itself into compliance and pay the reasonable costs associated with the inspection.

8. Data Transfers

8.1 **International Transfers.** Vendor shall (and shall procure that any Subcontractor shall) not Process or transfer (directly or via onward transfer) any Covered Data in or to a territory other than the territory in which the Covered Data was first collected (nor permit the Covered Data to be so Processed or transferred) unless: (i) it hasfirst obtained Mailchimp's prior written consent and (ii) it takes (and procures all Subcontractors take) such measures as are required to comply with this Section 8 and any other measures that Mailchimp may deem necessary to ensure such Processing or transfer is in compliance with Applicable Privacy Laws (including such measures as may be communicated by Mailchimp to Vendor from time to time). Mailchimp authorizes Vendor to transfer Covered Data to the United States, and from the United States to Japan in connection with the services.

8.2 **European Data Transfers.** Without prejudice to Section 8.1 above, Vendor shall not transfer (directly or via onward transfer) Covered Data that is subject to European Privacy Laws ("**European Data**") in or to any country or recipient not recognized as providing an adequate level of protection for Personal Data (as described in European Privacy Laws) (a "**nonAdequate Country**"), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with European Privacy Laws. Such measures may include (without limitation) transferring such data to a recipient in a country that has been designated by the European Commission or United Kingdom law (as applicable) as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Privacy Laws, or to a recipient that has executed appropriate standard contractual clauses adopted or approved by the European Commission or United Kingdom law (as applicable).

8.3 **European Data Transfer Mechanism.** Where Vendor is the recipient of European Data in a nonAdequate Country, any consent provided pursuant to Section 8.1 above shall be conditional on the Vendor complying with (and ensuring any Subcontractor complies with) the following:

(a) Vendor agrees to process such European Data in compliance with the Model Clauses, which are incorporated herein in full by reference and form an integral part of this DPA. The parties agree that for the purposes of the Model Clauses (i) **Annex A** of this DPA and the Security Measures will take the place of Appendixes 1 and 2 of the Model Clauses respectively and (ii) Vendor shall be the "data importer" and Mailchimp shall be the "data exporter" (notwithstanding that Mailchimp is located outside Europe and may itself be a Processor acting on behalf of a Controller). Further, it is not the intention of either party, nor the effect of this DPA, to contradict or restrict any of the provisions set forth in the Model Clauses. Accordingly, if and to the extent the Model Clauses conflict with any provision of this DPA, the Model Clausesshall prevail. In no event doesthis DPA restrict or limit the rights of any Data Subject or of any competent Supervisory Authority.

(b) If and to the extent Vendor is selfcertified to the Privacy Shield, Vendor represents and warrants that it shall: (i) maintain its Privacy Shield certification for the duration of the Contract(s); (ii) provide a least the same level of protection to European Data as is required by the Privacy Shield; and (iii) notify Mailchimp if it can no longer comply with or intends to withdraw from the Privacy Shield.

8.4 **Alternative Transfer Mechanism.** The parties agree that in the event that a Supervisory Authority and/or European Privacy Laws no longer allow the lawful transfer of Covered Data to Vendor and/or requires that Mailchimp adopt an alternative transfer solution that complies with European Privacy Laws, Vendor will fully cooperate with Mailchimp to discuss and agree an amendment to this DPA to remedy such noncompliance and/or cease Processing of Covered Data.
If the parties, acting in good faith, are unable to agree such changes within 30 days, Mailchimp may immediately terminate the Contract(s) without any further liability or obligation to Vendor, and Vendor shall refund to Mailchimp any amounts which were paid for work not yet performed under the Contract(s).

8.5 Vendor shall promptly notify Mailchimp if it makes a determination that it no longer meets its obligations under this Section 8, and in such event but without prejudice to any other right or remedy available to Mailchimp, Vendor shall:

(a) work with Mailchimp and promptly take all reasonable and appropriate steps to stop and remediate (if remediable) any processing until such time as the processing meets the level of protection as is required by this Section 8; and

(b) immediately cease (and require that all Subcontractors immediately cease) processing such Covered Data if in Mailchimp's sole discretion, Mailchimp determines that Vendor has not or cannot correct any noncompliance with this Section 8 within a reasonable time frame.

8.6 Vendor acknowledges that Mailchimp may disclose this DPA and any relevant privacy provisions in the Contract(s) to the US Department of Commerce, the Federal Trade Commission, a European data protection authority, or any other US or EU judicial or regulatory body upon their request.

9. Deletion & Return

9.1 Upon Mailchimp’s request, or upon termination or expiry of this DPA, Vendor shall (and shall procure that any Subcontractors shall): securely destroy (upon written instructions of Mailchimp) or return to Mailchimp all Covered Data (including copies) in its possession or control (including any Covered Data Processed by its Subcontractors and in back up), provided, that this requirement shall not apply to the extent that Vendor is required by any applicable law to retain some or all of the Covered Data, in which event Vendor shall isolate and protect the security and confidentiality of such Covered Data and prevent any further Processing except to the extent required by such law and shall destroy or return to Mailchimp all other Covered Data; and/or immediately cease Processing all Covered Data.

10. Liability

10.1 Notwithstanding anything else to the contrary in the Contract(s), Vendor acknowledges and agrees that: Vendor

acknowledges and agrees that:

(a) it shall be liable for any loss of Covered Data arising under or in connection with the Contract(s) and this DPA to the extent such loss results from any failure of the Vendor (or its Subcontractors) to comply with its obligations under this DPA and/or Applicable Privacy Laws;

(b) it shall be liable for any breach of this DPA and/or Applicable Privacy Laws.

(c) any exclusion of damages or limitation of liability that may apply to limit the Vendor’s liability in the Contract(s) shall not apply to the Vendor’s liability arising under or in connection with this DPA, howsoever caused, regardless of how such amounts orsanctions awarded are characterized and regardless of the theory of liability, which liability shall be expressly excluded from any agreed exclusion of damages or limitation of liability; provided; however, that Vendor’s liability shall not exceed $2,500,000.

11. General

11.1 Except for the changes made by this DPA, the Contract(s) remain unchanged and in full force and effect. If there is any conflict between any provision in this DPA and any provision in the Contract(s), this DPA controls and takes precedence.

11.2 The obligations placed upon the Vendor under this DPA (including, to the extent applicable, the Model Clauses) shall survive for the Term.

11.3 This DPA may not be modified except by a subsequent written instrument signed by both parties. Doc ID:

03b94585cf04063478fb323c4a1700f0636ce22b

11.4 The parties agree that this DPA shall replace any existing data Processing (or equivalent) agreement the parties may have previously entered into in connection with the Services.

11.5 This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions in the Contract(s), unless required otherwise by Applicable Privacy Laws. If no governing law and/or jurisdiction is specified in the Contract(s), then this DPA shall be governed and construed in accordance with the laws of England and Wales, and the parties shall submit to the exclusive jurisdiction of the English courts, unless required otherwise by Applicable Privacy Laws.

11.6 If any part of this DPA is held unenforceable, the validity of all remaining parts will not be affected. Doc ID:

Annex A Details of the Processing

Where the parties rely on the Standard Contractual Clauses, Mailchimp is the data exporter and Vendor is the data importer.

Nature of Services provided by Vendor:

The Nature of Services provided by Vendor includes processing of the data uploaded by Mailchimp to Vendor's contract management SaaS application.

Categories of Data Subjects:

- *Employees* – past, present, potential, and future staff (including volunteers, agents, independent contractors, interns, temporary and casual workers) of Mailchimp

- *Business partners, suppliers and vendors* – past, present, potential and future advisors, consultants, suppliers, contractors, subcontractors and other professionals engaged by Mailchimp and related staff**.**

Categories of Data

Vendor collects the following types of information: first and last name; title; position; employer; contact information (company, email, phone, physical business address); identification data (notably email addresses and phone numbers); and electronic identification data (notably IP addresses and mobile device IDs).

Special categories of data (if applicable):

Processing Purposes: The Purpose of processing of Mailchimp data by Vendor is the performance of the Services pursuant to the Contract.

Processing Operations:

The Covered Data Processed by Vendor and/or its Subcontractors will be subject to the Processing activities described in the Contract(s) and as strictly necessary to provide the Services to Mailchimp in accordance with the Contract(s) and/or as otherwise agreed by the parties. Covered Data may be Processed only to comply with Mailchimp's instructions issued in accordance with DPA.

Duration of Processing: For the Term

c ID: 03b94585cf04063478fb323c4a1700f0636ce22b

Ironclad, Inc.
71 Stevenson St. #600
San Francisco, CA 94105

Order Form

Customer Name: The Rocket Science Group LLC (d/b/a Mailchimp)	**Subscription Start Date:** July 30, 2021
Billing Contact: Mia McKay	**Subscription End Date:** July 29, 2024

Billing Address: 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, Georgia 30308	**Initial Term:** 36 months
Billing Email: ap@mailchimp.com	**Ironclad Account Executive:** Ed Achziger (ed.achziger@ironcladhq.com)
PO Required: Yes	**Billing Frequency:** Annual
Payment Terms: Net 30	**Offer Valid Until:** July 30, 2021

Invoice Schedule: Invoice in the amount of $138,000 will be issued upon execution of the contract.
Invoice in the amount of $118,000 will be issued on July 30, 2022.
Invoice in the amount of $118,000 will be issued on July 30, 2023.

Subscription Products	Annual Unit Price	Quantity	Total Price
Pro Package	$85,000.00	1	$85,000.00
Workflows	$5,000.00	25	Included
Power Users	$1,169.00	20	Included
Standard Users	$169.00	150	Included
CTP Basic Module	$15,000.00	1	$15,000.00
Digital Acceptance Legacy Module (Per Workflow Basis)	$3,000.00	3	$9,000.00
API Access	$10,000.00	1	$10,000.00
Enterprise Success Plan	$23,800.00 *(20% of the Subscription Products above)*	1	$23,800.00
		Subscription Subtotal:	$142,800.00
		Discount Total:	$24,800.00
		Subscription Total:	$118,000.00

Definitions of Subscription Products are available at https://legal.ironcladapp.com/#product-descriptions and hereby incorporated by reference.

One-Time Services	Unit Price	Quantity	Total Price
Accelerate	$8,000.00	1	$8,000.00
Design and Build a Workflow	$12,000.00	1	$12,000.00
		One-Time Total:	$20,000.00

First Year Price	**$138,000.00**

Services Description

Accelerate

Receive guided onboarding from an Ironclad Activation Manager over a series of weekly calls and offline Customer exercises to:

- Guide Customer through a co-build of 2 Standard Workflows using Workflow Designer, implementing digital contracting best practices through a series of eight 1-hour meetings. A Standard Workflow cannot exceed 3 unique contract templates.
- Guide customer through system setup, including eSignature, cloud storage, single-sign on, and permissions management. If applicable, Accelerate can also include coaching on configuration of a standard Salesforce integration, using Ironclad's Managed Package. Salesforce configuration will be limited to Ironclad providing guidance on Ironclad-side configuration settings and will not include advising or accessing Customer's Salesforce environment.
- Train Customer on Workflow Designer so that they can manage the independent design and build of future workflows.
- Provide adoption and rollout best practices, standard launch training collateral and leverage a train-the-trainer approach for ongoing success.

Ironclad's total hours commitment to this Accelerate service will not exceed 35 hours.

Design and Build a Workflow
Receive coaching and implementation services from an Ironclad Legal Engineer over a series of weekly calls and offline exercise to:

- Understand Customer's business requirements and conduct workflow discovery sessions, while providing consultative guidance on process improvements and digital contracting best practices.
- Prepare workflow design documentation, including process map and functional design proposal.
- Deliver 1 Ironclad Workflow, with dedicated milestones for development, iteration, quality assurance, user acceptance testing, and knowledge transfer.
- Provide Customer with handoff documentation on how they can maintain and update their Workflow independently to ensure successful long-term adoption.

Ironclad's total hours commitment for each unit of this Design and Build a Workflow service will not exceed 30 hours.

Special Contractual Terms:

1. Renewal Price Lock: Any renewal of this Order Form (for the same type and quantity of Enterprise Services) shall not exceed a three percent (3%) increase over the then-current subscription price for such Enterprise Services ("Price Lock"); provided, however, the Price Lock is limited to two (2) renewal terms.

c ID: 03b94585cf04063478fb323c4a1700f0636ce22b

I[redacted]c[redacted], I[redacted]c.
71 Stevenson St. #600
San Francisco, CA 94105

This “**Order Form**” and “**Enterprise Services Agreement**” is entered into as of the Effective Date by and between Ironclad and Customer. The Order Form is subject to and incorporates by reference the Enterprise Services Agreement attached hereto. The parties have caused this Order Form to be signed as of the Effective Date by their duly authorized representatives.

The Rocket Science Group LLC (d/b/a Mailchimp) Ironclad, Inc.

Signature: Signature:

Name: Koleen Henson Name: Jason Boehmig

Title: Senior Corporate Counsel Title: CEO

Date: Date: 07 / 29 / 2021 07 / 29 / 2021

IRONCLAD® MAY 2021 Confidential & Proprietary

Doc ID: 03b94585cf04063478fb323c4a1700f0636ce22b

Title

File Name

Document ID

Audit Trail Date Format Status

07 / 29 / 2021
22:21:59 UTC

07 / 29 / 2021
22:23:02 UTC

07 / 29 / 2021
17:57:05 UTC

07 / 30 / 2021
03:09:06 UTC

07 / 30 / 2021

03:09:44 UTC

Audit Trail

Enterprise Services Agreement and Order Form with The Rocket... document_0, document_1

03b94585cf04063478fb323c4a1700f0636ce22b

MM / DD / YYYY

Completed

Sent for signature to Jason Boehmig (jason@ironcladhq.com) and Koleen Henson (koleen@mailchimp.com) from

admin@ironclad.ai
IP: 35.247.59.63

Viewed by Koleen Henson (koleen@mailchimp.com) IP: 174.254.33.173

Signed by Koleen Henson (koleen@mailchimp.com)
IP: 174.254.33.173

Viewed by Jason Boehmig (jason@ironcladhq.com)
IP: 107.77.211.117

Signed by Jason Boehmig (jason@ironcladhq.com)
IP: 107.77.211.117

07 / 30 / 2021 The document has been completed. 03:09:44 UTC