Terms of Service & Privacy Policy

Version 4.8

Last update: 10 Jan 2025

The **oneapp Terms of Service** comprises the following agreements, the current version of which may be found at https://legal.withoneapp.com:

- Merchant Agreement
- Consumer Agreement
    - Applicant Disclosure
    - Authorization for Background Check
- Acceptable Use Policy
- SaaS and Area Specific Requirements
    - Asset and Income Verification SaaS
    - Email SaaS Policy
    - End User Attestations
        - Qualified Subscriber Attestation
    - Identity Verification SaaS
    - Messaging SaaS Policy
    - Payments SaaS
    - SaaS in Private Beta
    - SaaS using Phone Numbers
    - Screening SaaS
        - Qualified Subscriber Terms
- Fee and Payment Authorization Agreement

- Refund Policy
- Security Overview
- Data Protection Addendum
- Privacy Policy
- Sub-Processors
- Service Level Agreements
    - oneapp APIs Service Level Agreement
- Trademarks
- Customer Research and User Experience
- Updates to oneapp's Legal Terms and Conditions

Merchant Agreement

This Merchant Agreement is effective as of the date shown above ("Effective Date"), if you created your account or accepted or otherwise agreed to it on or after the Effective Date.

This Merchant Agreement is effective thirty (30) days after the Effective Date, if you created your account or accepted or otherwise agreed to a previous version of this Merchant Agreement prior to the Effective Date.

Please read our online notice, which explains changes to the Merchant Agreement and our other legal terms and conditions in more detail.

PLEASE REVIEW THIS MERCHANT AGREEMENT CAREFULLY. ONCE ACCEPTED, THIS MERCHANT AGREEMENT BECOMES A BINDING LEGAL COMMITMENT BETWEEN YOU AND ONEAPP.

BY USING, INSTALLING, OR ACCESSING THE SAAS (AS DEFINED IN SECTION 1 (DEFINITIONS) BELOW), AUTHORIZING A BUSINESS OR INDIVIDUAL TO USE OR ACCESS THE SAAS ON YOUR BEHALF, EXECUTING THIS MERCHANT AGREEMENT, OR CLICKING TO ACCEPT WHEN PROMPTED IN THE SAAS, YOU ACCEPT AND AGREE TO BE BOUND BY ALL AGREEMENTS THAT CONSTITUTE ONEAPP'S TERMS OF SERVICE, AND YOU AGREE THAT THE "TERMS OF SERVICE" MEANS EVERY AGREEMENT LINKED HEREIN AND INCLUDES THE

PRIVACY POLICY, ACCEPTABLE USE POLICY, FEE AND PAYMENTS AUTHORIZATION, AND REFUND POLICY. FOR THE AVOIDANCE OF DOUBT, THIS MERCHANT AGREEMENT ALSO INCORPORATES, FOR ANY END USER USING THE SCREENING SAAS (BOTH AS DEFINED IN SECTION 1 (DEFINITIONS) BELOW), THE SCREENING SAAS TERMS, THE QUALIFIED SUBSCRIBER ATTESTATION, AND THE QUALIFIED SUBSCRIBER TERMS AND CONDITIONS.

IF YOU DO NOT AGREE TO THESE TERMS OF SERVICE, YOU SHOULD NOT ACCEPT THEM OR USE THE SAAS.

THE SAAS ARE INTENDED FOR YOUR BUSINESS USE, OR USE IN CONNECTION WITH YOUR INDIVIDUAL TRADE, CRAFT, OR PROFESSION ONLY.

If you have a separate written agreement with oneapp for your use of the SaaS, the Merchant Agreement will not apply to you, unless that written agreement does not cover a particular SaaS application, in which case, this Merchant Agreement applies solely to your use of that particular SaaS application.

This Merchant Agreement sets forth the terms for your use of the SaaS and are effective as of the date you accept or otherwise agree to the terms of this Merchant Agreement (“Effective Date”). This Merchant Agreement is between the applicable oneapp entity identified below (“oneapp”) and the corporation, LLC, partnership, sole proprietorship, or other business entity on whose behalf you are accepting or otherwise agreeing to the terms of this Merchant Agreement (“you", "your", "yours", or "Merchant”).

If you are domiciled in:	**oneapp entity entering into this Merchant Agreement:**
The United States	With One App Inc., a Delaware corporation, with a place of business at 195 Plymouth Street, Suite 3/1, Brooklyn NY 11201, United States of America

oneapp may update the terms of this Merchant Agreement from time to time. oneapp will provide you with written notice of any *material* updates at least thirty (30) days prior to the date the updated version of this Merchant Agreement is effective, unless such material updates result from changes in laws, regulations, or requirements from oneapp’s suppliers. The updated version of this Merchant Agreement will be available at https://legal.withoneapp.com. Notices for material updates to the terms of this Merchant Agreement will be given in accordance with Section 9.5 (Notices). Following such notice, your continued use of the SaaS on or after the date the updated version of this

Merchant Agreement is effective and binding, as indicated at the top of this Merchant Agreement, constitutes your acceptance of the updated version of this Merchant Agreement. The updated version of this Merchant Agreement supersedes all prior versions. If you do not agree to the updated version of this Merchant Agreement, you must stop using the SaaS immediately.

If you are the party that agreed to the terms of this Merchant Agreement and you reassign your account to a third-party for administration purposes, such account reassignment will not excuse your obligations under this Merchant Agreement. Your use of the SaaS will continue to be subject to this Merchant Agreement.

1. Definitions

"*Affiliate*" means with respect to a party, any person or entity that controls, is controlled by, or is under common control with that party, where "control" means the power to direct or cause the direction of management and policies, whether through the ownership of voting securities, by contract, or otherwise.

"*Beta Offerings*" means SaaS that are identified as alpha, beta, not generally available, limited release, developer preview, or any similar SaaS offered by oneapp.

"*Consumer Agreement*" means such terms of service as oneapp may require for users of the SaaS who are not oneapp's customers or their employees, the current version of which is available at https://legal.withoneapp.com.

"*Consumers"* means any of Merchant's business or individual clients or other third parties, to whom Merchant gives access to the SaaS, including without limitation such users' agents and employees.

"*Merchant Data*" means data and other information made available by you to oneapp in connection with your use of the SaaS under this Merchant Agreement.

"*Merchant Services*" means any software application, products, services or Professional Services provided by you and used in connection with your use of the SaaS under this Merchant Agreement. If applicable, Merchant Services includes sources from which you choose to retrieve Merchant Data and destinations to which you choose to transmit Merchant Data using the SaaS.

"*Documentation*" means oneapp documentation, including any usage guides and policies, for the SaaS.

"*End User*" means any business or individual who uses the SaaS on Merchant's behalf or through Merchant's account or passwords, whether authorized or not, including without limitation Consumers.

“*Malicious Code*” means code, files, scripts, agents, or programs intended to do harm, including, for example, viruses, worms, time bombs and Trojan horses.

“oneapp Acceptable Use Policy” means certain terms relating to the use of the SaaS, including the Service and Area Specific Requirements set forth therein, the current version of which is available at https://legal.withoneapp.com.

“*oneapp Data Protection Addendum*” means the personal data processing-related terms for the SaaS, the current version of which is available at https://legal.withoneapp.com.

“*oneapp Security Overview*” means the security related terms for the SaaS, the current version of which is available at https://legal.withoneapp.com.

“*oneapp SLA*” means the service level agreement for the Services, the current version of which is available at https://legal.withoneapp.com.

“*Order*” means an order for access to the SaaS or Third Party Services, executed as follows: (a) successfully registering on oneapp for a customer account; (b) purchasing a subscription for an existing customer account; (c) funding your Merchant account with your payment method, and executing a SaaS clickwrap (d) adding or inviting End Users to access the SaaS under your Merchant account; (e) via completed API call from Merchant Services to your account.

“*Order Form*” means a physical Order document executed between you and oneapp.

“Professional Services” means only those services performed by individuals in connection with a trade, craft or profession.

“*SaaS*” means software as a service applications developed by oneapp or its Affiliates, provided on or through the oneapp cloud platform, as applicable, that (a) you use, including, without limitation, software as a service applications that are on a trial basis or otherwise free of charge or (b) you order under an Order Form. SaaS excludes any Merchant Services and Third Party Services (as defined below).

“*SaaS Usage Data*” means any data that is derived from the use of the SaaS that does not directly or indirectly identify you, your End Users, or any natural person and includes (a) data such as volumes, frequencies, bounce rates, and SaaS performance data and (b) subject to any restrictions under applicable law or regulation, data that is anonymized, de-identified, and/or aggregated such that it could no longer directly or indirectly identify you, your End Users, or any natural person.

“Third Party Services” means any products, services, Professional Services, or software components that are purchased by you from or through oneapp, but provided, or otherwise made available, by a third party (i.e., a party other than oneapp). Third Party

Services are governed by a separate agreement between you and the third-party provider.

Any capitalized term not defined in this Section 1 will have the meaning provided in this Merchant Agreement.

2. The SaaS

2.1 Provision of the SaaS. oneapp will: (a) provide the SaaS to you pursuant to this Merchant Agreement, the applicable Documentation, and any applicable Order Form(s); (b) comply with the oneapp SLA (c) comply with the security terms for the SaaS as set forth in the oneapp Security Overview; (d) provide the SaaS in accordance with laws applicable to oneapp's development of the SaaS for its customers generally (i.e., without regard for your particular use of the SaaS), subject to your use of the SaaS in accordance with this Merchant Agreement, the applicable Documentation, and any applicable Order Form(s); (e) make commercially reasonable efforts to use industry standard measures designed to scan, detect, and delete Malicious Code; (f) if applicable, use trained, qualified personnel to provide the SaaS; and (g) use commercially reasonable efforts to provide you with applicable support for the SaaS.

2.2 Merchant Responsibilities. You will: (a) be solely responsible for all use of the SaaS and Documentation under your account and the Merchant Services; (b) not transfer, resell, lease, license, or otherwise make available the SaaS to third parties (except to make the SaaS available to your End Users) or offer them on a standalone basis; (c) use the SaaS only in accordance with this Merchant Agreement, the oneapp Acceptable Use Policy, the applicable Documentation, any applicable Order Form(s), and applicable law or regulation; (d) be solely responsible for all acts, omissions, and activities of your End Users, including their compliance with this Merchant Agreement, the oneapp Acceptable Use Policy, the applicable Documentation, any applicable Order Form(s), and applicable law or regulation; (e) use commercially reasonable efforts to prevent unauthorized access to or use of the SaaS and notify oneapp promptly of any such unauthorized access or use; (f) provide reasonable cooperation regarding information requests from law enforcement, regulators, or oneapp's suppliers; and (g) comply with your representations and warranties set forth in Section 5 (Representations, Warranties, and Disclaimer).

2.2.1 End Users. Subject to the provisions below of this Section 2.2.1, you may authorize your End Users to access and use the SaaS in such numbers and according to such restrictions as are set forth in the applicable Order, solely for the purposes identified therein. You will: (a) provide complete name, current email address, and other required contact information for each proposed End User upon or before providing such access, and update such information as soon as you become aware of a change; (b)

require that each Consumer execute the then-standard Consumer Agreement; and (c) you will provide oneapp with each copy of your executed Consumer Agreement upon the Consumer's execution. You will make no representations or warranties regarding the SaaS or any other matter, to your End Users or any other third party, from or on behalf of oneapp, and you will not create or purport to create any obligations or liabilities for oneapp. You will be jointly and severally liable to oneapp for your Consumer's compliance with the Consumer Agreement. oneapp will have no obligation to provide support or other services, SLA remedies, or other remedies to your Consumers.

2.3 Suspension of Services. oneapp may suspend the SaaS upon written notice to you if oneapp, in good faith, determines: (a) that you or your End Users materially breach (or oneapp, in good faith, believes that you or your End Users have materially breached) the oneapp Acceptable Use Policy; (b) there is an unusual and material spike or increase in your use of the SaaS and that such traffic or use is fraudulent or materially and negatively impacting the operating capability of the SaaS; (c) that its provision of the SaaS is prohibited by applicable law or regulation; (d) there is any use of the SaaS by you or your End Users that threatens the security, integrity, or availability of the SaaS; or (e) that information in your account is untrue, inaccurate, or incomplete. You remain responsible for the Fees (as defined in Section 3.3 (Payment Terms)).

2.4 Changes to the SaaS. You acknowledge that the features and functions of the SaaS may change over time; provided, however, oneapp will not materially decrease the overall functionality of the SaaS. It is your responsibility to ensure the Merchant Services are compatible with the SaaS. oneapp endeavors to avoid changes to the SaaS that are not backwards compatible, however, if any such changes become necessary, oneapp will use commercially reasonable efforts to notify you at least sixty (60) days prior to implementation. In the event oneapp makes a non-backwards compatible change to certain SaaS applications and such change materially and negatively impacts your use of the SaaS ("*Adverse Change*"), (a) you will notify oneapp of the Adverse Change and (b) oneapp may agree to work with you to resolve or otherwise address the Adverse Change, except where oneapp, in its sole discretion, has determined that an Adverse Change is required for security reasons, by oneapp's suppliers, or to comply with applicable law or regulation.

2.5 Beta Offerings. From time to time, oneapp may make available Beta Offerings. You may, in your sole discretion, choose to use a Beta Offering. oneapp may discontinue a Beta Offering at any time, in its sole discretion, or decide not to make a Beta Offering generally available. To the extent you use any Beta Offerings that are only made available to a limited number of Merchants on an invitation basis in a non-public or private manner (collectively, "*Private Beta Offerings*"), the additional terms in Section 10.1 (Private Beta Offerings) apply to you.

3. Fees and Payment Terms

3.1 Fees. You agree to pay the fees set forth in the applicable Order Form(s). If you use any SaaS not set forth in the applicable Order Form(s), you will be charged the applicable rates available at https://withoneapp.com/#pricing.

3.2 Taxes and Communications Surcharges

3.2.1 Taxes. All fees are exclusive of any applicable taxes, levies, duties, or other similar exactions imposed by a legal, governmental, or regulatory authority in any applicable jurisdiction, including, without limitation, sales, use, value-added, consumption, communications, or withholding taxes (collectively, "*Taxes*"). You will pay all Taxes in connection with this Merchant Agreement, excluding any taxes based on oneapp's net income, property, or employees. If you are required by applicable law to withhold any Taxes from payments owed to oneapp, you will reduce or eliminate such withheld Taxes upon receipt of the appropriate tax certificate or document provided by oneapp. You will provide oneapp with proof of payment of any withheld Taxes to the appropriate authority. Taxes will be shown as a separate line item on an invoice.

3.2.2 Communications Charges. If applicable, all fees are exclusive of any applicable communications service, or telecommunication provider (e.g., supplier) fees or surcharges (collectively, "*Communications Surcharges*"). You will pay all Communications Surcharges in connection with your use of the SaaS. You will pay all costs, fines, or penalties that are imposed on oneapp by a government or regulatory body or a telecommunications service provider as a result of your or your End Users' use of the SaaS.

3.2.3 Exemption. If you are exempt from paying certain Taxes or Communications Surcharges, you will provide the necessary exemption information as requested by oneapp or a valid exemption certificate issued by the appropriate authority via e-mail to support@withoneapp.com. You will be exempt on a going-forward basis once oneapp has approved your exemption request. If the appropriate authority determines, at any time, that you are not exempt from paying any Taxes or Communications Surcharges, you will promptly pay such Taxes or Communications Surcharges to oneapp, plus any applicable interest or penalties.

3.3 Payment Terms. Except as otherwise expressly set forth herein, payment obligations are non-cancelable and fees, Taxes, and Communications Surcharges (collectively, "*Fees*"), once paid, are non-refundable. Except as otherwise set forth in the applicable Order Form(s) and subject to Section 3.3.3 (Payment Disputes), You will pay the Fees due hereunder in accordance with the following applicable payment method:

3.3.1 Credit Card. If you elect to add funds to your account by credit card and use such funds to pay the Fees due, you are responsible for ensuring such funds cover the Fees due. If your account does not have sufficient funds or your credit card declines a charge for the Fees due, oneapp may suspend the provision of the SaaS to all of your accounts until the Fees due are paid in full. You are prohibited from creating new accounts until the Fees due are paid in full.

3.3.2 Invoicing. If you request to receive invoices and oneapp approves you for the same, then, except as otherwise set forth in the applicable Order Form(s) and subject to Section 3.3.3 (Payment Disputes), you will be offered Payment Terms and payment methods at oneapp's discretion. Except as otherwise set forth in the applicable Order Form(s) or an invoice to the extent you procure the SaaS without any applicable Order Form(s), the Fees are payable in United States dollars. If you fail to pay the Fees and remedy such failure within fifteen (15) days of the date oneapp provides you with written notice of the same, then oneapp may (i) assess and you will pay a late fee of the lesser of 1.5% per month or the maximum amount allowable by law and (ii) suspend the provision of the SaaS to all of your accounts until the Fees due are paid in full. You are prohibited from creating new accounts until the Fees due are paid in full.

3.3.3 Payment Disputes. You will notify oneapp in writing within sixty (60) days of the date oneapp charges you for any Fees that you wish to dispute. Where you are disputing any Fees, you must act reasonably and in good faith and will cooperate diligently with oneapp to resolve the dispute. oneapp will not charge you a late fee, unless you fail to cooperate diligently with oneapp or oneapp determines the dispute is not reasonable or brought in good faith by you.

4. Ownership Rights, Merchant Data, and Confidentiality

4.1 Ownership Rights. As between the parties, oneapp exclusively owns and reserves all right, title, and interest in and to the SaaS, the Documentation, oneapp's Confidential Information (as defined in Section 4.3.1 (Definition)), SaaS Usage Data, and any feedback or suggestions you or your End Users provide regarding the SaaS. As between the parties, you exclusively own and reserve all right, title, and interest in and to the Merchant Services, your Confidential Information, and Merchant Data, subject to oneapp's rights to process Merchant Data in accordance with this Merchant Agreement.

4.2 Merchant Data. You grant oneapp and its Affiliates the right to process Merchant Data as necessary to provide the SaaS in a manner that is consistent with this Merchant Agreement and the oneapp Data Protection Addendum. You are responsible for the quality and integrity of Merchant Data.

4.3 Confidentiality

4.3.1 Definition. "*Confidential Information*" means any information or data, regardless of whether it is in tangible form, disclosed by either party ("*Disclosing Party*") to the other party ("*Receiving Party*") that is marked or otherwise designated as confidential or proprietary or that should otherwise be reasonably understood to be confidential given the nature of the information and the circumstances surrounding the disclosure, including, without limitation, this Merchant Agreement, Order Form(s), Merchant Data, security reports and attestations, audit reports, customer lists, pricing, concepts, processes, plans, designs and other strategies, "know how", inventions, and financial, technical, or other business information and materials of Disclosing Party and its Affiliates. Confidential Information does not include any information which: (a) is publicly available through no breach of this Merchant Agreement or fault of Receiving Party; (b) was properly known by Receiving Party, and to its knowledge, without any restriction, prior to disclosure by Disclosing Party; (c) was properly disclosed to Receiving Party, and to its knowledge, without any restriction, by another person without violation of Disclosing Party's rights; or (d) is independently developed by Receiving Party without use of or reference to the Confidential Information of Disclosing Party.

4.3.2 Use and Disclosure. Except as otherwise authorized by Disclosing Party in writing, Receiving Party will not (a) use any Confidential Information of Disclosing Party for any purpose outside of exercising Receiving Party's rights or fulfilling its obligations under this Merchant Agreement and (b) disclose or make Confidential Information of Disclosing Party available to any party, except to Receiving Party's Affiliates, and Receiving Party's and its Affiliates' respective employees, legal counsel, accountants, contractors, and in oneapp's case, subcontractors (collectively, "*Representatives*") who have a "need to know" as necessary for Receiving Party to exercise its rights or fulfill its obligations under this Merchant Agreement. Receiving Party will be responsible for its Representatives' compliance with this Section 4.3. Representatives will be legally bound to protect Confidential Information of Disclosing Party under terms of confidentiality that are at least as protective as the terms of this Section 4.3. Receiving Party will protect the confidentiality of Confidential Information of Disclosing Party using the same degree of care that it uses to protect the confidentiality of its own confidential information but in no event less than reasonable care.

4.3.3 Compelled Disclosure. Receiving Party may disclose Confidential Information of Disclosing Party if so required pursuant to a regulation, law, subpoena, or court order (collectively, "*Compelled Disclosures*"), provided Receiving Party gives Disclosing Party written notice of a Compelled Disclosure (to the extent legally permitted). Receiving Party will provide reasonable cooperation to Disclosing Party in connection with a Compelled Disclosure at Disclosing Party's sole expense.

4.3.4 Injunctive Relief. The parties expressly acknowledge and agree that no adequate remedy may exist at law for an actual or threatened breach of this Section 4.3 and that,

in the event of an actual or threatened breach of the provisions of this Section 4.3, the non-breaching party will be entitled to seek immediate injunctive and other equitable relief, without waiving any other rights or remedies available to it.

4.4 Use of Marks. You grant oneapp the right to use and display your name, logo, and a description of your use case(s) on oneapp's website, in earnings releases and calls, and in marketing and promotional materials, subject to your standard trademark usage guidelines that you expressly provide to oneapp.

5. Representations, Warranties, and Disclaimer

5.1 Power and Authority Representation. Each party represents and warrants that it has validly accepted or entered into this Merchant Agreement and has the legal power to do so.

5.2 Anti-Corruption and International Trade Laws. Each party (a) warrants that it will comply with all applicable anti-corruption, anti-money laundering, economic and trade sanctions, export controls, and other international trade laws, regulations, and governmental orders (collectively, "*Anti-Corruption and Trade Laws*") in the jurisdictions that apply directly or indirectly to the SaaS, including, without limitation, the United States, and (b) represents that it has not made, offered, promised to make, or authorized any payment or anything of value in violation of Anti-Corruption and Trade Laws. You will promptly notify oneapp in writing of any actual or potential violation of Anti-Corruption and Trade Laws in connection with the use of the SaaS and take all appropriate steps to remedy or resolve such violations, including any steps requested by oneapp. If applicable, you represent that you have obtained, and warrant that you will continue to obtain, all licenses or other authorizations required to export, re-export, or transfer the SaaS. Each party represents that it (and in your case, also your End Users) is not on any government prohibited, denied, or unverified-party, sanctions, debarment, or exclusion list or export-controlled related restricted party list (collectively, "*Sanctions Lists*"). You will immediately (i) discontinue your use of the SaaS if you become placed on any Sanctions List and (ii) remove your End Users' access to the SaaS if your End Users become placed on any Sanctions List. You represent that you have not, and warrant that you will not, export, re-export, or transfer the SaaS to an entity on any Sanctions List without prior authorization from the applicable governmental authority. Notwithstanding anything to the contrary in this Merchant Agreement, either party may terminate this Merchant Agreement immediately upon written notice to the other party if the other party is in breach of its obligations in this Section 5.2. If your account is blocked because it is operating in a country or region prohibited under this Section 5.2, you will receive notice of your account being inoperable when you attempt to log into your account in such prohibited country or region.

5.3 Consents and Permissions. You represent and warrant that you have provided and will continue to provide adequate notices, and that you have obtained and will continue to obtain the necessary permissions and consents, to provide Merchant Data to oneapp for processing pursuant to Section 4.2 (Merchant Data).

5.4 SaaS. oneapp represents and warrants that the SaaS perform materially in accordance with the applicable Documentation. Your exclusive remedy for a breach of this Section 5.4 will be, at oneapp's option, to (a) remediate any material non-conformity or (b) refund you the Fees paid for the time period during which the affected SaaS do not comply with this Section 5.4.

5.5 DISCLAIMER. WITHOUT LIMITING A PARTY'S EXPRESS WARRANTIES AND OBLIGATIONS HEREUNDER, AND EXCEPT AS EXPRESSLY PROVIDED HEREIN, THE SAAS ARE PROVIDED "AS IS," AND NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT TO THE FULLEST EXTENT PERMITTED BY LAW. ONEAPP ADDITIONALLY DISCLAIMS ALL WARRANTIES RELATED TO TELECOMMUNICATIONS PROVIDERS. YOU ACKNOWLEDGE THE INTERNET AND TELECOMMUNICATIONS PROVIDERS' NETWORKS ARE INHERENTLY INSECURE AND THAT ONEAPP WILL HAVE NO LIABILITY FOR ANY CHANGES TO, INTERCEPTION OF, OR LOSS OF MERCHANT DATA WHILE IN TRANSIT VIA THE INTERNET OR AN INFRASTRUCTURE SERVICE'S SYSTEMS AND NETWORK. BETA OFFERINGS ARE PROVIDED "AS IS" AND "AS AVAILABLE". ONEAPP MAKES NO WARRANTIES AND WILL HAVE NO LIABILITY FOR ANY BETA OFFERINGS, MERCHANT SERVICES, OR THIRD PARTY SERVICES WHATSOEVER.

6. Mutual Indemnification

6.1 Indemnification by oneapp

6.1.1 Scope of Indemnification. oneapp will defend you, your Affiliates, and each of their directors, officers, and employees (collectively, "*Merchant Indemnified Parties*") from and against any claim, demand, suit, or proceeding made or brought against a Merchant Indemnified Party by a third party alleging that oneapp's development of the SaaS infringes or misappropriates such third party's intellectual property rights ("*oneapp Indemnifiable Claim*"). oneapp will indemnify you from any fines, penalties, damages, attorneys' fees, and costs awarded against a Merchant Indemnified Party or for settlement amounts approved by oneapp for a oneapp Indemnifiable Claim.

6.1.2 Infringement Options. If oneapp's provision of the SaaS has become, or in oneapp's opinion is likely to become, the subject of any oneapp Indemnifiable Claim for third-party intellectual property rights infringement or misappropriation, oneapp may at its option and expense: (a) procure the right to continue to provide the SaaS as set forth herein; (b) modify the SaaS to make them non-infringing; or (c) if the foregoing options are not reasonably practicable, terminate this Merchant Agreement, or, if applicable, terminate the SaaS that are the subject of any oneapp Indemnifiable Claim for third-party intellectual property rights infringement or misappropriation, and refund you any unused pre-paid Fees.

6.1.3 Limitations. oneapp will have no liability or obligation under this Section 6.1 with respect to any oneapp Indemnifiable Claim arising out of (a) your use of the SaaS in breach of this Merchant Agreement; (b) the combination, operation, or use of the SaaS with other applications, portions of applications, products, or services, including, without limitation, the Merchant Services or Third Party Services, where the SaaS would not by themselves be infringing; or (c) SaaS for which there is no charge or Beta Offerings.

6.2 Indemnification by Merchant. You will defend oneapp, its Affiliates, and each of their directors, officers, and employees (collectively, "*oneapp Indemnified Parties*") from and against any claim, demand, suit, or proceeding made or brought against a oneapp Indemnified Party by a third party alleging or arising out of: (a) your or your End Users' breach of Section 2.2 (Merchant Responsibilities) or (b) any Merchant Services infringing or misappropriating such third party's intellectual property rights (collectively, "*Merchant Indemnifiable Claims*"). You will indemnify oneapp from any fines, penalties, damages, attorneys' fees, and costs awarded against a oneapp Indemnified Party or for settlement amounts that you approve for a Merchant Indemnifiable Claim.

6.3 Conditions of Indemnification. As a condition of the foregoing indemnification obligations: (a) the indemnified party ("*Indemnified Party*") will promptly notify the indemnifying party ("*Indemnifying Party*") of any Merchant Indemnifiable Claim or oneapp Indemnifiable Claim (individually or collectively referred to herein as a "*Claim*")in writing; provided, however, that the failure to give prompt written notice will not relieve Indemnifying Party of its obligations hereunder, except to the extent that Indemnifying Party was actually and materially prejudiced by such failure; (b) Indemnifying Party will have the sole authority to defend or settle a Claim; and (c) Indemnified Party will reasonably cooperate with Indemnifying Party in connection with Indemnifying Party's activities hereunder, at Indemnifying Party's expense. Indemnified Party reserves the right, at its own expense, to participate in the defense of a Claim. Notwithstanding anything herein to the contrary, Indemnifying Party will not settle any Claim for which it has an obligation to indemnify under this Section 6 admitting liability or fault on behalf of Indemnified Party, nor create any obligation on behalf of Indemnified Party without

Indemnified Party's prior written consent, which will not be unreasonably withheld, conditioned, or delayed.

6.4 Exclusive Remedy. This Section 6 states Indemnifying Party's sole liability to, and Indemnified Party's exclusive remedy against, the other party for any third-party claims.

7. Limitation of Liability

7.1 LIMITATION ON INDIRECT, CONSEQUENTIAL, AND RELATED DAMAGES. IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS MERCHANT AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, LOST DATA, BUSINESS INTERRUPTION, OR PUNITIVE DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF A PARTY'S OR ITS AFFILIATES' REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE. THE FOREGOING DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

7.2 LIMITATION OF LIABILITY. IN NO EVENT WILL THE AGGREGATE LIABILITY OF EITHER PARTY TOGETHER WITH ALL OF ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS MERCHANT AGREEMENT EXCEED THE AMOUNTS PAID OR PAYABLE BY YOU AND YOUR AFFILIATES HEREUNDER FOR THE SAAS GIVING RISE TO THE LIABILITY DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY.

7.3 EXCEPTIONS TO THE LIMITATION OF LIABILITY. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN SECTION 7.1 (LIMITATION ON INDIRECT, CONSEQUENTIAL, AND RELATED DAMAGES) AND SECTION 7.2 (LIMITATION OF LIABILITY), THE LIMITATIONS IN SECTION 7.1 AND SECTION 7.2 DO NOT APPLY TO (a) YOUR BREACH OF SECTION 2.2 (MERCHANT RESPONSIBILITIES); (b) YOUR AND YOUR AFFILIATES' BREACH OF SECTION 3 (FEES AND PAYMENT TERMS); OR (c) AMOUNTS PAYABLE PURSUANT TO A PARTY'S INDEMNIFICATION OBLIGATIONS UNDER SECTION 6 (MUTUAL INDEMNIFICATION).

8. Term, Termination, and Survival

8.1 Merchant Agreement Term. This Merchant Agreement will commence on the Effective Date and continue until terminated in accordance with Section 8.2 (Termination) ("*Term*").

8.2 Termination

8.2.1 For Convenience. Either party may terminate this Merchant Agreement for convenience by providing the other party with at least thirty (30) days prior written notice. Notwithstanding the preceding sentence, if there are any Order Form(s) in effect, this Merchant Agreement will not terminate until all such Order Form(s) have expired or have been terminated in accordance with the terms therein.

8.2.2 Material Breach. Either party may terminate this Merchant Agreement (including all Order Form(s) and SaaS that are in effect) in the event the other party commits any material breach of this Merchant Agreement and fails to remedy such breach within ten (10) days of the date of written notice of such breach. For the avoidance of doubt, a breach of the oneapp Acceptable Use Policy will be considered a material breach of this Merchant Agreement. If oneapp terminates this Merchant Agreement because of your material breach, then oneapp will also close your accounts.

8.2.3 Insolvency. Subject to applicable law, either party may terminate this Merchant Agreement immediately by providing written notice in the event of the other party's liquidation, commencement of dissolution proceedings, or any other proceeding relating to a receivership, failure to continue business, assignment for the benefit of creditors, or becoming the subject of bankruptcy.

8.3 Survival. Upon termination of this Merchant Agreement, the terms of this Section 8.3 and the terms of the following Sections will survive: Section 2.1(c) (regarding the oneapp Security Overview), Section 3 (Fees and Payment Terms), Section 4 (Ownership, Merchant Data, and Confidentiality), Section 5.5 (Disclaimer), Section 6 (Mutual Indemnification), Section 7 (Limitation of Liability), Section 9 (General), and any applicable terms in Section 10 (Additional Terms).

9. General

9.1.1 Affiliates of Merchant. Your Affiliates may use the SaaS under and in accordance with the terms of this Merchant Agreement. You represent and warrant that you have sufficient rights and the authority to make this Merchant Agreement binding upon each of your Affiliates. You and each of your Affiliates will be jointly and severally liable for the acts and omissions of such Affiliate in connection with this Merchant Agreement and such Affiliate's use of the SaaS. Only you will bring any claim against oneapp on behalf of your Affiliates.

9.1.2 Affiliates of oneapp. An Affiliate of oneapp may provide the SaaS, or a portion thereof, to you or your Affiliates, as applicable, in accordance with this Merchant Agreement and any applicable Order Form(s) with such Affiliate of oneapp. oneapp will (a) be responsible for the SaaS its Affiliates provide and (b) not be relieved of its obligations under this Merchant Agreement if its Affiliates provide the SaaS or a portion thereof. oneapp will enforce the terms of this Merchant Agreement relating to the SaaS its Affiliates provide. Notwithstanding anything to the contrary in this Merchant Agreement, an Affiliate of oneapp may directly bill you or your Affiliates, as applicable, (i) for the SaaS it provides or (ii) solely as a billing agent for oneapp or the Affiliate of oneapp providing the SaaS, as applicable.

9.2 Assignment. Neither party may assign or otherwise transfer this Merchant Agreement or any applicable Order Form(s), in whole or in part, whether by operation of law or otherwise, without the other party's prior written consent (not to be unreasonably withheld or delayed). Notwithstanding the foregoing, oneapp may assign this Merchant Agreement or any applicable Order Form(s), in whole or in part, without consent to (a) a successor to all or part of its assets or business or (b) an Affiliate. Any attempted assignment or transfer by either party in violation hereof will be void. Subject to the foregoing, this Merchant Agreement and any applicable Order Form(s) will be binding on the parties and their respective successors and permitted assigns.

9.3 Relationship. Each party is an independent contractor in the performance of each and every part of this Merchant Agreement. Nothing in this Merchant Agreement is intended to create or will be construed as creating an employer-employee relationship or a partnership, agency, joint venture, or franchise. Each party will be solely responsible for all of its employees and agents and its labor costs and expenses arising in connection therewith and for any and all claims, liabilities, damages, or debts of any type whatsoever that may arise on account of its activities, or those of its employees and agents, in the performance of this Merchant Agreement. Neither party has the authority to commit the other party in any way and will not attempt to do so or imply that it has the right to do so.

9.4 No Third-Party Beneficiaries. This Merchant Agreement does not confer any benefits on any third party (including your End Users or an Affiliate) unless it expressly states that it does.

9.5 Notices. Notices to oneapp will be provided via email to legalnotices@withoneapp.com. All notices to you will be provided via email to the relevant contact(s) you designate in your account.

9.6 Governing Law and Attorneys' Fees. This Merchant Agreement will be governed by and interpreted according to the laws of the applicable state or country identified below

without regard to conflicts of laws and principles that would cause the application of the laws of another jurisdiction. This Merchant Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods. Except as provided in Section 9.7 (Dispute Resolution), any legal suit, action, or proceeding arising out of or relating to this Merchant Agreement or the SaaS will be instituted in the applicable courts identified below and the parties hereby consent to the personal jurisdiction of these courts. In the event of any adjudication of any dispute under this Merchant Agreement, the prevailing party in such legal suit, action, or proceeding will be entitled to reimbursement of its attorneys' fees and related costs by the non-prevailing party.

If you are domiciled in:	**Governing law:**	**Courts with personal jurisdiction:**
The United States	State of Delaware	State or federal courts of Delaware, United States of America

9.7 Dispute Resolution. In the event of any dispute, claim, or controversy in connection with this Merchant Agreement (other than for disputes, claims, or controversies related to the intellectual property of a party) (collectively, "*Disputes*"), each party's senior representatives will, in good faith, attempt to resolve a Dispute. If the parties are unable to resolve a Dispute within thirty (30) days or within such other time period as the parties may agree in writing, then the parties may commence binding arbitration under JAMS' Comprehensive Arbitration Rules and Procedures. The parties will share equally the fees and expenses of the JAMS arbitrator. The arbitration will be conducted by a sole arbitrator mutually agreed to between the parties or, failing that, by JAMS under its then prevailing rules. Judgment on the award rendered by the arbitrator may be entered in any court of competent jurisdiction. The arbitrator will have the authority to grant specific performance or any other equitable or legal remedy, including provisional remedies. Each party will be responsible for its own incurred expenses arising out of any dispute resolution procedure. Any arbitration proceedings will take place in the English language in (a) New York, New York, if you are domiciled in The United States and any country outside of the United States.

9.8 Force Majeure. No failure, delay, or default in performance of any obligation of a party will constitute an event of default or breach of this Merchant Agreement to the extent that such failure to perform, delay, or default arises out of a cause, existing or future, that is beyond the control and without negligence of such party, including action or inaction of governmental, civil or military authority, fire, strike, lockout, or other labor dispute, flood, terrorist act, war, riot, theft, earthquake, or other natural disaster

(collectively, "*Force Majeure Events*"). The party affected by a Force Majeure Event will take all reasonable actions to minimize the consequences of any such event.

9.9 Waiver and Order of Precedence. No failure or delay by either party in exercising any right or enforcing any provision under this Merchant Agreement will constitute a waiver of that right or provision, or any other provision. Titles and headings of sections of this Merchant Agreement are for convenience only and will not affect the construction of any provision of this Merchant Agreement. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable Order Form(s), (2) the oneapp Data Protection Addendum, (3) the terms set forth in the body of this Terms of Service, (4) the oneapp Acceptable Use Policy, (5) any other terms incorporated by reference herein or any other exhibits or attachments hereto, and (6) the applicable Documentation.

9.10 Severability. In the event that any provision of this Merchant Agreement is held by a court or other tribunal of competent jurisdiction to be unenforceable, such provision will be limited or eliminated to the minimum extent necessary to render such provision enforceable and, in any event, the remainder of this Merchant Agreement will continue in full force and effect.

9.11 Entire Merchant Agreement. This Merchant Agreement (including all exhibits and attachments hereto) will constitute the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior and contemporaneous understandings, proposals, statements, sales materials, presentations, or non-disclosure or other agreements, whether oral or written. No oral or written information or advice given by oneapp, its agents, or its employees will create a warranty or in any way increase the scope of the warranties or obligations in this Merchant Agreement. The parties agree that any term or condition stated in your Order Form(s) or registration portal or in any purchase order document or similar document will be construed solely as evidence of your internal business processes and the terms and conditions contained therein will be void and have no effect with regard to this Merchant Agreement, even if accepted by oneapp or executed by the parties after the Effective Date.

10. Additional Terms

10.1 Private Beta Offerings. Any Private Beta Offerings made available to Merchant are strictly for testing and experimentation purposes only. Merchant acknowledges that, by their nature, Private Beta Offerings may (a) not meet speed or performance benchmarks or expectations; (b) have gaps in functionality; and (c) contain bugs. The oneapp SLA does not apply to Private Beta Offerings. Private Beta Offerings, and any information

related to such Private Beta Offerings, including their existence, are considered oneapp's Confidential Information.

10.6 Partner Program. If you are joining or participating in any oneapp partner program, the following terms apply:

10.6.1 Partner Program Acceptance Conditions. Your acceptance into the applicable Partner Program is conditioned on (a) oneapp's approval of your completed application to join such applicable Partner Program, if applicable; (b) your satisfaction of all Partner Program acceptance qualifications and requirements that are communicated to you in writing by oneapp; and (c) your acceptance and compliance with the terms of this Merchant Agreement.

10.6.2 Partner Program Guides and Policies. You will comply with the applicable Partner Program guides and policies as they are made available to you.

10.6.3 Use of Marks and Publicity. Each party ("Licensor") grants the other party ("Licensee") the right to use and display Licensor's trademarks, service marks, names, logos, images, Partner Program participation badges, collateral, or similar materials ("Brand Elements") (a) to identify the parties' relationship and (b) for marketing activities relating to the applicable Partner Program. Any Brand Elements will be used in accordance with Licensor's then-current Brand Elements and guidelines. oneapp's Brand Elements and guidelines are available at https://legal.withoneapp.com. oneapp's Brand Elements are non-transferrable, and oneapp may revoke your right to use and display oneapp's Brand Elements at any time upon written notice to you. Neither party will issue any press releases or public announcements relating to the Partner Program, or your participation in the Partner Program, without the other party's prior written approval.

10.6.4 Partner Program Removal. oneapp may, for any reason or no reason, remove you from the applicable Partner Program, or your access to the applicable Partner Program account portal, upon thirty (30) days prior written notice to you.

Consumer Agreement

This Consumer Agreement is effective as of the date shown above ("Effective Date"), if you created your account or accepted or otherwise agreed to it on or after the Effective Date.

This Consumer Agreement are effective thirty (30) days after the Effective Date, if you created your account or accepted or otherwise agreed to a previous version of this Consumer Agreement prior to the Effective Date.

Please read our online notice, which explains changes to this Consumer Agreement and our other legal terms and conditions in more detail.

PLEASE REVIEW THIS CONSUMER AGREEMENT CAREFULLY. ONCE ACCEPTED, THIS CONSUMER AGREEMENT BECOME A BINDING LEGAL COMMITMENT BETWEEN YOU AND ONEAPP.

BY USING, INSTALLING, OR ACCESSING THE SAAS (AS DEFINED IN SECTION 1 (DEFINITIONS) BELOW), AUTHORIZING A BUSINESS OR INDIVIDUAL TO USE OR ACCESS THE SAAS ON YOUR BEHALF, EXECUTING THIS CONSUMER AGREEMENT, OR CLICKING TO ACCEPT WHEN PROMPTED IN THE SAAS, YOU ACCEPT AND AGREE TO BE BOUND BY ALL AGREEMENTS THAT CONSTITUTE ONEAPP'S TERMS OF SERVICE, AND YOU AGREE THAT THE "TERMS OF SERVICE" MEANS EVERY AGREEMENT LINKED HEREIN AND INCLUDES THE PRIVACY POLICY, ACCEPTABLE USE POLICY, FEE AND PAYMENTS AUTHORIZATION, AND REFUND POLICY. FOR THE AVOIDANCE OF DOUBT, THIS AGREEMENT ALSO INCORPORATES, FOR ANY CONSUMER USING THE SCREENING SAAS (BOTH AS DEFINED IN SECTION 1 (DEFINITIONS) BELOW), THE APPLICANT DISCLOSURE AND AUTHORIZATION FOR BACKGROUND CHECK.

THE TERMS AND CONDITIONS SET FORTH IN THIS CONSUMER AGREEMENT, YOU ACCEPT THIS CONSUMER AGREEMENT AND AGREE TO BE BOUND BY THEM.

IF YOU DO NOT AGREE TO THIS CONSUMER AGREEMENT, YOU SHOULD NOT ACCEPT THEM OR USE THE SAAS.

SECTION 10 OF THE CONSUMER AGREEMENT CONTAINS PROVISIONS THAT GOVERN HOW CLAIMS THAT YOU AND WE HAVE AGAINST EACH OTHER ARE RESOLVED, INCLUDING, WITHOUT LIMITATION, ANY CLAIMS THAT AROSE OR WERE ASSERTED BEFORE THE EFFECTIVE DATE OF THE CONSUMER AGREEMENT. IN PARTICULAR, SECTION 10 SETS FORTH OUR ARBITRATION AGREEMENT WHICH WILL REQUIRE DISPUTES BETWEEN US TO BE SUBMITTED TO ARBITRATION, WITH LIMITED EXCEPTIONS. UNLESS YOU OPT OUT OF THE ARBITRATION AGREEMENT AND TO THE EXTENT PERMITTED BY APPLICABLE LAW: (1) YOU WILL ONLY BE PERMITTED TO PURSUE CLAIMS AND SEEK RELIEF AGAINST US ON AN INDIVIDUAL BASIS, NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY CLASS OR REPRESENTATIVE ACTION OR PROCEEDING (EXCEPT AS SET FORTH IN SECTION 10); AND (2) YOU ARE WAIVING YOUR RIGHT TO SEEK RELIEF IN A COURT OF LAW AND TO HAVE A JURY TRIAL ON YOUR CLAIMS.THE ARBITRATION AGREEMENT COULD AFFECT

YOUR RIGHT TO PARTICIPATE IN PENDING OR PROPOSED CLASS ACTION LITIGATION.

IN ADDITION:

- **SECTION 5 OF THE CONSUMER AGREEMENT REQUIRES YOU TO CONSENT TO ELECTRONIC COMMUNICATIONS AND SIGNATURES**
- **SECTION 7.1 OF THE CONSUMER AGREEMENT REQUIRES YOU TO CONSENT TO OUR ACCEPTABLE USE POLICY**
- **SECTION 7.2 OF THE CONSUMER AGREEMENT REQUIRES YOU TO CONSENT TO OUR PRIVACY NOTICE.**
- **SECTION 9 OF THE CONSUMER AGREEMENT CONTAINS PROVISIONS RELATING TO OUR USE OF CERTAIN USER CONTENT.**
- **SECTION 14 OF THE CONSUMER AGREEMENT CONTAINS PROVISIONS WHICH LIMIT OUR LIABILITY TO YOU.**

This Consumer Agreement ("Consumer Agreement") applies to users of the SaaS who are not oneapp customers or their employees. For clarity, oneapp's customers are corporations, LLCs, partnerships, sole proprietorships, or other business entities, who make the SaaS available for their business and professional purposes (each, a "Merchant"), and Merchants are subject to the Merchant Agreement, the current version of which is available at https://legal.withoneapp.com.

The Consumer Agreement sets forth the terms for your use of the SaaS and are effective as of the date you accept or otherwise agree to the terms of the Consumer Agreement ("Effective Date"). The Consumer Agreement are between the applicable oneapp entity identified below ("oneapp") and you or the organization on whose behalf you are accepting or otherwise agreeing to the terms of the Consumer Agreement ("you", "your", "yours", or "Consumer").

If you are domiciled in:	**oneapp entity entering into the Consumer Agreement:**
The United States	With One App Inc., a Delaware corporation, with a place of business at 195 Plymouth Street, Suite 3/1, Brooklyn NY 11201, United States of America

oneapp may update the terms of the Consumer Agreement from time to time, and notice may be provided via email, or by posting an updated version of this Consumer Agreement at https://legal.withoneapp.com. Following such notice, your continued use of the SaaS on or after the date the updated version of the Consumer Agreement is effective and binding, as indicated at the top of the Consumer Agreement, and

constitutes your acceptance of the updated version of the Consumer Agreement. The updated version of the Consumer Agreement supersedes all prior versions. If you do not agree to the updated version of the Consumer Agreement, you must stop using the SaaS immediately.

1. Definitions

"*Affiliate*" means with respect to a party, any person or entity that controls, is controlled by, or is under common control with that party, where "control" means the power to direct or cause the direction of management and policies, whether through the ownership of voting securities, by contract, or otherwise.

"*Beta Offerings*" means SaaS that are identified as alpha, beta, not generally available, limited release, developer preview, or any similar SaaS offered by oneapp.

"*Consumer Agreement*" means any such terms of service as oneapp may require for users of the SaaS who are not oneapp's customers or their employees, the current version of which is available at https://legal.withoneapp.com.

"*Consumers"* means any of Merchant's business or individual clients or other third parties, to whom Merchant gives access to the SaaS, including without limitation such users' agents and employees.

"*Merchant Data*" means data and other information made available by you to oneapp in connection with your use of the SaaS under this Agreement.

"*Merchant Services*" means any software application, products, services or Professional Services provided by you and used in connection with your use of the SaaS under this Agreement. If applicable, Merchant Services includes sources from which you choose to retrieve Merchant Data and destinations to which you choose to transmit Merchant Data using the SaaS.

"*Documentation*" means oneapp documentation, including any usage guides and policies, for the SaaS.

"*Consumer*" means any business or individual who uses the SaaS on Merchant's behalf or through Merchant's account or passwords, whether authorized or not, including without limitation Consumers.

"*Malicious Code*" means code, files, scripts, agents, or programs intended to do harm, including, for example, viruses, worms, time bombs and Trojan horses.

“oneapp Acceptable Use Policy” means certain terms relating to the use of the SaaS, including the Service and Area Specific Requirements set forth therein, the current version of which is available at https://legal.withoneapp.com.

“*oneapp Data Protection Addendum*” means the personal data processing-related terms for the SaaS, the current version of which is available at https://legal.withoneapp.com.

“*oneapp Security Overview*” means the security related terms for the SaaS, the current version of which is available at https://legal.withoneapp.com.

“*oneapp SLA*” means the service level agreement for the Services, the current version of which is available at https://legal.withoneapp.com.

“*Order*” means an order for access to the SaaS or Third Party Services, executed as follows: (a) successfully registering on oneapp for a Merchant account; (b) purchasing a subscription for an existing Merchant account; (c) funding your Merchant account with your payment method, and executing a SaaS clickwrap (d) adding or inviting Consumers to access the SaaS under your Merchant account; (e) via completed API call from Merchant Services to your account.

“*Order Form*” means a physical Order document executed between you and oneapp.

“Professional Services” means only those services performed by individuals in connection with a trade, craft or profession.

“*SaaS*” means software as a service applications developed by oneapp or its Affiliates, provided on or through the oneapp cloud platform, as applicable, that (a) you use, including, without limitation, software as a service applications that are on a trial basis or otherwise free of charge or (b) you order under an Order Form. SaaS excludes any Merchant Services and Third Party Services (as defined below).

“*SaaS Usage Data*” means any data that is derived from the use of the SaaS that does not directly or indirectly identify you, your Consumers, or any natural person and includes (a) data such as volumes, frequencies, bounce rates, and SaaS performance data and (b) subject to any restrictions under applicable law or regulation, data that is anonymized, de-identified, and/or aggregated such that it could no longer directly or indirectly identify you, your Consumers, or any natural person.

“Third Party Services” means any products, services, Professional Services, or software components that are purchased by you from or through oneapp, but provided, or otherwise made available, by a third party (i.e., a party other than oneapp). Third Party Services are governed by a separate agreement between you and the third-party provider.

Any capitalized term not defined in this Section 1 will have the meaning provided in this Agreement.

2. Eligibility

2.1 You may only enter into the Consumer Agreement if you are over the age of majority and/or able to enter into a legally binding contract in the area in which you are domiciled.

2.2 You must not use the SaaS if you have previously been terminated or suspended from using any of our SaaS. You may not enter into the Consumer Agreement or use any SaaS if you are the target of government sanctions, such as those applied by the U.S. Department of the Treasury Office of Foreign Assets Control, or any other national government.

2.3 You must be eligible for the particular SaaS to the extent they are available in your area. If oneapp presents an incorrect area for you or you move areas, then you must correct the area associated with you in the SaaS before using the SaaS again.

3. oneapp’s Role

3.1 You understand, acknowledge and agree that: (a) oneapp provides the SaaS to Merchants, who make the SaaS available to you to provide their Merchant Services offered through the SaaS; (b) oneapp is in the business of providing the SaaS, oneapp is not a provider of Professional Services such as a real estate broker or agent, landlord, lessor, property manager, debt collector, attorney, or merchant, and has no responsibility or liability for the acts or omissions of any Merchant; (c) Merchants are the merchants of Merchant Services offered through the Saas; (d) the SaaS facilitates the transmission of Orders and related Merchant Data initiated by Consumers; (e) oneapp will not guarantee the suitability, legality, or ability of any Merchant; (f) oneapp is not responsible for Merchants’ offerings or delivery or Merchant Services, or whether the photographs, images, real estate listing information, application requirements or lease terms displayed through the SaaS accurately reflect Merchant Services offered, sold or delivered by oneappMerchants; (g) oneapp does not verify Merchants' compliance with applicable laws or regulations; (h) oneapp has no responsibility or liability for acts or omissions by Merchant; (i) the Merchant Services you purchase will be provided through the SaaS by the Merchant you have selected, and that your orders for Merchant Services will be directed by your instructions to the Merchant, Consumers and third parties that you designate using information that you provide to the SaaS; and (j) oneapp does not acquire any ownership or other interest in any Merchant Services that you order through the SaaS.

3.2 Any contract for Merchant Services made using the SaaS is directly between you and the Merchant. You, and not oneapp, are responsible for the purchases you make using the SaaS. The Merchant, and not oneapp, is responsible for the Merchant Services that you may purchase from them using the SaaS, including but not limited to delivery, quality of goods, quality of services, refunds, fraud, advertising, liability relating to the Merchant's products or services, or non-compliance with applicable law.

3.3 Your access to and use of the SaaS does not change your relationship with the Merchant, Third Party Services or platforms or with your bank or credit or debit card company.

3.4 Except as provided otherwise in these Consumer Agreement, oneapp will not intervene in any dispute between you and a Merchant for any transactions using the SaaS. If you find yourself in a dispute with a Merchant or a third party, oneapp encourages you to contact the other party and try to resolve the dispute. You can submit a complaint regarding a Merchant via email to oneapp at support@withoneapp.com, and oneapp may forward your complaint to the Merchant with a request that they contact you directly. Except as provided otherwise in these Consumer Agreement, oneapp will not make judgments regarding factual disputes or legal issues or claims between you and the Merchant, and oneapp has no obligation to resolve any disputes. You release oneapp from any claims, demands, and damages arising out of disputes relating to your use of the SaaS, the Third Party Services, and the Merchant Services, including those with other users or parties.

3.5 oneapp makes no warranties with respect to the Merchant Services or information provided by Merchants, and oneapp is not responsible or liable for: (a) product liability claims in respect of Merchants; (b) claims that the offer or sale of Merchants' products or services fails to conform to any applicable legal or regulatory requirement; (c) claims respecting Merchants' products, services, or practices arising under consumer protection or similar legislation; (d) any inaccurate, incomplete or out of date information offered by a Merchant; or (e) the acts or omissions of any third party platform where you may interact with or purchase from.

4. Identification and Prevention of Fraud, Consumer Account

4.1 Identification and Prevention of Fraud. You agree that: (a) Information you provide about yourself and your use of the SaaS must be complete and accurate as of the time provided, and you must keep this information up-to-date; (b) to the extent law allows, oneapp, its subprocessors and Third Party Services may verify your identity; and (c) you must notify oneapp immediately via email at support@withoneapp.com if you become aware of any unauthorized use or access to the SaaS with your credentials. You are

responsible for any actions taken through the use of your credentials, except for actions taken after you have told us that your account or credentials have been compromised.

4.2 Consumer Account. You may be required to register for an account to use parts of the SaaS. You must provide accurate, current, and complete information during the registration process and at all other times when you use the SaaS, and to update the information to keep it accurate, current, and complete. You are the sole authorized Consumer of any account you create through the SaaS. You are solely and fully responsible for all activities that occur under your password or account. You agree that you shall monitor your account to prevent use by minors, and you will accept full responsibility for any unauthorized use of your password or your account. Neither oneapp nor other Consumers may access your Consumer account without your authorization, and you may not authorize other Consumers to access or use your Consumer account except as permitted by the Consumer Agreement or where the law requires. You may not assign or otherwise transfer your Consumer account to any other person or entity. Should you suspect that any unauthorized party may be using your password or account, you will notify oneapp immediately via email at support@withoneapp.com. oneapp will not be liable, and you may be liable, for losses, damages, liability, expenses, and fees incurred by oneapp or a third party arising from someone else using your account. If you provide any information to the SaaS in the creation or maintenance of your User Account that is untrue, inaccurate, not current, or incomplete, or if oneapp has reasonable grounds to suspect that such information is untrue, inaccurate, not current, or incomplete, oneapp has the right to suspend or terminate your Consumer account and refuse any and all current or future use of the SaaS (or any portion thereof). oneapp may enable or require you to use a single set of login credentials to use the SaaS. You agree not to create an account or use the SaaS if you have been previously removed from the oneapp platform by oneapp or if you have been previously banned from use of the SaaS.

5. Electronic Communications and Signatures

5.1 Consent. oneapp or other parties may send you certain terms and conditions, agreements, disclosures, notices, records, or other communications regarding the SaaS, or Merchant Services or Third Party Services provided through the SaaS (“Communications”). By accepting the Consumer Agreement, or by accessing or using the SaaS, you consent: (a) to receive Communications electronically; and (b) to use electronic signatures. You also agree that all Communications provided to you electronically satisfy any legal requirement for such communications to be in writing. You agree to keep your contact information, including email address, current. This Section 10 does not affect your statutory rights. If you choose not to consent to this

Disclosure or if you withdraw your consent, you may be unable to use the Consumer Services.

5.2 Paper Copy of the Consumer Agreement. To view and retain a copy of the Consumer Agreement, you will need (a) a device (such as a computer or mobile phone) with a web browser and Internet access, and (b) either a printer or storage space on such device.

5.3 How to Withdraw Your Consent. You may withdraw your consent to receive electronic Communications under this Section 10 by contacting oneapp via email at support@withoneapp.com or by writing to us at: With One App Inc., 195 Plymouth Street, Suite 3/1, Brooklyn NY 11201. You may only contact us by e-mail or mail to withdraw your consent. Your withdrawal of consent will cancel your ability to receive electronic Communications, and may terminate your ability to use the SaaS. Your withdrawal of consent to receive electronic Communications will be effective after oneapp has had a reasonable period of time to process your withdrawal.

5.4 Federal Law. You acknowledge and agree that if you are domiciled in the United States the SaaS are subject to the federal Electronic Signatures in Global and National Commerce Act ("E-SIGN Act"), and that you intend that the E-SIGN Act apply to validate your ability to engage in transactions related to the SaaS electronically.

6. Communications with oneapp

6.1 To the extent allowable under law, by providing us with a phone number, you consent to receiving text (SMS) messages, push notifications, and phone calls from the SaaS. Such communications may include, but are not limited to, requests for secondary authentication, receipts, reminders, notifications regarding updates to your account or account support, requests for product feedback, and marketing or promotional communications. You acknowledge that you are not required to consent to receive promotional texts or calls as a condition of using the SaaS. Call and text message communications may be generated by automatic telephone dialing systems. Standard message and data rates your cell phone carrier applies may apply to the text messages we send you.

6.2 You may opt-out of receiving promotional email communications we send to you by following the unsubscribe options on such emails or by managing your communications preferences in the app. You may opt-out of text messages from the SaaS by replying STOP or by following instructions that you receive in the text message. You may opt-out of phone calls by notifying the caller or by contacting support via email at support@withoneapp.com. You acknowledge that opting out of receiving communications may impact your use of the SaaS.

6.3 You authorize your wireless carrier to use or disclose information about your account and your wireless device, if available, to oneapp or its subprocessor for the duration of your business relationship, solely to help them identify you or your wireless device and to prevent fraud.

7. The SaaS

7.1 Use of the SaaS. You will use the SaaS in accordance with the Consumer Agreement, the Documentation, the oneapp Acceptable Use Policy, and applicable law.

7.2 Consent to Privacy Notice. You acknowledge having read and understood the oneapp Privacy Notice, and you consent to the collection, use, and disclosure of your personal information by the SaaS in accordance with the oneapp Privacy Notice, which is incorporated in the Consumer Agreement by reference.

7.3 4. Availability of the SaaS. You understand that use and availability of the SaaS may be interrupted, including for maintenance, upgrades, or network or equipment failures. oneapp may discontinue the SaaS, any of its features, and/or support for the SaaS, including its use on certain devices and platforms, at any time.

8. Fees and Payment Terms

8.1 Prices and Charges. You understand that: (i) the prices for items displayed through the SaaS are set by Merchants, and may differ from the prices offered or published by Merchants for the same items and/or from prices available at third party websites, and that such prices may not be the lowest prices at which the items are sold and may change at any time without notice; (ii) oneapp has no obligation to itemize its costs, profits, or margins when publishing such prices; and (iii) pricing may change at any time, in the discretion of a Merchant. For certain transactions, the subtotals shown at checkout are estimates that may be higher or lower depending on the final totals. In those situations, oneapp reserves the right to temporarily authorize or place a hold on your payment method for an amount that may be greater than the amount shown at checkout and to charge your payment method the final price after checkout. You are liable for all transaction taxes (other than taxes based on oneapp's income), including sales tax, use tax, goods and services tax, and other transaction taxes if applicable, on the SaaS provided under the Consumer Agreement. If transaction taxes, including sales tax, use tax, goods and services tax, and other transaction taxes, are applicable, oneapp reserves the right to charge you additional amounts on account of such taxes. Where legally required, all dollar amounts (including any fees, charges, prices, or amounts payable or receivable) displayed through the SaaS are stated on a goods and services tax-inclusive (if any) basis, except where noted; goods and services tax will be payable in addition to and at the same time as any amounts payable under these

Consumer Agreement. In the event that the charge to your payment method may incorrectly differ from the total amount, including subtotal, and fees displayed to you at checkout, oneapp reserves the right to make an additional charge to your payment method after the initial charge so that the total amount charged is consistent with the total amount displayed to you at checkout and/or after gratuity is selected. All payments will be processed by a oneapp or a Merchant's payments processor, using the preferred payment method designated in your account. If your payment details change, you or your card provider may provide us with updated payment details. oneapp may use these new details or details from other payment methods on file in order to help prevent any interruption to your use of the SaaS. This includes our right to charge any payment method on file if your initial form of preferred payment fails. It is your responsibility to keep your billing information up to date.

8.2 Strikethrough Pricing. The SaaS may use strikethrough pricing for certain items (for example, when presenting a discount or promotional price for items). oneapp does not represent that the strikethrough price was the regular or former price of items for any particular period of time and the time period may vary widely depending on the items. oneapp may also rely on Merchants to provide information about the regular or former price of items offered by those Merchants, and Merchants' strikethrough price therefore may represent the price that a Merchant offered the item for sale for some period of time. The strikethrough price may also be an introductory price that was offered for a short period of time.

8.2 Refunds. Charges paid by you for completed orders, or for orders confirmed by a Merchant or by the SaaS, are final and non-refundable. oneapp has no obligation to provide refunds or credits but may grant them gratuitously at oneapp's sole discretion in each case. In order to make a claim for a refund or credit, please email oneapp at support@withoneapp.com for the procedures set out in the oneapp Refund Policy.

8.3 Fees for the SaaS and Merchant Services. All fees, whether charged by oneapp, or by Merchants to you, will be referred to collectively as the "Fees." Merchants and oneapp may charge the Fees to you through the SaaS, where applicable. oneapp may change the Fees that oneapp charges you as oneapp deems necessary or appropriate for its business. The SaaS may offer different pricing to you based on a variety of factors, including but not limited to Merchants paying credits towards Consumer orders as part of a promotional offer, or from geographic areas or usage. oneapp may also charge you additional fees as required by law. Further, oneapp may charge fees to Merchants on orders that you place through the SaaS, and the SaaS may change those Merchant fees as oneapp deems necessary or appropriate for its business or to comply with applicable law. oneapp may charge you a service fee for the convenience of ordering through the oneapp platform. None of the service fee or any other fee charged to you by oneapp is for any right to access, install, or use any of the SaaS.

9. Ownership Rights, Data Protection

9.1 oneapp alone (and its licensors, where applicable) shall own all right, title, and interest, including all related intellectual property rights, in and to the SaaS and the Documentation. The Consumer Agreement is not a sale and does not convey to you any rights of ownership in or related to the SaaS, or any intellectual property rights owned by oneapp. oneapp names, oneapp logos, and the product names associated with the Technology and Services are trademarks of oneapp or third parties, and no right or license is granted to use them. You agree that you will not remove, alter, or obscure any copyright, trademark, service mark, or other proprietary rights notices incorporated in or accompanying the SaaS.

9.2 Feedback. oneapp welcomes any recommendations, suggestions, ideas, or feedback you have about the SaaS (collectively, “Feedback”). You understand that oneapp owns all Feedback that you provide and you are not entitled to any compensation or reimbursement of any kind for providing Feedback to oneapp or in connection with oneapp’s use of Feedback. Please email your Feedback to oneapp at support@withoneapp.com.

9.3 Data Protection. Please read the oneapp Privacy Notice and the oneapp Data Protection Addendum carefully to understand how the SaaS collects, uses, and shares your information in connection with Merchant Services. With regard to the collection of personal information through the SaaS, a Merchant may act either as a controller or processor, and oneapp is a processor.

10. Arbitration Agreement

THIS SECTION 10 OF THE CONSUMER AGREEMENT WILL BE REFERRED TO AS THE “ARBITRATION AGREEMENT.”

PLEASE READ THE FOLLOWING SECTION CAREFULLY. IF YOU ARE DOMICILED IN THE UNITED STATES, IT REQUIRES YOU TO RESOLVE DISPUTES BETWEEN YOU AND ONEAPP ON AN INDIVIDUAL BASIS THROUGH ARBITRATION, PROHIBITS YOU FROM MAINTAINING OR PARTICIPATING IN A CLASS ACTION LAWSUIT, WAIVES YOUR RIGHT TO A JURY TRIAL, AND LIMITS THE TIME IN WHICH A CLAIM MAY BE BROUGHT. THIS SECTION OF THE CONSUMER AGREEMENT SHALL BE REFERRED TO AS THE “ARBITRATION AGREEMENT.”

10.1 Scope of Arbitration Agreement. If you reside in the United States, you agree that any and all disputes or claims that have arisen or may arise between you and oneapp or that relate in any way to the SaaS, including without limitation federal and state statutory claims, common law claims, and those based in contract, tort, fraud, misrepresentation,

or any other legal theory, shall be resolved exclusively through final and binding individual arbitration, rather than in court, except that you or we may assert claims in small claims court, so long as the matter remains in such court and advances only on an individual (non-class, non-representative) basis. This Arbitration Agreement is intended to be broadly interpreted.

10.2 IF YOU AGREE TO ARBITRATION WITH ONEAPP, YOU ARE AGREEING IN ADVANCE THAT YOU WILL NOT PARTICIPATE IN OR SEEK TO RECOVER MONETARY OR OTHER RELIEF IN ANY CLASS, COLLECTIVE, REPRESENTATIVE, AND/OR PRIVATE ATTORNEY GENERAL LAWSUIT, WHETHER AS A NAMED OR UNNAMED CLAIMANT. INSTEAD, BY AGREEING TO ARBITRATION, YOU MAY BRING YOUR CLAIMS AGAINST ONEAPP IN AN INDIVIDUAL ARBITRATION PROCEEDING ONLY, NOT BEFORE A JUDGE OR JURY.

10.3 Informal Resolution. You and oneapp agree that good-faith informal efforts to resolve disputes often can result in a prompt, low-cost, and mutually beneficial outcome. You and oneapp therefore agree that, before either you or oneapp demand individual arbitration against the other, we will personally meet and confer, via telephone or videoconference, in a good-faith effort to resolve informally any claim covered by this Arbitration Agreement. If you are represented by counsel, your counsel may participate in the conference, but you shall also personally attend the conference. The party initiating the dispute must give notice to the other party in writing of its, his, or her intent to initiate an informal dispute resolution conference, which shall occur within 60 days after the other party receives such notice, unless an extension is mutually agreed upon by the parties. To notify oneapp that you intend to initiate an informal dispute resolution conference, email oneapp at legalnotices@withoneapp.com, providing your name, telephone number associated with your account in the SaaS (if any), the email address associated with you or your account in the SaaS, and a description of your claim, including the amount of monetary relief (if any) you seek. In the interval between the party receiving such notice and the informal dispute resolution conference, the parties shall be free to attempt to resolve the initiating party’s claims. Compliance with the informal dispute resolution conference, including your personal participation, is a requirement that must be fulfilled before commencing individual arbitration or small claims proceedings. The statute of limitations, the one-year limitations period provided herein, and any filing fee deadlines shall be tolled beginning from the date of written notice of a dispute and while the parties engage in the informal dispute resolution process required by this paragraph. If the dispute has not been resolved within 120 days of written notice having been provided, tolling shall be suspended and such periods shall resume, unless otherwise mutually agreed in writing.

10.4 Arbitration Rules and Forum. This Arbitration Agreement is governed by the Federal Arbitration Act (“FAA”) in all respects. If for whatever reason the rules and procedures of the FAA cannot apply, the state law governing arbitration agreements in New York will apply in any arbitration proceedings, without regard to principles of conflict of laws. The arbitration will be administered by JAMS (www.jamsadr.com) pursuant to JAMS' Optional Expedited Arbitration Procedures. The arbitration will be determined in New York County, New York or at another mutually agreed location before one arbitrator. If the value of the relief sought is $10,000 or less, you or oneapp may elect to have the arbitration conducted by telephone or based solely on written submissions, which election shall be binding on you and oneapp subject to the discretion of the arbitrator(s) to require an in-person hearing, if the circumstances warrant. In cases where an in-person hearing is held, you and/or oneapp may attend by telephone, unless the arbitrator(s) require(s) otherwise. Any settlement offer made by you or oneapp shall not be disclosed to the arbitrator(s). Judgment on the Award may be entered in any court having jurisdiction.

10.5 It is the intent of the parties that, barring extraordinary circumstances, arbitration proceedings will be concluded within one hundred and twenty days from the date the arbitrator is appointed. The arbitrator may extend this time limit in the interests of justice. Failure to adhere to this time limit shall not constitute a basis for challenging the award.

10.6 The cost of the arbitration proceeding and any proceeding in court to confirm or to vacate any arbitration award, as applicable (including, without limitation, reasonable attorneys’ fees and costs), shall be borne by the unsuccessful party, as determined by the arbitrators, and shall be awarded as part of the arbitrator’s award. It is specifically understood and agreed that any party may enforce any award rendered pursuant to this arbitration provisions by bringing suit in any court of competent jurisdiction. The parties agree that the arbitrator shall have authority to grant injunctive or other forms of equitable relief to any party. This Arbitration Agreement shall survive the termination or cancellation of the Consumer Agreement.

10.7 Except as may be required by law, neither a party nor its representatives may disclose the existence, content, or results of any arbitration hereunder without the prior written consent of the other party. This clause shall not preclude parties from seeking provisional remedies in aid of arbitration from a court of appropriate jurisdiction.

10.8 At the time of commencement of an individual arbitration proceeding, in addition to complying with the rules JAMS' Optional Expedited Arbitration Procedures, you must send a “Demand for Arbitration” by certified mail to:

With One App, Inc. Attn: Legal Department,195 Plymouth Street, Suite 3/1, Brooklyn NY 11201

oneapp will send any Demand for Arbitration to you to the address associated with you or your account in the SaaS, as applicable; it is your responsibility to keep your address up to date.

10.9 To be valid, the Demand for Arbitration must contain all information called for in the applicable Demand for Arbitration form made available by JAMS, including the email address and phone number associated with you, or you account in the SaaS, a description of the nature and basis of the claims you are asserting, and the specific relief sought. Mass, group, collective, or consolidated notices of dispute are not permitted. In addition, if you have asked an attorney to submit your Demand for Arbitration for you, the notice also must include your signed statement authorizing oneapp to disclose private information about you (such as your account records and transaction history) to your attorney if necessary in resolving your claim. Your privacy is important to us and protected by law.

10.10 The individual arbitration shall be held in the county in which you reside or at another mutually agreed location. If the value of the relief sought is $10,000 or less, you or oneapp may elect to have the arbitration conducted by telephone or based solely on written submissions, which election shall be binding on you and oneapp subject to the discretion of the arbitrator(s) to require an in-person hearing, if the circumstances warrant. In cases where an in-person hearing is held, you and/or oneapp may attend by telephone, unless the arbitrator(s) require(s) otherwise. Any settlement offer made by you or oneapp shall not be disclosed to the arbitrator(s).

10.11 Arbitrator Powers. The arbitrator, and not any federal, state, or local court or agency, shall have exclusive authority to resolve any dispute relating to the interpretation, applicability, enforceability, or formation of this Arbitration Agreement, including, but not limited to any claim that all or any part of this Arbitration Agreement is void or voidable. All disputes regarding the payment of arbitrator or arbitration-organization fees, including the timing of such payments and remedies for nonpayment, shall be determined exclusively by an arbitrator, and not by any court. The arbitrator will decide the rights and liabilities, if any, of you and oneapp. Except as expressly agreed to in the Consumer Agreement, the arbitration proceeding will not be consolidated with any other matters or joined with any other proceedings or parties. The arbitrator will have the authority to grant motions dispositive of all or part of any claim or dispute. The arbitrator will have the authority to award, on an individual basis, monetary damages and to grant any non-monetary remedy or relief available to an individual under applicable law, the arbitral forum’s rules, and this Arbitration Agreement, but only

in favor of the individual party seeking relief and only to the extent necessary to provide relief warranted by that party's individual claim. The arbitrator will issue a written statement of decision describing the essential findings and conclusions on which any award (or decision not to render an award) is based, including the calculation of any damages awarded. The award shall benefit and be binding among only the individual parties to the arbitration and shall have no preclusive effect in any other arbitration or other proceeding involving a different party. The arbitrator(s) shall not be bound by rulings in prior arbitrations involving different Consumers, but is/are bound by rulings in prior arbitrations involving the same Merchant to the extent required by applicable law as if the matter had been litigated in a court in that jurisdiction. The arbitrator shall follow the applicable law. The arbitrator's decision is final and binding on you and oneapp. In the event a monetary award is not paid within 60 days, judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

10.12 Waiver of Jury Trial. YOU AND ONEAPP WAIVE ANY CONSTITUTIONAL AND STATUTORY RIGHTS TO SUE IN COURT AND RECEIVE A JUDGE OR JURY TRIAL. You and oneapp are instead electing to have claims and disputes resolved by arbitration, except as specified this Arbitration Agreement. There is no judge or jury in arbitration, and court review of an arbitration award is limited.

10.13 Waiver of Class or Consolidated Actions. EXCEPT AS EXPRESSLY AGREED TO IN THE CONSUMER AGREEMENT, YOU AND ONEAPP AGREE TO WAIVE ANY RIGHT TO RESOLVE CLAIMS WITHIN THE SCOPE OF THIS ARBITRATION AGREEMENT ON A CLASS, COLLECTIVE, REPRESENTATIVE, OR PRIVATE ATTORNEY GENERAL BASIS. ALL CLAIMS AND DISPUTES WITHIN THE SCOPE OF THIS ARBITRATION AGREEMENT MUST BE ARBITRATED ON AN INDIVIDUAL BASIS EXCEPT AS SET FORTH IN THIS ARBITRATION AGREEMENT. CLAIMS OF MORE THAN ONE CONSUMER OR USER CANNOT BE ARBITRATED OR LITIGATED JOINTLY OR CONSOLIDATED WITH THOSE OF ANY OTHER CONSUMER OR USER EXCEPT AS SET FORTH IN THE CONSUMER AGREEMENT. Subject to oneapp's consent, this provision does not prevent you from participating in a class-wide settlement of claims against oneapp.

10.14 Two Year Limitations Period. You agree that any claim against oneapp must be brought within two years of the date on which you first become aware, or reasonably should have become aware, of facts giving rise to such controversy, claim or dispute. You agree that this two-year limitations period is reasonable and that if you fail to provide notice of intent to initiate an informal dispute resolution conference within such time, your claim will be forever barred and may not be pursued against oneapp, either in arbitration or a court.

10.15 Opt Out. Within 30 days of first accepting the Consumer Agreement containing this Arbitration Agreement, you can choose to reject this Arbitration Agreement by mailing us a written opt-out notice. The opt-out notice must be postmarked no later than 30 days after the date you accept this Arbitration Agreement for the first time. You must mail the opt-out notice to:

With One App, Inc. Attn: Legal Department,195 Plymouth Street, Suite 3/1, Brooklyn NY 11201

or by contacting oneapp via email at legalnotices@withoneapp.com. The opt-out notice must include your name, address, phone number, and the email address(es) associated with you in the SaaS, and can only be submitted on behalf of yourself. You agree to maintain your own copy of any opt-out request that you mail to oneapp. Mass, group, collective, or consolidated opt-outs are not permitted. This procedure is the only way you can opt out of the Arbitration Agreement. If you opt out of this Arbitration Agreement, all other parts of the Consumer Agreement will continue to apply. Opting out of this Arbitration Agreement has no effect on any previous, other, or future arbitration agreements that you may have or may enter into with us. If you do not opt out of this Arbitration Agreement, but reject a future change to arbitration provisions, you agree that you will individually arbitrate any dispute in accordance with the language of this version of the Arbitration Agreement.

10.16 Severability and Survival. If, after exhaustion of all appeals, any of these prohibitions on non-individualized relief, class, collective, representative, private attorney general, or consolidated relief is found to be unenforceable with respect to a particular claim or with respect to a particular request for relief (such as a request for public injunctive relief), then the parties agree that such a claim or request for relief shall be decided by a court after all other claims and requests for relief are arbitrated. This Arbitration Agreement survives any termination of the Consumer Agreement.

10.17 Court Proceedings. Subject to and without waiver of the Arbitration Agreement, you and we each submit to exclusive personal jurisdiction and agree that any judicial proceedings (other than small claims actions) will be brought in the federal or state courts of the state of Delaware.

11. Interactions with Merchant Services and Third Party Services

11.1 The oneapp website and the SaaS platform contains links to Merchant Services and Third Party Services. When you click or tap on a link to Merchant Services and Third Party Services, the SaaS may not warn you that you have left the oneapp’s website or the SaaS, and may not warn you that you are subject to the terms and conditions (including privacy policies) of another website, service or destination. Such

Merchant Services and Third Party Services are not under the control of oneapp. oneapp is not responsible for any Merchant Services and Third Party Services. oneapp provides links to these Merchant Services and Third Party Services only as a convenience and does not warrant or make any representations with respect to such Merchant Services and Third Party Services. You use all links in Merchant Services and Third Party Services at your own risk. You should review applicable terms and policies, including privacy and data gathering practices, of any Merchant Services and Third Party Services, and make whatever investigation you feel necessary or appropriate before proceeding with any off-platform transaction with any Merchant or Third Party.

12. Warranty Disclaimer

12.1 UNITED STATES FEDERAL LAW AND SOME STATES ND OTHER JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF CERTAIN IMPLIED WARRANTIES, SO SOME OF THE EXCLUSIONS IN THIS SECTION 12 MAY NOT APPLY TO YOU. THIS SECTION 12 APPLIES TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW. THE SAAS ARE PROVIDED “AS IS,” AND ONEAPP MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND ONEAPP SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT TO THE FULLEST EXTENT PERMITTED BY LAW.

13. Indemnification

13.1 You will defend oneapp and oneapp’s officers, directors, employees, and affiliated entities (collectively, “oneapp Indemnified Parties”) from and against any claim, demand, suit, or proceeding made or brought against a oneapp Indemnified Party by a third party alleging or arising out of your use of the SaaS (“Claim”). You will indemnify oneapp from any damages, fines or penalties imposed by a government or regulatory body, attorneys’ fees, and costs awarded against a oneapp Indemnified Party or for settlement amounts approved by you for a Claim.

13.2 oneapp reserves the right, at its own expense, to participate in the defense of any Claim. You will not do the following without oneapp’s prior written consent: (a) settle any Claims for which you have an obligation to indemnify pursuant to this Section 8 or (b) admit to liability or fault or create any obligation on behalf of oneapp as part of a settlement of a Claim.

14. Limitation of Liability

14.1 This Section 9 applies to the fullest extent permitted by applicable law, and some provisions in this Section 9 may not apply in certain jurisdictions. You understand and

agree that a key element of the SaaS and the Consumer Agreementt is your and our mutual desire to keep the SaaS simple and efficient and to provide the SaaS at low cost. You understand and agree to the limitations on remedies and liabilities set forth in this Section 9 to keep the SaaS simple and efficient, and costs low, for all Consumers.

14.2 Cap on Liability. NOTWITHSTANDING ANYTHING TO THE CONTRARY IN THIS CONSUMER AGREEMENT, ONEAPP'S AGGREGATE LIABILITY TO YOU OR ANY THIRD PARTY ARISING OUT OF THIS CONSUMER AGREEMENT OR OTHERWISE IN CONNECTION WITH the SAAS WILL IN NO EVENT EXCEED THE GREATER OF AMOUNTS ACTUALLY PAID BY AND/OR DUE FROM YOU TO ONEAPP IN THE SIX (6) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH CLAIM.. YOU ACKNOWLEDGE AND AGREE THAT THE ESSENTIAL PURPOSE OF THIS SECTION 9 IS TO ALLOCATE THE RISKS UNDER THIS CONSUMER AGREEMENT BETWEEN THE PARTIES AND ONEAPP HAS RELIED ON THESE LIMITATIONS IN DETERMINING WHETHER TO PROVIDE YOU THE RIGHTS TO ACCESS AND USE the SAAS.

14.3 Disclaimer of Certain Damages. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, ONEAPP SHALL NOT BE LIABLE TO YOU OR ANYONE ELSE FOR ANY INDIRECT, PUNITIVE, SPECIAL, EXEMPLARY, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES OF ANY TYPE OR KIND (INCLUDING PERSONAL INJURY, LOST PROFITS, PAIN AND SUFFERING, EMOTIONAL DISTRESS, AND LOSS OF DATA, REVENUE, USE, AND ECONOMIC ADVANTAGE). **THE FOREGOING DISCLAIMER OF PUNITIVE AND EXEMPLARY DAMAGES, AND THE ENTIRE DISCLAIMER OF DAMAGES FOR PERSONAL INJURY OR PROPERTY DAMAGE, OR FOR ANY INJURY CAUSED BY ONEAPP'S FRAUD OR FRAUDULENT MISREPRESENTATION, SHALL NOT APPLY TO USERS WHO RESIDE IN THE STATE OF NEW JERSEY IN THE UNITED STATES.**

15. Term, Termination and Survival

15.1 You may terminate these Consumer Agreement at any time, for any or no reason, by immediately ceasing your use of the SaaS. If you commence using the SaaS again, you are consenting to these Consumer Agreement. oneapp may, in its sole discretion, suspend or terminate these Consumer Agreement immediately (a) if oneapp suspects you are in breach of these Consumer Agreement; (b) if oneapp determines that you are engaged in activity that is suspected or actually fraudulent, illegal or otherwise malicious or fails to comply with applicable law; or (c) to prevent harm to the security, stability, availability, or integrity of oneapp. oneapp reserves the right to take appropriate legal action, including without limitation, pursuing civil, criminal, or injunctive redress. Even after your right to use the SaaS is terminated, the Consumer Agreement will remain

enforceable against you. All provisions which by their nature should survive to give effect to those provisions shall survive the termination of the Consumer Agreement.

16. General

16.1 Relationship. No joint venture, partnership, employment, or agency relationship exists between you, oneapp, or any third party as a result of the Consumer Agreement or use of the SaaS.

16.2 Choice of Law. Without giving effect to any principles that provide for the application of the law of any other jurisdiction, the Consumer Agreement is governed by the laws of the State of Delaware consistent with the Federal Arbitration Act, except where prohibited by applicable law.

16.3 Consumer Complaints. If you have a complaint about the SaaS or Merchant Services, please email oneapp at support@withoneapp.com. For Consumers domiciled in the United States Consumers who are residents of the State of California, and in accordance with California Civil Code § 1789.3, you may also contact the Complaint Assistance Unit of the Division of Consumer Services of the California Department of Consumer Affairs in writing at 1625 North Market Blvd., Suite N 112, Sacramento, CA 95834 or by telephone at (800) 952-5210.

16.4 Notice. Where oneapp or the SaaS requires that you provide an email address, you are responsible for providing oneapp with your most current email address. In the event that the last email address you provided to oneapp or the SaaS is not valid, or for any reason is not capable of delivering to you any notices required or permitted by the Consumer Agreement, oneapp's dispatch of the email containing such notice will nonetheless constitute effective notice. You agree that all agreements, notices, disclosures, payment or renewal notifications, and other communications that oneapp provides to you electronically (such as through email or posting through the SaaS, including in your oneapp account) satisfy any legal requirement that such communications be in writing or be delivered in a particular manner. You agree that you have the ability to store such electronic communications such that they remain accessible to you in an unchanged form. You may give notice to oneapp by emailing support@withoneapp.com. Such notice shall be deemed given on the next business day after such notice is actually received by oneapp.

16.5 Currency. Unless otherwise indicated, all prices and other amounts displayed through the SaaS are in U.S. Dollars.

16.6 Use Only Where Legally Allowed. You shall not access or use any portion of the SaaS if you are not legally allowed to do so where you are located.

16.7 Severability. In the event that any provision of the Consumer Agreement is held by a court or other tribunal of competent jurisdiction to be unenforceable, such provision will be limited or eliminated to the minimum extent necessary to render such provision enforceable and, in any event, the remainder of the Consumer Agreement will continue in full force and effect.

16.8 Entire Agreement. The Consumer Agreement (including all exhibits and attachments hereto) will constitute the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior and contemporaneous understandings, proposals, statements, sales materials, presentations, or non-disclosure or other agreements, whether oral or written. No oral or written information or advice given by oneapp, its agents, or its employees will create a warranty or in any way increase the scope of the warranties or obligations in the Consumer Agreement.

Applicant Disclosure for the Procurement of Consumer Reports

The Merchant inviting you to submit your application for Merchant's rental housing listing through oneapp may request consumer reports, as defined by the federal Fair Credit Reporting Act ("FCRA"), about you from a consumer reporting agency in connection with your application and for purposes of contracting a rental housing lease. A consumer report is a compilation of information that might affect your ability to contract for the Merchant's listing. These reports may contain information about your character, general reputation, personal characteristics and mode of living. The reports may also contain information about you relating to your criminal history, credit history, or employment history, or other background checks.

California Residents
If you are a resident of California, the Merchant may request background information about you from a consumer reporting agency that California's Investigative Consumer Reporting Agencies Act ("ICRAA") defines as an "investigative consumer reporting agency" in connection with your above-mentioned application and for purposes of contracting a rental housing lease. The ICRAA defines these consumer reports as an "investigative consumer report." These reports may contain information about your character, general reputation, personal characteristics and mode of living. The reports may also contain information about you relating to your criminal history, credit history or employment history, or other background checks. The reports may involve personal interviews with sources such as your neighbors, friends or associates.

Authorization for Background Check

I have carefully read and understand the Applicant Disclosure for the Procurement of Consumer Reports. By executing this document or clicking to “accept” when prompted in the oneapp software as a service, I authorize Merchant (as defined in the Consumer Agreement) to share the contents of this consumer report or investigative consumer report with its partners and clients in an effort to place me into rental housing under a lease contracted with those partners. Merchant will only share the background report as necessary, and as authorized, for this sole purpose. I understand that if I successfully contract for a lease with Merchant’s partners, my consent will apply, and Merchant may obtain reports throughout my lease contract where state law allows. I also understand that the information contained in my application or otherwise disclosed by me before or during my lease contract, if any, may be used for the purpose of obtaining consumer reports and/or investigative consumer reports. By executing this document or clicking to “accept” when prompted in the oneapp software as a service, I authorize law enforcement agencies, information service bureaus, credit bureaus, record/data repositories, courts (federal, state and local), motor vehicle records agencies, my past or present employers, the military, and other individuals and sources to furnish any and all information on me that is requested by the consumer reporting agency. If applicant is younger than 18 years old, a Legal Guardian must provide his/her own email address and execute or otherwise accept this document.

I authorize Merchant to contact my current employer if necessary, to verify my current employment status on and after the date of this Authorization for Background Check.

Contact Merchant at the information they have provided you to receive a free copy of any Consumer Report or Investigative Consumer Report.

Acceptable Use Policy

This Acceptable Use Policy (“*AUP*”) describes rules that apply to any party (“*you*”, “*your*”, “*yours*”, or “*Merchant*”) using software as a service applications developed by oneapp or any its affiliates, provided on or through the oneapp platform as applicable (“*SaaS*”), and any user of the SaaS, including via any software application, products, or services provided by Merchant (“*End User*”). oneapp together with its affiliates will be referred to as *"*oneapp*"* in this AUP. The prohibited conduct in this AUP is not exhaustive. Merchant is responsible for its End Users’ compliance with this AUP. If Merchant or any End User violates this AUP, oneapp may suspend Merchant’s and End User’s use of the SaaS. This AUP may be updated by oneapp from time to time upon reasonable notice, which may be provided via End User’s account, email, or by posting an updated version of this AUP at https://legal.withoneapp.com.

No Inappropriate Content or Users. Do not use the SaaS to transmit or store any content or communications (commercial or otherwise) that is illegal, harmful, unwanted, inappropriate, or objectionable, including, but not limited to, content or communications

which oneapp determines (a) is false or inaccurate; (b) is hateful or encourages hatred or violence against individuals or groups; or (c) could endanger public safety. This prohibition includes use of the SaaS by a hate group. Merchant and its End Users are also prohibited from using the SaaS to promote, or enable the transmission of or access to, any prohibited content or communications described in this paragraph.

Prohibited Activities. Do not use the SaaS to engage in or encourage any activity that is illegal, deceptive, harmful, a violation of others' rights, or harmful to oneapp's business operations or reputation, including:

- **Violations of Laws or Standards.** Violating laws, regulations, governmental orders, industry standards, or telecommunications providers' requirements or guidance in any applicable jurisdiction, including any of the foregoing that require (a) consent be obtained prior to transmitting, recording, collecting, or monitoring data or communications or (b) compliance with opt-out requests for any data or communications.
- **Interference with the SaaS.** Interfering with or otherwise negatively impacting any aspect of the SaaS or any third-party networks that are linked to the SaaS.
- **Reverse Engineering.** Reverse engineering, copying, disassembling, or decompiling the SaaS.
- **Falsification of Identity or Origin.** Creating a false identity or any attempt to mislead others as to the identity of the End User or the origin of any data or communications.

No Service Integrity Violations. Do not violate the integrity of the SaaS, including:

- **Bypassing Service Limitations.** Attempting to bypass, exploit, defeat, or disable limitations or restrictions placed on the SaaS.
- **Security Vulnerabilities.** Finding security vulnerabilities to exploit the SaaS or attempting to bypass any security mechanism or filtering capabilities.
- **Disabling the SaaS.** Any denial of service (DoS) attack on the SaaS or any other conduct that attempts to disrupt, disable, or overload the SaaS.
- **Harmful Code or Bots.** Transmitting code, files, scripts, agents, or programs intended to do harm, including viruses or malware, or using automated means, such as bots, to gain access to or use the SaaS.
- **Unauthorized Access.** Attempting to gain unauthorized access to the SaaS.

Data Safeguards. Merchant is responsible for determining whether the SaaS offers appropriate safeguards for Merchant's use of the SaaS, including, but not limited to, any safeguards required by applicable law or regulation, prior to transmitting or processing, or prior to permitting End Users to transmit or process, any data, communications or transactions via the SaaS.

SaaS and Area Specific Requirements. Additional requirements for specific (a) SaaS applications, including requirements for geographic areas, and (b) SaaS that are purchased from oneapp, but provided, or otherwise made available, by a third party are, in either case, set forth at https://legal.withoneapp.com and apply solely to the extent End User uses those specific (i) SaaS or (ii) third-party products and services.

Violations of this AUP, including any prohibited content or communications, may be reported to support@withoneapp.com. End User agrees to immediately report any violation of this AUP to oneapp and provide cooperation, as requested by oneapp, to investigate and/or remedy that violation.

SaaS and Area Specific Requirements

Merchant's use of the SaaS is subject to Merchant's compliance with the SaaS and Area Specific Requirements below (collectively, "*Requirements*") to the extent applicable.

If any of the following terms are used but not defined within a Requirement below, they will have the meanings set forth in the oneapp Acceptable Use Policy ("*AUP*"): "*you*", "*your*", "*yours*", "*Merchant*", "*oneapp*", "*End User*", and "*SaaS.*" oneapp may update or modify these Requirements from time to time. The updated version of these Requirements will be available at https://legal.withoneapp.com, which the End User deems as reasonable and sufficient notice for such updates and modifications. End User's continued use of the SaaS constitutes End User's acceptance of the updated or modified Requirements. oneapp recommends that End User periodically reviews these Requirements.

These Requirements are part of the AUP.

SaaS Specific Requirements

The SaaS Specific Requirements for a particular SaaS application apply solely to the extent Merchant and its End Users use the identified SaaS or services in the agreements linked below.

- Asset, Income and Employment Verification SaaS
- Email SaaS Policy
- End User Attestations
- Identity Verification SaaS
- Messaging SaaS Policy
- Payment SaaS
- SaaS in Private Beta
- SaaS using Phone Numbers
- Screening SaaS

Third Party Services

The third party services set forth below are offered to you and your End Users through the SaaS ("*Third Party Services*"). If End User purchases or uses any Third Party Services, such Third Party Services are solely provided by the applicable third party set forth below ("*Third Party Provider*"). Your use of any Third Party Services is subject to the applicable Third Party Provider's terms set forth below ("*Third Party Terms*"). oneapp is not a party to any Third Party Terms and is not liable for any Third Party Services whatsoever.

Third Party Services:	**Third Party Provider:**	**Third Party Terms:**
Equifax ACROFILE and ACROFILEPlus	Equifax Information Services LLC	Qualified Subscriber Terms and Conditions
VantageScore v3.v4	Equifax Information Services LLC	Qualified Subscriber Terms and Conditions

Area Specific Requirements

The Area Specific Requirements for a particular geographic area apply solely to the extent Merchant and End Users use the SaaS in the identified area, regardless of where Merchant is located, domiciled, or doing business in such area.

Asset Income and Employment Verification SaaS

These oneapp Asset Income and Employment Verification requirements ("*AIEV Requirements*") will apply to Merchant and its End Users use of the AIEV SaaS (as defined below).

Any capitalized term not defined in the AIEV SaaS Terms will have the meaning provided in the Terms of Service.

1. Definitions

"*Asset, Income and Employment Verification Data*" means certain data attributes returned to a Merchant by a Consumer through the AIEV SaaS.

"*AIEV SaaS*" means oneapp's cloud platform for Consumers to self-verify personal assets, income, and employment, authenticated by a third party processor under the direction and control of Consumer, and delivered to Merchant as AIEV Data.

2. Permitted Uses

2.1 Merchant may use the AIEV SaaS solely to allow Consumers to validate personal identity for the purpose of preventing fraud, or errors in Merchant Data, and for no other purpose.

3. Restrictions

3.1 Merchant will not use the AIEV SaaS or AIEV Data (a) for marketing purposes or to sell products or services; (b) to create a consumer report or allow use by a consumer reporting agency for the purpose of creating a consumer report; or (c) for verifying worthiness or eligibility for credit, insurance, or employment.

4. Application, Use Case Attestation and Approval

4.1 If applicable, Merchant must submit an application in the form of a use case attestation to certain data service providers, which sets forth a true, accurate, and complete description of Merchant's business and intended use case(s) for the AIEV SaaS, and which complies with Section 2 of these Identity Verification Requirements. Merchant's use of the Screening SaaS is subject to the applicable data service provider(s) review and approval of Merchant's use case attestation. For the avoidance of doubt, oneapp has no control over a data service provider(s) approval of Merchant's

application. Merchant is not entitled to any refunds or credits if: (a) a data service provider(s) rejects Merchant's use case attestation; or (b) Merchant's application contains information that is untrue, inaccurate, or incomplete. Merchant will not use the AIEV SaaS for any use case that is not approved by the applicable data service provider(s). If Merchant wants to modify its approved use case(s), Merchant must submit a new application for such modified use case(s) for approval.

5. Representations and Warranties

5.1 By Consumer. Consumer represents and warrants that: (a) Consumer's personal asset, income, and employment information is under the control of Consumer's control; (b) the software application provided by oneapp's sub-processor for the IEAV SaaS cannot access or otherwise process Consumer's IEAV Data without initiation, instruction and control by Consumer; (c) Consumer will assemble and evaluate IEAV Data for completeness and accuracy prior to furnishing IEAV Data to Merchant; (d) Consumer will only furnish IEAV Data to Merchant that Consumer confirms to be complete and accurate; and (e) if Consumer believes that any IEAV data is incomplete or inaccurate, Consumer will immediately notify oneapp via email support@withoneapp.com to investigate the issue.

Email SaaS Policy

This oneapp Email SaaS Policy ("*Email SaaS Policy*") applies to oneapp Email SaaS ("*oneapp Email Saas*"). This Email SaaS Policy provides the restrictions and requirements you must abide by to use the oneapp Email SaaS. This Email SaaS Policy applies to you and your organization, end users, and customers, and any references to "you" in this Email SaaS Policy includes your organization, end users, and customers. These restrictions and requirements ensure that all emails sent via the oneapp Email SaaS are safe, wanted, and legal.

This Email SaaS Policy applies in addition to, and forms part of, oneapp's Acceptable Use Policy, which you are encouraged to read.

Affirmative Consent ("opt-in") Requirements

Except for transactional emails (i.e., non-marketing emails that contain information about an action or transaction a recipient has taken or agreed to and, if applicable, updates or notifications to that recipient about that action or transaction), you must obtain affirmative consent prior to sending any emails to a recipient via the oneapp Email SaaS. Any affirmative consent must be freely given by each recipient to each

sender (e.g., blanket consents or consents provided on behalf of a third party are not acceptable), informed, and unambiguous. This means a recipient must be (a) presented with the choice to provide or withhold consent; (b) informed of the sender's identity (see Sender Identification paragraph below), how its email address will be used, and the subject matter of the emails it will receive; and (c) made aware of how to withdraw, at any time, any previously provided affirmative consent. You must obtain affirmative consent from a recipient again if you send that recipient an email after an extended period of non-engagement.

Any affirmative consent that you obtain from a recipient is strictly for the subject matter for which that recipient provided that affirmative consent. Please also note that any affirmative consent that you obtain is not transferable to your affiliates or any other party.

You are required to retain proof of all affirmative consents obtained from recipients at least until the recipient withdraws its affirmative consent. Upon written request from oneapp, you must promptly provide proof of a recipient's affirmative consent and the date and the method through which that recipient's email address was obtained.

Sender Identification Requirements

Each email that you send via the oneapp Services must (a) clearly identify and accurately represent the sender (i.e., the party that obtained the affirmative consent from a recipient or the party that is initiating the transmission of the email) and (b) include a clear non-deceptive subject line, which accurately describes the content and purpose of the email (e.g., if the email is an advertisement or a promotion, the subject line should clearly reflect this).

Revocation of Affirmative Consent ("opt-out") Requirements

Except for transactional emails (as defined above), the body of each email that you send via the oneapp Services must include (a) an active and accurate physical mailing address where a recipient can send an unsubscribe request via mail; (b) clear, conspicuous, and functioning unsubscribe hyperlink; and (c) a hyperlink to your privacy policy applicable to the emails you send.

A recipient must have the ability to revoke its affirmative consent at any time. You must honor all affirmative consent withdrawal requests within (10) days of the date they are sent, or the timeframe required under applicable law or regulation, whichever is shorter. You may not send emails to a recipient that has withdrawn its affirmative consent, unless that recipient provides its subsequent affirmative consent. This paragraph does not apply to transactional emails (as defined above).

Prohibited Content

The following content is prohibited from being sent via the oneapp Email SaaS:

- Pornography or sexually explicit content;
- Escort services, mail-order bride or spouse finders, international marriage brokers, and other similar services;
- Statements about products claiming to prevent, treat, or cure health issues (e.g., illness or disease) that have not been approved by the applicable government authority or are not permitted under applicable law or regulation;
- Advertising for prescription medication that cannot legally be sold over-the-counter; and
- Content that is fraudulent or that oneapp determines in good faith is intended to mislead a recipient (e.g., phishing emails, chain letters, pyramid schemes) or cause harm or damage (e.g., malware or viruses).

Prohibited Actions

You are prohibited from using the oneapp Email SaaS in the following ways:

- Sending unsolicited or unwanted emails in bulk;
- Sending emails to email addresses that you obtained from the Internet or social media or to generic email aliases (e.g., webmaster@domain.com or info@domain.com) without obtaining prior affirmative consent;
- Using third-party email addresses and domain names without proper consent or authorization from the third party;
- Using or embedding tracking technologies (e.g., tracking pixels or cookies) in emails sent to a recipient prior to obtaining consent from that recipient to the extent and in the manner required by applicable law or regulation;
- Using purchased or rented email lists or email lists of recipients that have not affirmatively consented to receive emails from you;
- Using techniques or practices to evade mechanisms, filters (e.g., spam filters), and detection capabilities (e.g., anti-abuse or spam detection mechanisms) designed to identify unsolicited or unwanted emails, including, but not limited to, snowshoeing (i.e., sending spam emails across multiple domains or IP addresses to dilute reputation metrics and evade filters) and waterfalling (i.e., list

owner “waterfalls” the same illicitly obtained address list through a series of (usually) unknowing, innocent email service providers. Each time they clean out bounces, complainants and maybe non-respondents, with the end goal being to send the final result through a good email service provider with solid deliverability);

- Disguising, falsifying, or manipulating the subject matter, header, or transmission path information of any email; and

- Conducting security testing, including simulated phishing and other activities that may resemble social engineering or similar attacks.

Deliverability and oneapp Email SaaS Performance Risks

Sending certain emails may result in email deliverability issues or negatively affect the performance of the oneapp Email SaaS or oneapp’s business reputation, any one of which may constitute a violation of this Email SaaS Policy, as determined by oneapp, on a case-by-case basis. These include, but are not limited to, sending emails that result in (a) complaints from third parties (e.g., complaints from inbox providers or law enforcement agencies) or an unreasonable number of complaints from recipients (e.g., complaints of spam or similar complaints) or (b) excessive block listings or listings that exceed a reasonable period of time to resolve.

Age Gating

If you are sending emails related to content intended for adults that is not prohibited under this Email SaaS Policy, then you must verify that a recipient is at least of legal age to provide affirmative consent to receive such an email based on where that recipient is located. Upon written request from oneapp, you will provide proof of the age gating mechanisms that are in place.

Creation of Excess Accounts

You are prohibited from creating an excessive number of oneapp Email SaaS accounts for the purposes of circumventing oneapp’s internal controls. In general, accounts are limited to one paid oneapp Email SaaS account per customer with the ability to (a) allow multiple users to use the oneapp Email SaaS from a single account and (b) segregate email sending and API activity.

Unauthorized Access and Access Removal

You will use reasonable efforts to (a) prevent unauthorized access to your oneapp Email SaaS account and the oneapp Email SaaS and (b) detect and remove your end users and customers who violate this Email SaaS Policy in connection with their use of the oneapp Email SaaS.

End User Attestations

The table below outlines each attestation ("*Attestation*") and the specific services that are covered by the corresponding Attestation ("*Covered Services*"). Any capitalized term used but not defined below will have the meaning provided in the corresponding Attestation.

Attestation:	**Attesting End User:**	**Covered Services:**
Qualified Subscriber Attestation	Merchant	Screening SaaS and Third Party Services

Qualified Subscriber Attestation for Third Party Services

This Qualified Subscriber Attestation for Third Party Services ("QSA") is effective on the Last Updated date written above.

PLEASE REVIEW THIS QSA CAREFULLY. ONCE ACCEPTED, THE QSA BECOMES A BINDING LEGAL COMMITMENT BETWEEN YOU AND ONEAPP. IF YOU DO NOT AGREE WITH THE QSA, YOU SHOULD NOT ACCEPT THEM, USE THE SCREENING SAAS OR THE THIRD PARTY SERVICES, OR OTHERWISE AGREE TO THEM.

Instructions for Submission

The QSA is completed as your declaration of Merchant's assessment against the combined data security standards of nationwide consumer reporting agencies that do business as Equifax, Experian and TransUnion ("Consumer Reporting Industry Data

Security Standard" or "CRI DSS") Requirements and Credentialing Procedures ("Assessment").

The QSA incorporates information and authorization from Merchant's SaaS account and the associated order or written Order Form (collectively, "Order"). The completed QSA reflects the results documented in an associated Qualified Subscriber Report ("QSR").

oneapp uses the completed QSA and associated QSR to enroll Merchant as a Qualified Subscriber to Third Party Services, and ensure Merchant's compliance with Assessments required of Merchant to access the Screening SaaS and Third Party Services.

The completed QSA and associated QSR is Merchant's confidential information, and may be used by oneapp solely for the purposes described in the QSA or as otherwise authorized by Merchant.

Definitions

"*Qualified Subscriber*" is a Merchant that successfully completes the Assessment to access the Screening SaaS, and Third Party Services that provide consumer reports and related information.

"*Company Principal"* is an owner, founder, CEO, or a senior representative of Merchant. Principals are subject to background checks, which may be performed during initial and subsequent Assessments.

"*Assessment Contact*" is an individual familiar with Merchant's use of Screening SaaS and Third Party Services, and will serve as a primary contact for inquiries related to Assessments, and Merchant's use of Screening SaaS and Third Party Services.

"*Company Attestor*" is an individual authorized by Merchant to provide the information in the QSA, and certify on behalf of Merchant the information provided is accurate and the QSA is complete.

Capitalized terms used but not otherwise defined in this document have the meanings provided in the Terms of Service

Merchant Acknowledgement and Certification

Company Attestor is Merchant's undersigned authorized representative to the Merchant's Order. Company Attestor certifies (Select all that apply):

☑ Company Attestor is authorized to provide the information in the QSA, has provided accurate information, certifies the QSA is complete, and has knowledge

of Merchant's business and intended use of consumer report data sufficient to make this certification;

☑ The Merchant Application was completed according to CRI DSS, and was completed according to instructions therein;

☑ CRI DSS requirements and controls will be maintained at all times, as applicable to Merchant.

Merchant Attestation

This attestation is made by Company Attestor on behalf of Merchant, contemporaneous with the effective date of Merchant's Order.

Section 1 Merchant Application

Merchant has completed each of the Application Fields below with information referenced in Merchant's Order.

Part 1. Company Contact	
Application Fields	**Provided in Order Fields**
Company Name:	Name of Merchant's Business Entity
Company Website:	Merchant's Website
Company Physical Address:	Merchant's Business Address
Company Phone:	Billing Contact Phone
Company Email:	Billing Contact Email
Part 2. Company Principal	
Application Fields	**Provided in Order Fields**
Company Principal Name:	Printed Name, Merchant Authorized Representative
Company Principal Title:	Title, Merchant Authorized Representative
Part 3. Assessment Contact	
Application Fields	**Provided in Order Fields**
Assessment Contact Name:	Inspection Contact Name

Assessment Contact Phone:	Inspection Contact Phone
Assessment Contact Email:	Inspection Contact Email
Part 4. Company Attestor	
Application Fields	**Provided in Order Fields**
Company Attestor Name:	Printed Name, Merchant Authorized Representative
Company Attestor Title:	Title, Merchant Authorized Representative
Company Attestor Signature:	Signature, Authorized Representative
Part 5. Company Business Information	
Application Fields	**Provided Below**
Business License/Registration Issuer:	Secretary of State
Regulatory Agency:	State of Organization, Merchant's Business Address
License Number:	File Number, Secretary of State
Industry:	Real Estate
Nature of Business:	Real Estate Sales & Rentals
Company Physical Address is Residential:	No
Company Shares Office Space with Other Company or Entity:	No
Company Consumes Consumer Report Data:	Yes
Permissible Purpose:	For a legitimate business need tied to a transaction initiated by the consumer: Tenant screening.
Company has operations or agents outside US:	No

Identity Verification SaaS

These oneapp Identity Verification requirements ("*Identity Verification Requirements*") will apply to Merchant and End Users use of the IDV SaaS (as defined below).

Any capitalized term not defined in the Identity Verification SaaS Terms will have the meaning provided in the Terms of Service.

1. Definitions

"*Identity Verification Data*" means certain data attributes returned to a Merchant by a Consumer through the IDV SaaS.

"*IDV SaaS*" means oneapp's cloud platform for Consumers to automatically self-verify personal identity, authenticated by a third party processor under the direction and control of Consumer, and delivered to Merchant as Identity Verification Data.

2. Permitted Uses

2.1 Merchant may use the IDV SaaS solely to allow Consumers to validate personal identity for the purpose of preventing fraud, or errors in Merchant Data, and for no other purpose.

3. Restrictions

3.1 Merchant will not use the IDV SaaS or Identity Verification Data (a) for marketing purposes or to sell products or services; (b) to create a consumer report or allow use by a consumer reporting agency for the purpose of creating a consumer report; or (c) for verifying worthiness or eligibility for credit, insurance, or employment.

4. Application, Use Case Attestation and Approval

4.1 If applicable, Merchant must submit an application in the form of a use case attestation to certain data service providers, which sets forth a true, accurate, and complete description of Merchant's business and intended use case(s) for the IDV SaaS, and which complies with Section 2 of these Identity Verification Requirements. Merchant's use of the Screening SaaS is subject to the applicable data service provider(s) review and approval of Merchant's use case attestation. For the avoidance of doubt, oneapp has no control over a data service provider(s) approval of Merchant's application. Merchant is not entitled to any refunds or credits if: (a) a data service provider(s) rejects Merchant's use case attestation; or (b) Merchant's application contains information that is untrue, inaccurate, or incomplete. Merchant will not use the IDV SaaS for any use case that is not approved by the applicable data service

provider(s). If Merchant wants to modify its approved use case(s), Merchant must submit a new application for such modified use case(s) for approval.

5. Representations and Warranties

5.1 By Consumer. Consumer represents and warrants that: (a) Consumer's personal asset, income, and employment information is under the control of Consumer's control; (b) the software application provided by oneapp's subprocessor for the IDV SaaS cannot access or otherwise process Consumer's IDV Data without initiation, instruction and control by Consumer; (c) Consumer will assemble and evaluate IDV Data for completeness and accuracy prior to furnishing IDV Data to Merchant; (d) Consumer will only furnish IDV Data to Merchant that Consumer confirms to be complete and accurate; and (e) if Consumer believes that any IDV data is incomplete or inaccurate, Consumer will immediately notify oneapp via email support@withoneapp.com to investigate the issue.

Messaging SaaS Policy

This oneapp Messaging SaaS Policy applies to SMS, MMS, Chat, and WhatsApp messaging channels. We all expect that the messages we *want* to receive will reach us, unhindered by filtering or other blockers. An important step oneapp and our customers can take to make that expectation reality is to prevent and eliminate *unwanted* messages. Towards that end, we strive to work with our customers so that messages are sent with the consent of the message recipient, and that those messages comply with applicable laws, communications industry guidelines or standards, and measures of fairness and decency.

This principle is central to oneapp's Acceptable Use Policy.

oneapp Messaging SaaS

oneapp treats all messaging transmitted via oneapp's platform - regardless of use case or phone number type (*e.g.,* long code, short code, or toll-free) - as Application-to-Person (A2P) messaging. All A2P messages originating from oneapp's platform are subject to this oneapp Messaging SaaS Policy, which covers rules and /or prohibitions regarding:

- Consent ("opt-in");
- Revocation of Consent ("opt-out");

- Sender Identification;
- Messaging Usage;
- Filtering Evasion; and
- Enforcement.

This policy applies to all customers who use oneapp's messaging channels. If you provide your own end users or clients with the ability to send messages through oneapp, for example as an ISV ("*Independent Software Vendor*"), you are responsible for the messaging activity of these users. You must ensure that any messaging activity generated by your users is in compliance with oneapp policies.

Consent/Opt-in

What Is Proper Consent?

Consent can't be bought, sold, or exchanged. For example, you can't obtain the consent of message recipients by purchasing a phone list from another party.

Aside from two exceptions noted later in this section, you need to meet each of the consent requirements listed below. If you are a software or platform provider using oneapp's platform for messaging within your application or service, you must require your customers to adhere to these same requirements when dealing with their users and customers.

Consent Requirements

- Prior to sending the first message, you must obtain agreement from the message recipient to communicate with them - this is referred to as "consent", you must make clear to the individual they are agreeing to receive messages of the type you're going to send. You need to keep a record of the consent, such as a copy of the document or form that the message recipient signed, or a timestamp of when the customer completed a sign-up flow.
- If you do not send an initial message to that individual within a reasonable period after receiving consent (or as set forth by local regulations or best practices), then you will need to reconfirm consent in the first message you send to that recipient.
- The consent applies only to you, and to the specific use or campaign that the recipient has consented to. You can't treat it as blanket consent allowing you to

send messages from other brands or companies you may have, or additional messages about other uses or campaigns.

- Proof of opt-in consent should be retained as set forth by local regulation or best practices after the end user opts out of receiving messages.

Alternative Consent Requirements

While consent is always required and the consent requirements noted above are generally the safest path, there are two scenarios where consent can be received differently.

Contact initiated by an individual

If an individual sends a message to you, you are free to respond in an exchange with that individual. For example, if an individual texts your phone number asking for your hours of operation, you can respond directly to that individual, relaying your open hours. In such a case, the individual's inbound message to you constitutes both consent and proof of consent. Remember that the consent is limited only to that particular conversation. Unless you obtain additional consent, don't send messages that are outside that conversation.

Informational content to an individual based on a prior relationship

You may send a message to an individual where you have a prior relationship, provided that individual provided their phone number to you, and has taken some action to trigger the potential communication, and has not expressed a preference to *not* receive messages from you. Actions can include a button press, alert setup, appointments, or order placements. Examples of acceptable messages in these scenarios include appointment reminders, receipts, one-time passwords, order/shipping/reservation confirmations, drivers coordinating pick up locations with riders, and repair persons confirming service call times.

The message can't attempt to promote a product, convince someone to buy something, or advocate for a social cause.

Periodic Messages and Ongoing Consent

If you intend to send messages to a recipient on an ongoing basis, you should confirm the recipient's consent by offering them a clear reminder of how to unsubscribe from those messages using standard opt-out language (defined below). You must also respect the message recipient's preferences in terms of frequency of contact. You also need to proactively ask individuals to reconfirm their consent as set forth by local regulations and best practices.

Identifying Yourself as the Sender

Every message you send must clearly identify you (the party that obtained the opt-in from the recipient) as the sender, except in follow-up messages of an ongoing conversation.

Opt-out

The initial message that you send to an individual needs to include the following language: “Reply STOP to unsubscribe,” or the equivalent using another standard opt-out keyword, such as STOPALL, UNSUBSCRIBE, CANCEL, END, and QUIT.

Individuals must have the ability to revoke consent at any time by replying with a standard opt-out keyword. When an individual opts out, you may deliver one final message to confirm that the opt-out has been processed, but any subsequent messages are not allowed. An individual must once again provide consent before you can send any additional messages.

Usage Limitations

Content We Do Not Allow

The key to ensuring that messaging remains a great channel for communication and innovation is preventing abusive use of messaging platforms. That means we never allow some types of content on our platform, even if our customers get consent from recipients for that content. The oneapp Acceptable Use Policy prohibits sending any content that is illegal, harmful, unwanted, inappropriate, objectionable, confirmed to be criminal misinformation, or otherwise poses a threat to the public, even if the content is permissible by law. Other prohibited uses include:

- Anything that is illegal or otherwise unlawful in the jurisdiction where the message recipient lives.
- Hate speech, harassment, exploitative, abusive, or any communications that originate from a hate group.
- Fraudulent messages.
- Malicious content, such as malware or viruses.
- Any content that is designed to intentionally evade filters (see below).

Area-Specific Rules

All messages should comply with the rules applicable to the area in which the message recipient lives, which may be found in our SaaS and Area Specific Requirements.

Age and Geographic Gating

If you are sending messages in any way related to adult content, then more restrictions apply. In addition to obtaining consent from every message recipient, you must ensure that no message recipient is younger than the legal age of consent based on where the recipient is located. You also must ensure that the message content complies with all applicable laws of the jurisdiction in which the message recipient is located or applicable communications industry guidelines or standards.

You need to be able to provide proof that you have in place measures to ensure compliance with these restrictions.

oneapp Messaging SaaS Policy Violation Detection and Prevention Evasion

Customers may not use oneapp's platform to evade oneapp's or a telecommunications provider's unwanted messaging detection and prevention mechanisms. Subject to oneapp's Privacy Notice, oneapp collects and monitors the content of text messages that are transmitted via oneapp's platform to certain areas in order to detect spam, fraudulent activity, and violations of the oneapp Acceptable Use Policy.

Examples of prohibited practices include:

- Content designed to evade detection. As noted above, we do not allow content which has been specifically designed to evade detection by unwanted messaging detection and prevention mechanisms. This includes intentionally misspelled words or non-standard opt-out phrases which have been specifically created with the intent to evade these mechanisms.
- Snowshoeing. We do not permit snowshoeing, which is defined as spreading similar or identical messages across many phone numbers with the intent or effect of evading unwanted messaging detection and prevention mechanisms.
- Simulated social engineering attacks. You are prohibited from transmitting messages that are used for security testing, including simulated phishing and other activities that may resemble social engineering or similar attacks.
- Other practices identified and prohibited by this policy and oneapp's Acceptable Use Policy.

How We Handle Violations

When we identify a violation of these principles, where possible, we will work with customers in good faith to get them back into compliance with this policy. However, to protect the continued ability of all our customers to freely use messaging for legitimate purposes, we reserve the right to suspend or remove access to oneapp's platform for customers or customers' end users' that we determine are not complying with the oneapp Messaging SaaS Policy, or who are not following the law in any applicable area or applicable communications industry guidelines or standards, in some instances with limited notice in the case of serious violations of this policy.

Payments SaaS

These oneapp Payments SaaS requirements ("*Payments SaaS Terms*") will apply to Merchant to the extent Merchant uses the Payments SaaS (as defined below). These Payments SaaS Terms supplement the terms of the Terms of Service between Merchant and oneapp covering Merchant's and End Users' use of the SaaS ("*Agreement*"). Except as otherwise expressly set forth in these Payments SaaS Terms, the terms of the Agreement, including, without limitation, any indemnifications, disclaimers and liability limitations set forth therein, will apply to the use of the Payments SaaS.

Any capitalized term not defined in the Screening SaaS Terms will have the meaning provided in the Terms of Service.

1. Definitions

"*Authorized Payments User*" means a Merchant employee, contractor or agent that Merchant has authorized to order or access the Payments SaaS and who is trained on Merchant's obligations under this Agreement with respect to the ordering and use of the Payments SaaS including Merchant's legal and other obligations with respect to the access and use of the Payments SaaS.

"Cards" means a credit card, debit card and other types of payments.

"Card Not Present Transactions" means internet-based transactions.

"Card Present Transactions" means in-person, point-of-sale payment transactions.

"*Merchant Services*" has the meaning set forth in the Agreement.

"Financial Services Provider" means a financial institution in the United States.

"Keyed Transactions" means manually entered transactions.

“*oneapp Payments SaaS*” or “*Payments SaaS*” means the SaaS Merchants use for (1) payment account onboarding; (2) payment underwriting; and, (3) payment data transmission that helps Merchants integrate with a Processor (as defined below).

“*Payment Processing*” means the processing and settlement of Transactions (as defined below).

“*Processor*” is Stripe, Inc., organized under the laws of Delaware, which is a technical services provider and may offer the services as an agent of one or more Financial Services Providers. oneapp reserves the right to change Processor at any time, and Merchant will provide the Payments SaaS with any information required to set up an account with any such alternate payment processor. For the avoidance of doubt, oneapp is not a payment processor, bank, payment institution, or money services business.

“Transactions” collectively means Card Not Present Transactions, Card Present Transactions, and Keyed Transactions.

“SaaS” has the meaning set forth in the Agreement.

2. Representations and Warranties, Covenants

2.1 SPECIFIC TO THE PAYMENTS SAAS TERMS, THE REPRESENTATIONS AND WARRANTIES SET FORTH BELOW IN THIS SECTION ARE EACH PARTY’S ONLY REPRESENTATIONS AND WARRANTIES AND NO OTHER REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WILL APPLY.

2.1 Merchant Representations and Warranties. You represent and warrant to us that: (i) the name identified by you when you registered is your name or business name under which you sell goods and services and the information that you have provided to us is accurate and complete; (ii) you are not a member of an organized crime group, a party who has been a member of an organized crime group in the past five years, a quasi-member of an organized crime group, a corporate racketeer, or other similar party, nor are any of your officers or employees a member of the foregoing; and, (iii) you will not carry out, nor use a third party to carry out, any of the following unlawful acts: (a) the act of making violent demands; (b) the act of making unreasonable demands exceeding legal responsibilities; (c) the act of using threatening behavior or violence in relation to a transaction; (d) the act of spreading rumors, using fraudulent means, or using force to harm the other party’s reputation or obstruct the party’s business; (e) the act of selling products for the purpose of money laundering; (f) the act of using a Card held by you for a sale without reasonable grounds or another act similar to those set forth in (a) through (f).

2.2 Merchant Covenants. You hereby covenant to us that: (i) any Transactions submitted by you will represent a bona fide sale by you; (ii) any Transaction submitted by you will accurately describe the goods and/or services sold and delivered to a End User; (iii) you will fulfill all of your obligations to each End User for which you submit a Transaction and will resolve any disputes or complaints directly with your End Users; (iv) you and all Transactions initiated by you will comply with all applicable laws, rules, and regulations applicable to your business, including, but not limited to, any applicable tax laws and regulations; (v) except in the ordinary course of business, no Transaction submitted by you through the Payments SaaS will represent a sale to any principal, partner, proprietor, or owner of your entity; (vi) you will not use the Payments SaaS, directly or indirectly, for any fraudulent undertaking or in any manner so as to interfere with the use of the Payments SaaS; and, (vii) any information you provide to us will be accurate and complete.

3. Application, Use Case Attestation and Approval

3.1 If applicable, Merchant must submit an application in the form of a use case attestation to Processor and certain Financial Service Provider(s), which sets forth a true, accurate, and complete description of Merchant's business and intended use case(s) for Payment Processing, and which complies with Subsection 2.2 of these Payments SaaS Terms. Merchant's use of the Payments is subject to the Processor's and applicable Financial Service Provider(s) review and approval of Merchant's use application. For the avoidance of doubt, oneapp has no control over Processor's or a Financial Service Provider(s) approval of Merchant's application. Merchant is not entitled to any refunds or credits if: (a) Processor's or a Financial Service Provider(s) rejects Merchant's application; or (b) Merchant's application contains information that is untrue, inaccurate, or incomplete. Merchant will not use the Payments SaaS for any use case that is not approved by Processor's or a Financial Service Provider(s). If Merchant wants to modify its approved use case(s), Merchant must submit a new application for such modified use case(s) for approval.

4. The Processor

4.1 Payment Processing is carried out by the Processor and any of the Financial Services Providers under a separate Stripe Connected Account Agreement, including the United States Stripe Services Agreement and the applicable Financial Services Terms, and to the extent you use a payment method that is subject to additional terms, the Payment Terms (collectively, the "Processor Terms"). By accepting this Agreement, you are also accepting and agreeing to be bound by the Processor Terms, which is the legal agreement between you and the Processor.

4.2 oneapp is not a party to the Processor Terms and is not liable to you in respect thereof. By accepting this Agreement and the Processor Terms you are agreeing to the creation of an account with the Processor for Payment Processing (the "Processor

Account"). We reserve the right to change the Processor, subject to the terms of our agreement with the Processor. In the event of any inconsistency between this Agreement and the Processor Terms, this Agreement shall prevail, except in the event of any inconsistency between this Agreement and the Processor Terms concerning Payment Processing or the Processor Account, in which case the Processor Terms shall prevail.

4.3 The Processor's role is to accept and process Cards with respect to sales of your Card Not Present Transactions, and if applicable, transmission of data to the Processor from Card Present Transactions, as well as Keyed Transactions.

4.4 oneapp is not a payment processor nor is oneapp providing Merchant with, directly or indirectly, any payment processing services. oneapp is not responsible for (a) the acts or omissions of any payment processor, including, without limitation, a payment processor's failure to process any payments; (b) any data provided by Merchant to oneapp that is in a payment processor's possession; or (c) network connectivity problems outside of oneapp's network.

5. Merchant Responsibilities

5.1 To utilize the Payments SaaS, you must be a business located in the United States.

5.2 You shall not: (i) permit any third party to access the Payments SaaS, except for your Authorized Payments User(s) or as permitted herein, and to carry out Transactions; (ii) create derivative works based on the Payments SaaS; (iii) copy, frame or mirror any part of the content of the Payments SaaS, other than copying or framing for your internal business purposes; (iv) reverse engineer, disassemble, decompile, or otherwise attempt to discover the source code or trade secrets for any of the Payments SaaS; or, (v) access the Payments SaaS in order to build a competitive product or service.

5.3 It is your responsibility to obtain your End Users' consent to be billed for each Transaction or, as the case may be, on a recurring basis, in compliance with applicable legal requirements and Visa Europe Ltd., Visa U.S.A., Inc., Visa Canada Inc. and Visa International (collectively, "Visa"), MasterCard International Incorporated ("MasterCard"), American Express or other applicable Card networks' (such networks being, collectively, the "Payment Networks") payment rules (the "Payment Network Rules").

6. Payment Methods

6.1 The Payments SaaS support most Payment Network Cards, including credit, debit, pre-paid, or gift cards. You assume sole and exclusive responsibility for the use of the Payments SaaS. You also assume sole and exclusive responsibility for Transactions

under the Processor Terms. You are solely responsible for verifying the identity of End Users and of the eligibility of a presented Card used to purchase your services, and oneapp does not guarantee or assume any liability for Transactions authorized and completed that may later be reversed or charged back (see section 25 (Your Liability and Indemnification Concerning Liabilities) below). You are solely responsible for all reversed or charged back transactions regardless of the reason for, or timing of the reversal or chargeback. oneapp or the Processor may add or remove one or more types of Payment Networks or Cards, in their sole discretion, at any time, without prior notice to you.

7. Merchant Support

7.1 oneapp will use its commercially reasonable efforts to provide you with customer support to help resolve issues relating to the Payments SaaS. The Processor retains sole and exclusive responsibility for Payment Processing of Transactions, including the settlement of funds, but oneapp will provide reasonable assistance in liaising between you and the Processor concerning the Payment Processing services. You assume sole and exclusive responsibility for providing customer service or support to your End Users for any and all issues related to your products and services, including, but not limited to, issues arising from the processing of Cards through the Payments SaaS.

7.2 In the event an End User submits a complaint about the SaaS via oneapp’s support channels, oneapp may, in its sole reasonable discretion, issue a credit, partial refund, or full refund to such End User. Merchant shall bear the full cost of that credit or refund, as applicable, if the complaint was caused by Merchant or Merchant Services.

8. Taxes

8.1 You have sole and exclusive responsibility to determine what, if any, taxes apply to the sale of your goods and services and/or the payments you receive in connection with your use of the Payments SaaS ("Taxes"). It is solely your responsibility to assess, collect, report, or remit the correct Taxes to the proper tax authority, whether in End Users’ jurisdictions, your jurisdiction or elsewhere. We are not obligated to, nor will we, determine whether Taxes apply, or calculate, collect, report, or remit any Taxes to any tax authority, arising from any Transaction. oneapp retains the right, but not the obligation, at its sole discretion, to complete and file tax or related reports with tax authorities regarding Transactions in those jurisdictions where oneapp deems such reporting necessary. You hereby indemnify and hold oneapp harmless from and against any and all liability related to Taxes and filings made by oneapp in respect thereof.

8.2 You agree to receive all federal and state tax statements in an electronic format and acknowledge that paper tax statements will not be provided. We will notify you when an

electronic statement is available in accordance with Section 19.5 of the SaaS Terms (Notices). Specific instructions for access and download will be included.

8.3 In the event you withdraw consent with the SaaS Terms and/or these terms, you will receive all electronic tax-related statements for the duration of time the agreement was authorized.

9. Your End Users

7.1 If prohibited by law, you will not impose any fee or surcharge on an End User that seeks to use an eligible Card. You will provide an informational slip or receipt to your End User at the conclusion of the Transaction that includes all information required under Payment Network Rules and applicable law.

10. Security

10.1 We maintain commercially reasonable administrative, technical and physical procedures to protect all the personal information regarding you and your customers that is stored in our servers from unauthorized access, accidental loss, or modification. oneapp cannot, however, guarantee that unauthorized third parties will never be able to defeat those measures or use such personal information for improper purposes.

11. Data Security

11.1 You assume full responsibility for the security of data on your website or otherwise in your possession or control. You agree to comply with all applicable laws and rules in connection with your collection, security, and dissemination of any personal, financial, Card, or Transaction information (collectively, “Data", and as pertains to your End Users, “Cardholder Data”). You agree that at all times you shall be compliant with applicable Payment Card Industry Data Security Standards (“PCI-DSS”) and, as applicable, the Payment Application Data Security Standards (“PA-DSS”). You agree to promptly provide oneapp with documentation evidencing your compliance with PCI-DSS and/or PA-DSS upon request. You also agree that you will use only PCI-DSS and PA-DSS compliant service providers in connection with the storage or transmission of Card information, including a cardholder’s account number, expiration date, and CVV2. You must not store CVV2 data at any time. Information on PCI-DSS can be found on the PCI Council’s website. It is your responsibility to comply with these standards and all the Payment Network Rules. We may request additional security measures at any time and reserve the right to adjust these requirements at our discretion.

12. Audit Right

12.1 If oneapp believes that a security breach, personal data breach, or other compromise of data may have occurred, oneapp may require you to have a third-party auditor that is approved by oneapp conduct a security audit of your systems and facilities and issue a report to be provided to oneapp and, at oneapp's discretion, to the Processor, its Financial Services Provider, Payment Networks, and law enforcement, at your sole cost and expense.

13. Privacy

13.1 Your privacy and the protection of your data are very important to us. You acknowledge that you have received, read in full, and agree with the terms of the Processor Privacy Policy. You also acknowledge that the Processor is required to report your business name and the name of your principals to the Member Alert to Control High-Risk merchants list of MasterCard ("MATCH List") maintained by MasterCard and accessed and updated by American Express, to the VMAS database upheld by Visa Europe, and/or to the Consortium Merchant Negative File maintained by Discover, if applicable, pursuant to the requirements of the Payment Network Rules.

13.2 You acknowledge that the Payments SaaS relies on you for direction as to the extent to which the Payments SaaS is entitled to use and process the personal data in the Cardholder Data that you provide. Consequently, oneapp will not be liable for any claim brought by a data subject arising from any action or omission by oneapp or your use of the Payments SaaS, to the extent that such action or omission resulted from your instruction.

13.3 You consent to the exchange of your information between the account you have established through the SaaS and the Payments SaaS established under this Agreement. oneapp will commingle such accounts and refers to them together in this Agreement as the "oneapp Payments Account".

13.4 In order to process, use, record, and disclose your personal information, information related to your business, and Data, we or our agents may transfer such information to and receive it from the Processor, its Financial Services Provider, or their respective agents and, in so doing, we may transmit or possess it outside of your jurisdiction.

13.5 In order to provide the Payments SaaS, we use a variety of third party "sub-processors" that fall into many broad categories—for example, we use sub-processors to help us: (i) protect you and oneapp from potentially risky transactions, security threats, or fraud; (ii) perform administrative tasks; (iii) deliver

portions of the Payments Services (e.g., third parties that work with us to actually process credit card payments or conduct any shipping); (iv) develop and improve our products and the Payments SaaS; (v) generate analytics or other information relating to the Payments SaaS; and, (vi) build our technical infrastructure (e.g., using cloud storage providers or information security vendors). By using the Payments SaaS, you consent to our use of sub-processors, a list of which are provided below.

14. Privacy of Others

14.1 You represent to us that you are in compliance with all applicable privacy laws and that you maintain a publicly accessible privacy policy that accurately discloses how you collect, use, and disclose personal data, including through the Payments SaaS. Additionally, you represent to us that you have obtained all necessary rights and consents under applicable law to allow us and the Processor to collect, use, retain, and disclose any Cardholder Data that you provide to, or authorize us to collect, including information that we may collect directly from you of your End Users via cookies or other means and to use that data to provide the Payments SaaS (e.g., to process Transactions and to screen for fraud or compliance purposes).

14.2 Further, you represent that we will not be in breach of any such laws by collecting, receiving, using, and disclosing such information in connection with the Payments SaaS as described in our Privacy Notice. As between the parties to this Agreement, you are solely responsible for disclosing to your End Users that the Payments SaaS will collect and process their Cardholder Data in oneapp's provision of the Payments SaaS to you, and that in so doing the Payments SaaS may transmit or possess it outside of your or their jurisdiction, and that it may be subject to disclosure as required by applicable law.

14.3 If you receive information about others, including cardholders and other End Users, through the use of the Payments SaaS, you must keep such information confidential and only use it in connection with the Payments SaaS or as otherwise permitted by the subject of such information. You may not disclose or distribute any such information to a third party or use any such information for marketing purposes unless you receive the express consent of the subject thereof to do so. You may not disclose Cardholder Data to any third party other than in connection with processing a Transaction requested by your End User.

15. Restricted Use

15.1 You are required to obey all laws, rules, and regulations applicable to your use of the Payments SaaS (e.g., including those governing financial services, consumer protections, unfair competition, anti-discrimination, or false advertising). In addition to any other requirements or restrictions set forth in this Agreement, you shall not: (i) utilize

the credit available on any Card to provide cash advances to cardholders; (ii) submit any Transaction for processing that does not arise from your sale of goods or service to a End User; (iii) act as a payment intermediary or aggregator or otherwise resell the Payments SaaS on behalf of any third party; (iv) send what you believe to be potentially fraudulent authorizations or fraudulent Transactions; (v) use the Payments SaaS or the Payment Processing services in a manner that a Payment Network reasonably believes to be an abuse of the Payment Network or a violation of the Payment Network Rules; or, (vi) work around any of the technical limitations of the Payments SaaS or oneapp's checkout, use any tool to enable features or functionalities that are otherwise disabled in the Payments SaaS, or decompile, disassemble, or otherwise reverse engineer the Payments SaaS, except to the extent that such restriction is expressly prohibited by law.

15.2 You further agree not to permit any third party to do any of the following: (i) access or attempt to access our systems, programs, or data that are not made available for public use; (ii) copy, reproduce, republish, upload, post, transmit, resell, or distribute, in any way, material from us; (iii) permit any third party to use and benefit from the Payments SaaS via a rental, lease, timesharing, service bureau, or other arrangement; (iv) transfer any rights granted to you under this Agreement; (v) work around any of the technical limitations of the Payments SaaS or oneapp's checkout, use any tool to enable features or functionalities that are otherwise disabled in the Payments SaaS, or decompile, disassemble, or otherwise reverse engineer the Payments SaaS, except to the extent that such restriction is expressly prohibited by law; (vi) perform or attempt to perform any actions that would interfere with the proper working of the Payments SaaS, prevent access to or use of the Payments SaaS by our other users, or impose an unreasonable or disproportionately large load on our infrastructure; or, (vii) otherwise use the Payments SaaS except as expressly allowed under this section.

16. Suspicion of Unauthorized or Illegal Use

16.1 We reserve the right to not provide the Payments SaaS in respect of any Transaction you submit that we believe, in our sole discretion, is in violation of this Agreement, any other oneapp or Processor agreement, or exposes you, oneapp, the Processor, or any other third party to actual or potential risk or harm, including, but not limited to, fraud and other criminal acts. You are hereby granting us authorization to share information with law enforcement about you, your Transactions, or your oneapp Payments Account.

17. Payment Network Rules

17.1 The Payment Networks have established guidelines, bylaws, rules, and regulations in the form of the Payment Network Rules. You are required to comply with all

applicable Payment Network Rules. The Payment Network Rules for Visa, MasterCard and American Express are available on the Internet at the following links: Visa, MasterCard and American Express. The Payment Networks may amend the Payment Network Rules at any time and without notice to us or to you. Insofar as the terms of this Agreement and/or the Processor Terms are inconsistent with the Payment Network Rules, the Payment Network Rules shall prevail. We reserve the right to amend this Agreement at any time, with notice to you, as may be necessary to comply with the Payment Network Rules.

18. Disclosures and Notices

18.1 You agree that oneapp can provide disclosures and notices, including tax forms, that we deem appropriate regarding the Payments SaaS to you by posting such disclosures and notices in accordance with Section 19.5 of the SaaS Terms (Notices). You also agree that electronic disclosures and notices have the same meaning and effect as if we had provided you with a paper copy. Such disclosures and notices shall be considered to be received by you within twenty-four (24) hours of the time it is emailed to you, unless we receive notice that the email was not delivered.

19. Automatic Reminders

19.1 We may use automated telephone dialing, text messaging systems, and email to provide messages to you about your oneapp Payments Account. The telephone messages may be played by a machine automatically when the telephone is answered, whether answered by you or another party. These messages may also be recorded by your answering machine or voicemail. You give us permission to call or send a text message to any telephone number that you have given us and to play pre-recorded messages or send text messages with information about this Agreement or your account over the phone. You agree that we will not be liable to you for any such calls or electronic communications even if information is communicated to an unintended recipient. You understand that when you receive such calls or electronic communications you may incur a charge from the company that provides you with telecommunications, wireless and/or Internet services. You agree that we have no liability for such charges. You agree to immediately notify us if you change telephone numbers or are otherwise no longer the subscriber or customary user of a telephone number or email address you have previously provided to us.

20. oneapp Payments SaaS Fees

20.1 You agree to pay the fees for processing that are set out in the applicable Order Form(s), or if not set forth in the applicable Order Form(s), you will be charged the

applicable rates available at https://withoneapp.com/#pricing, which are incorporated herein by reference (the "Processing Fees"). Processing Fees shall be collected from you by the Processor on our behalf in accordance with the terms of the Stripe Connected Account Agreement.

20.2 Fees for the SaaS are collected by oneapp pursuant to the Terms of Service. All fees, whether charged by oneapp, or charged by you to your Merchants will be referred to collectively as the "Fees". You agree that oneapp may charge any of oneapp's Fees for the SaaS to you or your End Users, where applicable.

20.3 You are obligated to pay all applicable taxes, fees and other charges imposed by any governmental authority, including, without limitation, any value added tax, goods and services tax, harmonized sales tax and/or provincial or territorial sales tax, on the Payments SaaS provided under this Agreement. If you are tax-exempt, you will provide us with an appropriate certificate or other evidence of tax exemption that is satisfactory to us.

20.4 We reserve the right to change the Fees at any time, subject to a thirty (30) day notice period to you in accordance with Section 19.5 of the SaaS Terms (Notices). If you continue to use the Payments SaaS and the Processor Services for such thirty (30) days, then you are deemed to have accepted the change in Fees contemplated by such notice. Notwithstanding the thirty (30) day notice period referred to above, if oneapp or the Processor suspends, disables, or otherwise makes your oneapp Payments Account unavailable to you, and then subsequently reinstates your access to your oneapp Payments Account, the then current Fees at the time of reinstatement shall apply to you.

20.5 In addition to the Fees, you are also responsible for any penalties and fines imposed on you or on us by any bank, money services business, payment network, financial institution, or other financial intermediary resulting from your use of the Payments SaaS in a manner not permitted by this Agreement or by such financial intermediary's rules and regulations.

21. Security Interest

21.1 As security for performance of your obligations under this Agreement, you grant us a first priority lien and security interest on all funds processed and deposited into all Payout Accounts (as defined in the Processor Terms), and any other bank accounts associated with your oneapp Payments Account, and in any funds processed using the Payment Processing services. These security interests and liens will secure payment and performance of all of your obligations under this Agreement and any other agreements now existing or later entered into between us and you, including, without

limitation, your obligation to pay any amounts due and owing to us. You will execute, deliver and pay the fees for any documents we request to create, perfect, maintain, and enforce this security interest.

21.2 Our Collection Rights To the extent permitted by law, we may collect any obligations you owe us under this Agreement by requesting that the Processor deduct the corresponding amounts from the Reserve Account (as that term is defined below) or from funds payable to you arising from the settlement of Transactions. Fees will be assessed at the time a Transaction is processed and will be first deducted from the funds received for such Transaction. If these amounts are not sufficient to meet your obligations to us, we may charge the payment method associated with your oneapp Payments Account for any amounts owed to us. Your failure to fully pay amounts that you owe us on demand will be a breach of this Agreement. You will be liable for our costs associated with collection in addition to the amount owed, including, without limitation, attorneys' fees and expenses, costs of any arbitration or court proceeding, collection agency fees, and any applicable interest.

21.3 Further, we may deduct, or request that the Processor deduct, from any accounts associated with your oneapp Payments Account, including the Processor Account and the Reserve Account, any amounts that you owe to us under this Agreement or any other agreement you have entered into with us or our affiliates.
Additionally, we may require a personal guarantee from a principal of a business for funds owed under this Agreement. If we require a personal guarantee we will specifically inform you in advance.

21.4 In addition to the amount due, delinquent accounts may be charged with fees that are incidental to the collection of delinquent accounts and chargebacks, including, but not limited to, collection fees and convenience fees and other third-party charges.

21.5 You hereby explicitly agree that all communication in relation to delinquent accounts will be made by electronic mail or by phone, as provided to oneapp by you. Such communication may be made by oneapp or by anyone on its behalf, including, but not limited to, a third-party collection agent.

22. Reserves

22.1 Funds held in reserves are amounts of money set aside to cover chargebacks, refunds, or other payment obligations under this Agreement (the "Reserve Account"). We, in our discretion, will set the terms of your Reserve Account and notify you of such terms, which may require that a certain amount (including the full amount) of the funds received for a Transaction are held for a period of time, or that additional amounts are held in the Reserve Account. We, in our discretion, may elect to change the terms of the

Reserve Account at any time, for any reason, based on your payment processing history or as requested by our payment processors.

22.2 We may require you to fund the Reserve Account by means of: (i) any funds payouts made or due to you for Transactions submitted to the Payments SaaS; or, (ii) amounts available in your bank account by means of ACH debit to your oneapp Payments Account; or, (iii) other sources of funds associated with your oneapp Payments Account; or, (iv) requesting that you provide funds to us for deposit to the Reserve Account. In accordance with the Processor Terms you authorize us to debit your bank account without separate notice, and according to the applicable User Bank Account Debit Authorization (as defined in the Processor Terms), to collect amounts you owe under this Agreement.

22.3 You agree that: (i) you are not entitled to any interest or other compensation associated with the funds held in the Reserve Account; (ii) you have no right to direct that account; (iii) you have no legal interest in those funds or that account; and, (iv) you may not assign any interest in those funds or that account.

23. Payment Issues

23.1 Merchant is solely responsible for managing and resolving all complaints, refunds, or credits or payment issues, disputes, reversals, chargebacks, or adjustments.

24. Contesting Chargebacks

24.1 You or oneapp may elect to contest chargebacks assessed to your account. oneapp may provide you with assistance, including notifications and software to help contest your chargebacks. We do not assume any liability for our role or assistance in contesting chargebacks.

24.2 You grant us permission to share records or other information required with the cardholder, the cardholder's financial institution, and your financial institution to help resolve any chargeback. You acknowledge that your failure to provide us with complete and accurate information in a timely manner may result in an irreversible chargeback being assessed.

24.3 If the cardholder's issuing bank or the Payment Network does not resolve a dispute in your favor, we may recover the chargeback amount and any associated fees from you as described in this Agreement.

24.4 We reserve the right, upon notice to you, to charge a fee for mediating or investigating chargeback disputes.

25. Effects of Termination

25.1 Upon termination and closing of your oneapp Payments Account, we will immediately discontinue your access to the Payments SaaS. You agree to complete all pending Transactions, immediately remove all logos for Cards, and stop accepting new Transactions through the Payments SaaS. You will not be refunded the remainder of any Fees that you have paid for the Payments SaaS if your access to or use of the Payments SaaS is terminated or suspended. Any funds in the Financial Services Provider's custody will be paid out to you subject to the terms of your Payout Schedule (as defined in the Processor Terms).

25.2 Termination does not relieve you of your obligations as defined in this Agreement, and the Processor may elect to continue to hold any funds deemed necessary, pending resolution of any other terms or obligations defined in this Agreement, including, but not limited to, chargebacks, fees, refunds, or other investigations or proceedings.

25.3 Termination of this Agreement will not necessarily terminate your SaaS Terms, unless oneapp determines otherwise.

25.4 Upon termination you agree: (i) to immediately cease your use of the Payments SaaS; (ii) to discontinue use of any oneapp or Processor trademarks and to immediately remove any oneapp or Processor references and logos from your website and/or physical location, if applicable; (iii) that the license granted under this Agreement shall end; (iv) that we reserve the right (but have no obligation) to delete all of your information and account data stored on our servers; (v) that we will not be liable to you for compensation, reimbursement, or damages in connection with your use of the Payments SaaS, or any termination or suspension of the Payments SaaS, or deletion of your information or account data; and, (vi) that you will still be liable to us for any fees or fines, or other financial obligation incurred by you or through your use of the Payments SaaS prior to termination.

26. Your Liability and Indemnification Concerning Liabilities

26.1 Nothing in this Agreement shall serve to diminish your liability under the Processor Terms or SaaS Terms. You are obliged to fulfill your obligations under this Agreement and those under the Processor Terms and SaaS Terms.

26.2 oneapp has agreed to indemnify and hold the Processor harmless for some, and, in some cases, all of your liabilities occurring under the Processor Terms, including, but not limited to, disputes (including, but not limited to, chargebacks), refunds, reversals, returns and fines (as such terms are defined in the Processor Terms). Insofar as oneapp

becomes liable to the Processor or any other third party for any penalties, fines, fees, or other liabilities under or in respect of the Processor Terms, the Payments SaaS, the Payment Processing services, or the Payment Network Rules, you agree to indemnify and hold oneapp harmless from and against any and all such liabilities.

26.3 Additionally, we may require a personal guarantee from a principal of a business for funds owed under this Agreement.

26.4 You will be required to reimburse us for your liability. You will not receive a refund of any Fees paid to us. If you are liable for any amounts owed to us, we may immediately remove such amounts from your Reserve Account and deduct the amounts owed to us from such Reserve Account funds. If you do not have sufficient funds in the Reserve Account to cover your liability, you will be required to immediately add additional funds to your Reserve Account to cover funds owed to us. If you do not do so, we may engage in collections efforts to recover such amounts from you at your cost and expense.

27. Change of Business

27.1 You agree to give us at least thirty (30) days prior notification of your intent to change your current product or services types, your business or trade name, or the manner in which you accept payment. You agree to provide us with prompt notification within three (3) days if you are the subject of any voluntary or involuntary bankruptcy or insolvency application, petition or proceeding, receivership, bankruptcy, or similar action or proceeding initiated by or against you or any of your principals (any of the foregoing, a “Bankruptcy Proceeding”). You also agree to promptly notify us within three (3) days of any adverse change in your financial condition, any planned or anticipated liquidation or substantial change in the basic nature of your business, any transfer or sale of twenty-five percent (25%) or more of your total assets, or any change in the control or ownership of your or your parent entity. You will also notify us within three (3) days of any judgment, writ, warrant of attachment or execution, or levy against twenty-five percent (25%) or more of your total assets.

27.2 You will include us on the list and matrix of creditors as filed with any bankruptcy, commercial or civil court in connection with any Bankruptcy Proceeding, whether or not a claim may exist at the time of filing. Failure to do so will be cause for immediate termination of this Agreement and shall allow the pursuit of any other action available to us under the applicable Payment Network Rules or law.

28. Third-Party Services and Links to Other Web Sites

28.1 You may be offered services, products, and promotions provided by third parties and not by us. If you decide to use these third-party services, you will be responsible for reviewing and understanding the terms and conditions associated with these services. You agree that we are not responsible for the performance of these services. The oneapp website may contain links to third-party websites as a convenience to you. The inclusion of any website link does not imply an approval, endorsement, or recommendation by us. You agree that your access to any such website is at your own risk, and that the site is not governed by the terms and conditions contained in this Agreement. We expressly disclaim any liability for these websites. Please remember that when you use a link to go from our website to another website, our Privacy Notice is no longer in effect. Your browsing and interaction on any other website, including those that have a link on our website, is subject to that website's own rules and policies.

SaaS in Private Beta

These SaaS in Private Beta requirements ("*Private Beta SaaS Terms*") will apply to Merchant to the extent Merchant and its End Users use the Private Beta SaaS Offerings (as defined below). These SaaS in Private Beta Terms supplement the terms of the Terms of Service. Except as otherwise expressly set forth in these Private Beta SaaS Terms, the Terms of Service, including, without limitation, any disclaimers and liability limitations set forth therein, will apply to the use of the Private Beta SaaS.

Any capitalized term not defined in the Private Beta SaaS Terms will have the meaning provided in the Terms of Service.

1. Availability

From time to time, oneapp may make available certain SaaS that are identified as alpha, beta, not generally available, limited release, developer preview, or any similar SaaS that are, in all the foregoing cases, only made available to a limited number of customers on an invitation basis in a non-public or private manner (collectively, "*Private Beta SaaS Offerings*"). Private Beta Offerings made available to Merchant are strictly for testing and experimentation purposes only. Merchant acknowledges that, by their nature, Private Beta Offerings may (a) not meet speed or performance benchmarks or expectations; (b) have gaps in functionality; and (c) contain bugs. Any terms relating to support, service levels, or performance standards in the Agreement do not apply to Private Beta Offerings.

2. Merchant Discretion

Use of any Private Beta Offerings will solely be at Merchant's and End User's own discretion and risk.

3. Confidentiality

Private Beta Offerings, and any information related to such Private Beta Offerings, including their existence, are considered oneapp's Confidential Information.

4. Discontinuation

oneapp may discontinue a Private Beta Offering at any time, in its sole discretion, or in rare circumstances, decide not to make a Private Beta Offering generally available.

SaaS using Phone Numbers

These SaaS using Phone Numbers requirements ("Phone Numbers Requirements") will apply to Merchant to the extent Merchant uses a phone number with any of the SaaS ("SaaS using Phone Numbers"). These Phone Numbers Requirements supplement the Terms of Service. Except as otherwise expressly set forth in these Phone Numbers Requirements, the Terms of Service, including, without limitation, any disclaimers and liability limitations set forth therein, will apply to the use of the SaaS using Phone Numbers.

Any capitalized term not defined in these SaaS using Phone Numbers requirements ("Phone Numbers Requirements") will have the meaning provided in the Terms of Service.

Phone Number Compliance

Merchant will provide oneapp with true, accurate, and complete information associated with Merchant's use of any phone number with the SaaS for which oneapp is required to have an address or any other information of Merchant or an End User, if applicable, on record. Merchant will keep the foregoing information current and provide reasonable cooperation regarding information requests from law enforcement, regulators, or telecommunications providers. Furthermore, if Merchant uses any SaaS that require the use of a phone number, Merchant will comply with any law or regulation that is or becomes applicable as a result of Merchant's software application or service interfacing with the SaaS.

Phone Number Porting

Merchant agrees not to obtain phone numbers via Merchant's account for the sole purpose of immediately porting them out.

Merchant agrees to provide oneapp with explicit consent in the form required by oneapp for each phone number that Merchant seeks to port out. If Merchant is not the person that makes use of a phone number that is to be ported out, Merchant agrees to obtain such explicit consent from the person that makes use of such phone number prior to initiating a port-out request with oneapp. Merchant agrees not to take any action to prevent the execution of a port-out request once it has instructed oneapp to facilitate such port-out request.

Merchant's port-out request may not be possible if (a) the phone number is not in service; (b) the port-out request is prohibited by applicable law or regulation; (c) the port-out request is not supported by the underlying telecommunications provider or entity receiving the port-in request; or (d) the port-out request is unauthorized, incomplete, or incorrect.

Withdrawal & Replacement of Phone Numbers

Merchant acknowledges that phone numbers associated with Merchant's account are subject to (a) domestic and international laws, policies, and regulations and (b) requirements of underlying telecommunications providers, international intergovernmental organizations (e.g., International Telecommunications Union (ITU)), and phone numbering plan administrators ((a) and (b) collectively, "Phone Number Rules"). oneapp may withdraw or replace any phone number associated with Merchant's account (x) if required pursuant to the Phone Number Rules; (y) if the use of such phone number violates Phone Number Rules; or (z) for technical reasons. oneapp will, where possible, provide Merchant with notice prior to any phone number withdrawal or replacement for the foregoing reasons.

Separately, oneapp may withdraw or replace any phone number without prior notice if such phone number is associated with (x) a trial account that has not been used for more than ninety (90) days or (y) Merchant's account that has been suspended for more than ninety (90) days.

Screening SaaS

These oneapp Screening SaaS requirements ("*Screening SaaS Terms*") will apply to Merchant to the extent Merchant uses the Screening SaaS (as defined below). The

Screening SaaS Terms supplement the terms of the Terms of Service between Merchant and oneapp covering Merchant's use of the SaaS ("*Agreement*"). Except as otherwise expressly set forth in these Screening SaaS Terms, the terms of the Agreement, including, without limitation, any indemnifications, disclaimers and liability limitations set forth therein, will apply to the use of the Screening SaaS.

Any capitalized term not defined in the Screening SaaS Terms will have the meaning provided in the Terms of Service.

1. Definitions

"*Application for Service*" means a service order between Merchant and a Third Party Provider, which sets forth any other terms contained therein.

"*Consumer Credit Data*" means individual consumer credit report data and derivative information published and distributed by a Consumer Data Service Provider. Consumer Credit Data may be provided to Merchants by the Consumer Data Service Provider entities identified below:

- Consumer Data Service, LLC
- TransUnion, LLC
- Experian Information Solutions, Inc.

"*Consumer Data*" means certain attributes returned to Merchant by a Consumer Data Service Provider relating to End Users' submission of any data or information relating to Consumers through the Screening SaaS. Consumer Data includes Consumer Credit Data and Consumer Public Records Data.

"*Consumer Data Service Provider*" means the Consumer Data services provided by certain data service providers, which provide Merchant with Consumer Data that constitute a consumer report. For the avoidance of doubt, oneapp is not a Consumer Data Service Provider.

"*Consumer Public Records Data*" means individual consumer data and other information copied from official, government records available to the public that are reproduced and distributed by a Consumer Data Service Provider.

"*Order Form*" means an ordering document or service addendum between Merchant and oneapp, which sets forth the fees for the Screening SaaS and any other terms contained therein.

"*Screening SaaS*" means the cloud platform provided by oneapp where Merchants may order services provided by certain Data Service Providers.

2. Certifications, Representations and Warranties

2.1 SPECIFIC TO THE SCREENING SAAS TERMS, THE REPRESENTATIONS AND WARRANTIES SET FORTH BELOW IN THIS SECTION ARE EACH PARTY'S ONLY REPRESENTATIONS AND WARRANTIES AND NO OTHER REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WILL APPLY.

2.2 Merchant certifies, represents and warrants that: (a) consumer reports, as defined by the federal Fair Credit Reporting Act, 1681 U.S.C. et seq. ("FCRA"), will be ordered only when intended to be used for the sole permissible purpose of Merchant's legitimate business need for the information in connection with a business transaction that is initiated by the consumer, and such reports will be used for no other purpose, including, without limitation, resale or disclosure (except as permitted in Section 7 below) to the subject consumer or to another reseller or broker of consumer reports; (b) consumer reports will not be used for employment purposes; (c) consumer reports on Merchant's employees will be requested only by its designated representative; (d) Merchant will forbid its End Users from attempting to obtain or obtaining consumer reports on themselves or associates, or on any other person except in the exercise of their official duties; (e) Merchant will establish strict procedures so that Merchant's employees do not access Consumer Data Service information except on behalf of Merchant; (f) Merchant has read and understands its obligations under the FCRA and the penalties for requesting consumer report information under false pretenses; (g) Merchant's policies and procedures are designed to comply with the FCRA and other applicable state or federal laws; and (h) Merchant acknowledges and agrees to comply with the policies and procedures governing Merchant's use of the Screening SaaS as set forth by oneapp and Consumer Data Service Provider(s), and any future new or amended policies or procedures that from time to time are made known to Merchant.

3. Application, Use Case Attestation and Approval

If applicable, Merchant must submit an application in the form of a use case attestation to certain Consumer Data Service Providers, which sets forth a true, accurate, and complete description of Merchant's business and intended use case(s) for consumer reports, and which complies with Subsection 2.2 of these Screening SaaS Terms. Merchant's use of the Screening SaaS is subject to the applicable Consumer Data Service Provider(s) review and approval of Merchant's application. For the avoidance of doubt, oneapp has no control over a Consumer Data Service Provider(s) approval of Merchant's application. Merchant is not entitled to any refunds or credits if: (a) a Consumer Data Service Provider(s) rejects Merchant's application; or (b) Merchant's application contains information that is untrue, inaccurate, or incomplete. Merchant will not use the Screening SaaS for any use case that is not approved by the applicable

Consumer Data Service Provider(s). If Merchant wants to modify its approved use case(s), Merchant must submit a new application for such modified use case(s) for approval.

4. Merchant Monitoring and Review

4.1 Merchant Monitoring. Merchant acknowledges and agrees to monitoring of its use of the Screening SaaS by oneapp and Consumer Data Service Providers on an ongoing basis to confirm and ensure that Merchant's business situation has not changed, that Merchant is using Consumer Data that constitute a consumer report only for the FCRA permissible purposes allowed under the Agreement, and that Merchant, in all other respects, continues to meet the "qualified" requirements of Merchant's application to certain Consumer Data Service Providers (including without limitation, those set forth in Section 2.2 of these Screening SaaS Terms). Merchant additionally acknowledges and agrees that the Screening SaaS will immediately cease providing Consumer Data to Merchant if oneapp or Consumer Data Service Provider(s) determine that Merchant is no longer "qualified."

4.2 Merchant Review. Merchant understands and agrees that oneapp and/or Consumer Data Service Providers may periodically audit Merchant regarding their compliance with the FCRA and the obligations of the Agreement. Audits will be conducted by mail whenever possible and will require the Merchant to provide documentation as to permissible uses of particular consumer reports. Merchant will cooperate fully and promptly in the conduct of such audits.

5. Processing Locations

For the purposes of this Section, "*Processing*" means accessing (including access to view), transmitting, using or storing Consumer Data. Merchant may Process Consumer Data provided by a Consumer Data Service Provider from the United States, Canada, and the United States territories of American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, and the U. S. Virgin Islands (collectively, the "*Permitted Territory*"). Merchant must not Processing Consumer Data provided by a Consumer Data Service Provider from a location outside of the Permitted Territory. Notwithstanding the foregoing, Merchant is prohibited from Processing Consumer Data provided by a Consumer Data Service Provider from an Embargoed Country. "*Embargoed Country*" means any country or geographic region subject to comprehensive economic sanctions or embargoes administered by the U.S. Department of the Treasury's Office of Foreign Asset Control ("*OFAC*") or the European Union.

6. Service Providers

6.1 Merchant may not allow a third party service provider (hereafter "*Service Provider*") to access, use, store, or perform any services related to the Consumer Data on Merchant's behalf unless Merchant complies with all procedures and

requirements set forth in the Policy and Standards, as defined below, and, with respect to storing Consumer Data, obtains oneapp's prior written consent and enters into such written agreements as oneapp may require. Merchant shall be as fully responsible to oneapp for the acts and omissions of Service Providers as it is for the acts and omissions of its own employees. In addition, the territorial provisions in Section 5 above are fully applicable to any Service Provider of Merchant that has access to Consumer Data.

7. Transmission and Storage

The Screening SaaS will, in relaying any and all Consumer Data to Merchant, reliably and accurately transmit the Consumer Data from Consumer Data Service Providers in its entirety, including, but not limited to, transmitting the date the information was last checked or revised by Consumer Data Service Provider and the full name, mailing address, and other contact details of the Consumer Data Service Provider office providing the Consumer Data. The Screening SaaS will provide the Consumer Data procured on behalf of a Merchant to only that Merchant and will not make any other use of that Consumer Data. oneapp does not and will not maintain, copy, capture, re-use or otherwise retain in any manner any Consumer Data provided to Merchant; except to the extent required by law as described in Section 8.1. Notwithstanding the foregoing sentence, oneapp may capture and retain the name and address of the subjects of the information and the date and time of inquiries solely for the purpose of: (a) audit trail; (b) calculation of the amount of usage of Consumer Data and provision of specifics relating to such usage to Merchant; and (c) billing.

8. Requests for Disclosure

oneapp has established strict procedures so that oneapp's employees and the Screening SaaS refer to Consumer Data Service Provider all requests for disclosure from the subject of Consumer Data, except that oneapp may disclose consumer report information to subject consumers, pursuant to the FCRA, state and local law, and as limited below, who have been denied a benefit based on information contained in the consumer report. In those disclosures to consumers, oneapp may disclose only the information disclosed to the applicable consumers. oneapp may not access Consumer Data without the express written permission of Merchant, may not access Consumer Data for purposes of disclosure to consumers who wish disclosure for "curiosity" reasons only, and may not handle consumer disputes of Consumer Data, except as required by law or otherwise expressly permitted pursuant to a written agreement with Consumer Data Service Provider. Consumer requests for disclosure based on curiosity, and all consumer disputes, will be referred to Consumer Data Service Provider for handling.

9. Data Security.

9.1 This Section 9 applies to any means through which Merchant orders or accesses

the Consumer Data including, without limitation, system-to-system, personal computer or the Internet. For the purposes of this Section 9, the term "*Authorized Screening User*" means a Merchant employee, contractor or agent that Merchant has authorized to order or access the Consumer Data and who is trained on Merchant's obligations under the Agreement with respect to the ordering and use of the Consumer Data including Merchant's FCRA and other obligations with respect to the access and use of consumer reports.

9.2 Merchant will, with respect to handling the Consumer Data:

(a) ensure that only Authorized Screening Users can order or have access to the Consumer Data and take all necessary measures to prevent unauthorized ordering of or access to the Consumer Data by any person other than an Authorized Screening User for permissible purposes, including, without limitation, limiting the knowledge of the Merchant security codes, member numbers, User IDs, and any passwords Merchant may use to those individuals with a need to know. In addition, the User IDs must be unique to each person, and the sharing of User IDs or passwords is prohibited;

(b) ensure that Authorized Screening Users are trained not to order consumer reports for personal reasons or provide consumer reports to third parties except as permitted by the Agreement and that any unauthorized access or use of consumer reports may subject them to civil and criminal liability under the FCRA, punishable by fines and imprisonment;

(c) ensure that secure authentication practices are utilized when accessing the Consumer Data , including but not limited to restricting access based on Authorized Screening User location and only permitting access to the Consumer Data through Merchant approved devices;

(d) ensure that Consumer Data is encrypted in transit with Advanced Encryption Standard (AES)-256 or an equivalent or better National Institute of Standards and Technology (NIST) approved cypher;

(e) use commercially reasonable efforts to secure Consumer Data at rest, including: (i) encrypting all Consumer Data at rest in accordance with industry accepted encryption standards; (ii) separating Consumer Data from the Internet or other public networks by firewalls configured to meet industry accepted best practices; (iii) protecting Consumer Data through multiple layers of network security, including but not limited to, industry-recognized firewalls, routers, and intrusion detection/prevention devices (IDS/IPS), (iv) securing access (both physical and network) to systems storing Consumer Data; and (v) patching servers on a timely basis with appropriate security-specific system patches, as they are available;

(f) ensure that: (i) all hard copy Consumer Data is stored in a secure manner; (ii) Consumer Data, including electronic and hard copy information, is securely destroyed when no longer needed for the Consumer Data ; and (iii) maintain documented policies to ensure compliance with the foregoing;

(g) not allow Consumer Data to be displayed via the Internet unless utilizing, at a minimum, a three-tier architecture configured in accordance with industry best practices;

(h) use commercially reasonable efforts to establish procedures and logging mechanisms for systems and networks that will allow tracking and analysis in the event there is a compromise, and maintain an audit trail history;

(i) provide prompt notification to Consumer Data Service Provider of any change in address or office location where Consumer Data are or will be accessible, which location is subject to an onsite visit of the new location by Consumer Data Service Provider or its designated representative; and

(j) in the event Merchant has a Security Incident involving Consumer Data, Merchant will notify oneapp and Consumer Data Service Provider as soon as possible, but in no event more than twenty-four (24) hours following the Security Incident, and: (i) fully cooperate with oneapp and Consumer Data Service Provider in a security assessment process; (ii) promptly remediate any finding; and (iii) take all necessary actions to prevent a recurrence. For purposes of this Section "*Security Incident*" means any suspected or actual breach, theft or unauthorized access, use, misuse, theft, vandalism, modification or transfer of or to Consumer Data or Consumer Data

9.3 If oneapp or Consumer Data Service Provider reasonably believes that Merchant has violated this Section 9, oneapp or Consumer Data Service Provider may, in addition to any other remedy authorized by the Agreement, with reasonable advance written notice to Merchant and at oneapp or Consumer Data Service Provider's sole expense, conduct, or have a third party conduct on its behalf, an audit of Merchant's network security systems, facilities, practices and procedures to the extent Consumer Data Service Provider reasonably deems necessary, including an on-site inspection, to evaluate Merchant's compliance with the data security requirements of this Section 9.

10. Security Policies and Standards

Merchant acknowledges it has received a copy of the applicable security policies and standards, and agrees to comply with the policies and procedures set forth therein, and any future new or amended policies or procedures that oneapp may from time to time make known to Merchant in writing (including electronic communication) (collectively, the "*Policy and Standards*"). Such Policy and Standards are hereby incorporated into the Agreement. Merchant understands and agrees that its compliance with the Agreement and the Policy and Standards will not relieve Merchant of the obligation to observe any other or further contractual, legal, or regulatory requirements, rules or terms applicable to the security of the Consumer Data.

11. Audit

oneapp or Consumer Data Service Provider may not more than once each calendar year, upon reasonable prior written notice to Merchant, conduct, or have a third party conduct on its behalf, at oneapp or Consumer Data Service Provider's sole expense, an audit reasonably designed to monitor Merchant's compliance with the obligations set forth in the Agreement; provided, however if oneapp or Consumer Data Service Provider has a reasonable belief that Merchant is not in compliance with one or more of the obligations of the Agreement, this restriction shall not apply. Merchant agrees that any failure to cooperate fully and promptly in the conduct of any audit requested pursuant to this Section will constitute grounds for immediate suspension of the Screening SaaS in whole or in part under, or termination of, the Agreement.

12. Payment

Merchant will pay oneapp for all Consumer Data requested by Merchant on behalf of itself or End Users according to the terms and conditions of the applicable Order Form(s). If you use any SaaS not set forth in the applicable Order Form(s), you will be charged the applicable rates available at https://withoneapp.com/#pricing, and will pay any applicable taxes and charges for any other services rendered by Consumer Data Service Provider.

13. Reporting of Information

Merchant understands that Consumer Data Service Provider is under no obligation, and will refuse, to accept information from Merchant, regarding Merchant's accounts, for inclusion in Consumer Data.

14. Promotion and Training

14.1 Consumer Data Service Provider must approve prior to use any Merchant-created advertising, marketing and promotional material that describes Consumer Data in detail or which refers to the nature or capabilities of Consumer Data Service Provider or Consumer Data, or otherwise mentions or refers to Consumer Data Service Provider by name.

14.2 Merchant is responsible for training End Users in the use of Consumer Data and for developing and distributing training materials as it reasonably believes are necessary or useful to enable End Users to use Consumer Data. Consumer Data Service Provider will have the opportunity to review and the right to approve material regarding Consumer Data that Merchant proposes to provide to End Users.

15. Release and Covenant with Respect to Consumer Data

Merchant recognizes that the accuracy or completeness of any information furnished is not guaranteed by Consumer Data Service Provider, and Merchant releases Consumer Data Service Provider and its directors, officers, employees, agents, employees, independent contractors, successors and assigns (the "*Consumer Data Service*

Provider Entities") from liability for any acts or omissions in connection with the preparation of Consumer Data and from any loss or expense suffered by Merchant or Merchant's Subscribers or users resulting directly or indirectly from Consumer Data. Merchant, on its own and on behalf of its Subscribers, covenants not to sue or maintain any claim, cause of action, demand, cross-action, counterclaim, third-party action or other form of pleading against Consumer Data Service Provider or Consumer Data Service Provider Entities arising out of or relating in any way to the currency, accuracy or inaccuracy, validity or nonvalidity, or completeness of any of the Consumer Data.

16. DISCLAIMER OF WARRANTIES

CONSUMER DATA SERVICE PROVIDER MAKES NO REPRESENTATIONS, WARRANTIES OR GUARANTEES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, RESPECTING CONSUMER DATA SERVICE PROVIDER'S CREDIT REPORTING SYSTEM (THE "*SYSTEM*") OR ANY OTHER CONSUMER DATA, MACHINERY, EQUIPMENT, MATERIALS, PROGRAMMING AIDS OR OTHER ITEMS UTILIZED BY CONSUMER DATA SERVICE PROVIDER IN CONNECTION WITH OR RELATED TO, OR RESPECTING THE CURRENCY, ACCURACY OR COMPLETENESS OF, ANY CONSUMER DATA FURNISHED BY CONSUMER DATA SERVICE PROVIDER TO MERCHANT OR TO ANY CONSUMERS OF MERCHANT.

17. Indemnification by Merchant

Merchant will indemnify and hold harmless Consumer Data Service Provider and the Consumer Data Service Provider Entities from and against any and all liabilities, claims, losses, demands, actions, causes of action, damages, expenses (including, without limitation, attorneys' fees and costs of litigation), or liability, arising from or in any manner related to any allegation, claim, demand or suit, whether or not meritorious, brought or asserted by any third party arising out of or resulting from any actual or alleged negligence or intentional misconduct of Merchant, whether or not any negligence of Consumer Data Service Provider is alleged to have been contributory thereto, the failure of Merchant to duly and fully perform its obligations under the Agreement, the failure of Merchant to insure the reliable and accurate delivery of Consumer Data, misuse or improper access to Consumer Data by Merchant or Qualified Subscribers, or the failure of Merchant to comply with applicable laws or regulations.

18. Confidentiality

Merchant acknowledges that Consumer Data Service Provider is the owner of the System and of all interests, programs, codes, software, software documentation or other appurtenances related to it and derived from it. Merchant further acknowledges that the

System and any codes, procedures or System documentation are confidential and proprietary to Consumer Data Service Provider. Consumer Data Service Provider does not convey or transfer, nor does Merchant obtain any right or interest in, any of the programs, systems, data, material, or credit information utilized or provided by Consumer Data Service Provider in the performance of the Agreement. During the term of the Agreement and thereafter, Merchant will maintain, and Merchant will cause its directors, officers, employees and agents to maintain, in strict confidence and not to disclose to any other person or entity any information, including Consumer Data (except as authorized by the Agreement), materials and know-how as may be provided to Merchant by Consumer Data Service Provider during the term of the Agreement and to take any actions necessary to protect against disclosure thereof. Merchant will make no use of any information, including Consumer Data, materials and know-how whatsoever except solely for the purpose of the Agreement, in accordance with the terms and during the existence of the Agreement. Upon the termination of the Agreement, Merchant will (i) return to Consumer Data Service Provider or (ii) destroy all copies and partial copies of manuals, materials and documents pertaining to Consumer Data Service Provider or the System obtained from Consumer Data Service Provider during the term of the Agreement. Upon the request of Consumer Data Service Provider, an officer of Merchant will confirm in writing that all such information has been returned or destroyed.

19. Release and Covenant with Respect to Consumer Data

19.1 Merchant acknowledges that Consumer Data Service Provider is the owner of the System and of all interests, programs, codes, software, software documentation or other appurtenances related to it and derived from it. Merchant further acknowledges that the System and any codes, procedures or System documentation are confidential and proprietary to Consumer Data Service Provider. Consumer Data Service Provider does not convey or transfer, nor does Merchant obtain any right or interest in, any of the programs, systems, data, material, or credit information utilized or provided by Consumer Data Service Provider in the performance of the Agreement. During the term of the Agreement and thereafter, Merchant will maintain, and Merchant will cause its directors, officers, employees and agents to maintain, in strict confidence and not to disclose to any other person or entity any information, including Consumer Data (except as authorized by the Agreement), materials and know-how as may be provided to Merchant by Consumer Data Service Provider during the term of the Agreement and to take any actions necessary to protect against disclosure thereof. Merchant will make no use of any information, including Consumer Data, materials and know-how whatsoever except solely for the purpose of the Agreement, in accordance with the terms and during the existence of the Agreement. Upon the termination of the Agreement, Merchant will (i) return to Consumer Data Service Provider or (ii) destroy all copies and partial copies of manuals, materials and documents pertaining to Consumer Data Service

Provider or the System obtained from Consumer Data Service Provider during the term of the Agreement. Upon the request of Consumer Data Service Provider, an officer of Merchant will confirm in writing that all such information has been returned or destroyed.

19.2 Merchant acknowledges that its failure to comply with this Section 18 will give rise to irreparable injury to Consumer Data Service Provider which cannot be adequately compensated in damages and that Consumer Data Service Provider may seek equitable, injunctive relief to prevent or restrain non-compliance with Section 18, together with any other remedies which may be available to Consumer Data Service Provider.

20. Additional Terms for Vantagescore

20.1 Merchant will request VantageScores only for Merchant's and its End Users' exclusive use. The VantageScores may be stored solely for Merchant's and End Users' use in furtherance of Merchant's or the End Users' original purpose for obtaining the VantageScores.

20.2 Neither Merchant nor End Users shall use the VantageScores for model development or model calibration, except in compliance with the following conditions: (1) the VantageScores may only be used as an independent variable in custom models; (2) only the raw archived VantageScore and VantageScore segment identifier will be used in modeling (*i.e.*, no other VantageScore information including, but not limited to, adverse action reasons, documentation, or VantageScorecards will be used); and (3) Merchant's or End Users' depersonalized analytics and/or depersonalized third party modeling analytics performed on behalf of Merchant or End Users, using VantageScores, will be kept confidential and not disclosed to any third party other than as expressly provided for below in subsection (ii), (iv), (v) and/or (vi) of Subsection 19.4 below.

20.3 Neither Merchant nor End User shall reverse engineer the VantageScore.

20.4 All VantageScores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any person or entity, except: (i) to those employees, agents, and independent contractors of Merchant or End Users with a need to know and in the course of their employment; (ii) to those third party processing agents and other contractors of Merchant or End Users who have executed an agreement that limits the use of the VantageScores by the third party only to the use permitted to Merchant or End Users and contains the prohibitions at least as restrictive as those set forth herein; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the VantageScore (provided, that, accompanying reason codes are not required to the extent permitted by law); (iv) to government regulatory agencies; (v) to ratings agencies, dealers, investors and other third parties for the purpose of evaluating assets or investments (e.g., securities) containing or based on obligations of the

consumers to which the VantageScores apply (e.g., mortgages, student loans, auto loans, credit cards), provided that, as it relates to this subsection (v), (a) Merchant or End Users may disclose VantageScores only in aggregated formats (e.g., averages and comparative groupings) that do not reveal individual VantageScores, (b) neither Merchant nor End Users shall provide any information that would enable a recipient to identify the individuals to whom the VantageScores apply, and (c) Merchant or End Users shall enter into an agreement with each recipient that limits the use of the VantageScores to evaluation of such assets or investments; or (vi) as required by law.

20.5 Merchant agrees, and shall cause its End Users to agree, that the trademarks, trade names, product names, brands, logos, and service marks ("*Marks*") for VantageScore credit scores and credit scoring models will remain the sole property of VantageScore Solutions, LLC. Merchant and its Qualified Subscriber obtain a limited, non-exclusive, non-transferable, royalty free license to use and display the Marks in connection with the activities solely permitted by the Agreement. The use of the Marks under the preceding license is limited to use only in connection with the Services covered by the Agreement, and the Merchant agrees, and shall cause its End Users to agree, not to use the Marks in connection with any products or services not covered by the Agreement. Any use of the Marks is subject to VantageScore Solutions, LLC's prior written authorization. Merchant further agrees, and shall cause its End Users to further agree, to include the Marks in all advertising and marketing materials which reference the VantageScores or the Vantage models and to comply with the VantageScore Trademark Policy and Brand Guidelines, which may be changed from time to time upon written notice. All use of the Marks will accrue solely to the benefit of VantageScore Solutions, LLC."

21. Compliance with Laws

Merchant will comply with applicable federal and state laws, rules and regulations relating to Merchant's performance of its obligations under the Agreement including, but not limited to, all applicable consumer financial protection laws. In addition, Merchant shall not engage in any unfair, deceptive, or abusive acts or practices.

22. Relationship of Parties

The relationship of the parties established by the Agreement is solely that of independent contractors. Neither party is the representative or agent of the other for any purpose and neither has power or authority to act as agent for or to represent, act for, bind, or otherwise create or assume any obligation on behalf of the other.

23. No Third-Party Benefits

Consumer Data Service Provider and Merchant acknowledge and intend that the Agreement was entered into solely for the respective benefit of each of them and their respective successors and assigns, and nothing in the Agreement will be

construed as giving any person, firm, corporation or other entity (including any Subscriber of Merchant), other than the parties to the Agreement and their respective successors and permitted assigns, any right, remedy or claim under or in respect of the Agreement or any of its provisions.

24. Assignment

Consumer Data Service Provider may assign the Agreement or any rights or obligations under the Agreement to an entity that is controlled by, controls or is under common control with Consumer Data Service Provider. Due to the special and unique purposes of the Agreement, neither the Agreement nor any rights or obligations in it, nor any Agreements for Service or any rights or obligations in them, are assignable by Merchant without the prior written consent of Consumer Data Service Provider (which consent will not be unreasonably withheld). Any dissolution, merger, consolidation or other reorganization of Merchant, the sale or other transfer of all or substantially all of the assets or properties of Merchant, or the sale or other transfer of a 50% or more interest in the outstanding voting or other equity interest of Merchant by any person, or group of persons acting in concert, shall constitute an assignment of the Agreement for all purposes of this Section 23. Any attempt that is contrary to the terms of this section to assign the Agreement or to delegate or otherwise transfer in any manner any rights or obligations arising under it will be void.

25. Term and Termination

25.1 The Agreement will begin on the Effective Date and continue until either party provides ten (10) days prior written notice of termination of the Agreement to the other party. Such written notice of termination shall be effective regardless of any pricing commitments the parties may have entered into during the term of the Agreement. Notwithstanding the foregoing, if Merchant is delinquent in the payment of charges, violates the FCRA or other applicable law or violates a material term of the Agreement, Consumer Data Service Provider may, at its election, discontinue providing services to Merchant and terminate the Agreement immediately by written notice to Merchant. In the event of termination of the Agreement, the obligations of Sections 2 (final paragraph only), 7, 8, 9, 10, 11, 12, 15, 16, 17, 18, 22, 24, 27, and 28 will remain in full force and effect.

25.2 Notwithstanding anything to the contrary in the Agreement, if the continued provision of the Consumer Data or any affected component thereof becomes impossible, impractical, or undesirable due to a change in applicable federal, state or local laws or regulations, as determined by Consumer Data Service Provider in its reasonable judgment, or due to circumstances imposed by Consumer Data Service Provider's third party vendors or data sources, or due to a change in Consumer Data Service Provider's policies relating to compliance with law and/or data security, Consumer Data Service Provider may either (a) cease to provide the Consumer Data or any affected component thereof within, or pertaining to persons residing

within, the affected jurisdiction, or (b) establish new prices which will apply to the Consumer Data or any affected component thereof when provided or delivered within, or pertaining to persons residing within, the affected jurisdiction, which prices will be reasonably calculated to cover the costs incurred by Consumer Data Service Provider in complying with the applicable laws or regulations or circumstances imposed by third party vendors and will become effective on the date specified in such notice unless Merchant objects in writing, in which case Consumer Data Service Provider may exercise its rights under clause (a) above. Consumer Data Service Provider will attempt to provide written notice of its actions as far in advance of the effective date as is reasonably possible under the circumstances.

25.3 No Damages or Indemnification for Termination. Neither party shall be liable to the other party for any costs or damages of any kind, including direct, special, exemplary, punitive, indirect, incidental or consequential damages, or for indemnification, solely on account of the lawful termination of the Agreement, even if informed of the possibility of such damages.

26. No Third-Party Benefits

Neither party will be liable to the other by reason of any failure or delay of performance, whether foreseen or unforeseen, hereunder (except failure to pay any amount when due) if such failure arises out of causes beyond the non-performing party's reasonable control, including but not limited to governmental emergency orders, judicial or governmental action, emergency regulations, sabotage, riots, vandalism, labor strikes or disputes, acts of God, (e.g. fire, flood, inclement weather, epidemic, or earthquake), war or act of terrorism, electrical failure, mechanical failure, major computer hardware or software failures, equipment delivery delays, acts of third parties.

27. Notices

All notices to Consumer Data Service Provider under the Agreement will be provided via email to legalnotices@withoneapp.com. All notices from Consumer Data Service Provider to Merchant will be provided via email to the relevant contact(s) you designate in your account. The parties may, by notice given under this section, designate additional or different addresses to which notices must be sent.

28. Severability

In the event any provision of the Agreement is found to be illegal or unenforceable under applicable law, by a court having jurisdiction, such provision shall be unenforceable only to the extent necessary to make it enforceable without invalidating any of the remaining provisions of the Agreement.

Qualified Subscriber Terms and Conditions

With One App, Inc. (“CRA”) acts as a reseller of the Third Party Services set forth below in Section 1. If Merchant purchases any Third Party Services from CRA, such Third Party Services are solely provided by Equifax Information Services, LLC (“Equifax”). Merchant’s use of any Third Party Services is subject to these Qualified Subscriber Terms and Conditions. CRA is not a party to any Qualified Subscriber Terms and Conditions, and is not liable to Merchant for any Third Party Services whatsoever.

PLEASE REVIEW THESE QUALIFIED SUBSCRIBER TERMS AND CONDITIONS CAREFULLY. ONCE ACCEPTED, THESE QUALIFIED SUBSCRIBER TERMS AND CONDITIONS BECOME A BINDING LEGAL COMMITMENT BETWEEN YOU AND EQUIFAX. IF YOU DO NOT AGREE TO THESE QUALIFIED SUBSCRIBER TERMS, YOU SHOULD NOT ACCEPT THEM, OR USE THE THIRD PARTY SERVICES (AS DEFINED IN SECTION 1 BELOW).

Third Party Provider may update these Third Party Terms from time to time. The updated version of Third Party Terms will be available at https://legal.withoneapp.com. Merchant’s continued use of the Third Party Services constitutes Merchant’s acceptance of the updated Third Party Terms. CRA recommends that Merchant periodically reviews these Third Party Terms.

Notices from Third Party Provider to you will be provided via Merchant’s account, or e-mail to the relevant contact(s) you designate in your account.

By accepting or otherwise agreeing to these Qualified Subscriber Terms and Conditions, Merchant affirms that it is a “Qualified Subscriber” to the Third Party Services provided by Equifax.

Equifax Information Services (as defined below) will be received by Qualified Subscriber through CRA subject to the following conditions (the “Terms and Conditions”):

1. Any information services and data originating from Equifax (the “Equifax Information Services” or “Equifax Information”) will be requested only for Subscriber's exclusive use and held in strict confidence except to the extent that disclosure to others is required or permitted under the last sentence of this Paragraph. Only designated representatives of Qualified Subscriber will request Equifax Information Services on Qualified Subscriber’s employees, and employees are forbidden to obtain consumer reports on themselves, associates or any other persons except in the exercise of their official duties. Qualified Subscriber will not disclose Equifax Information to the subject of the report except as permitted or required by law, but will refer the subject to Equifax.

2. Qualified Subscriber will hold Equifax and all its agents harmless on account of any expense or damage arising or resulting from the publishing or other disclosure of Equifax Information by Qualified Subscriber, its employees or agents contrary to the conditions of Paragraph 1 or applicable law.

3. Recognizing that information for the Equifax Information Services is secured by and through fallible human sources and that, for the fee charged, Equifax cannot be an insurer of the accuracy of the Equifax

Information Services, Qualified Subscriber understands that the accuracy of any Equifax Information Service received by Qualified Subscriber is not guaranteed by Equifax, and Qualified Subscriber releases Equifax and its affiliate companies, agents, employees, and independent contractors from liability, even if caused by negligence, in connection with the Equifax Information Services and from any loss or expense suffered by Qualified Subscriber resulting directly or indirectly from Equifax Information.

4. Qualified Subscriber will be charged for the Equifax Information Services by CRA, which is responsible for paying Equifax for the Equifax Information Services.

5. Written notice by either party to the other will terminate these Terms and Conditions effective ten (10) days after the date of that notice, but the obligations and agreements set forth in Paragraphs 1, 2, 3, 6, 7, and 8 herein will remain in force.

6. Qualified Subscriber certifies that it will order Equifax Information Services that are consumer reports, as defined by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq. ("FCRA"), only when Qualified Subscriber intends to use that consumer report information: (a) in accordance with the FCRA and all state law counterparts; and (b) for one of the following permissible purposes: (i) in connection with a credit transaction involving the consumer on whom the consumer report is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; (ii) in connection with the underwriting of insurance involving the consumer; (iii) as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; (iv) when Qualified Subscriber otherwise has a legitimate business need for the information either in connection with a business transaction that is initiated by the consumer, or to review an account to determine whether the consumer continues to meet the terms of the accounts; or (v) for employment purposes; provided, however, that QUALIFIED SUBSCRIBER IS NOT AUTHORIZED TO REQUEST OR RECEIVE CONSUMER REPORTS FOR EMPLOYMENT PURPOSES UNLESS QUALIFIED SUBSCRIBER HAS AGREED IN WRITING TO THE TERMS AND CONDITIONS OF THE EQUIFAX PERSONA SERVICE. Qualified Subscriber will comply with applicable federal and state laws, rules and regulations relating to such party's performance of its obligations under these Terms and Conditions including, but not limited to, all applicable consumer financial protection laws. In addition, Qualified Subscriber shall not engage in any unfair, deceptive, or abusive acts or practices. Qualified Subscriber will use each consumer report ordered under these Terms and Conditions for one of the foregoing purposes and for no other purpose.

7. It is recognized and understood that the FCRA provides that anyone "who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under Title 18, United States Code, imprisoned for not more than two (2) years, or both." Equifax may periodically conduct audits of Qualified Subscriber regarding its compliance with these Terms and Conditions, including, without limitation, the FCRA, other certifications and security provisions in these Terms and Conditions. Audits will be conducted by mail whenever possible and will require Qualified Subscriber to provide documentation as to permissible use of particular consumer reports. Qualified Subscriber gives its consent to Equifax to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or Qualified Subscriber's material breach of these Terms and Conditions, constitute grounds for immediate suspension of service or termination of these Terms and Conditions, notwithstanding Paragraph 5 above. If Equifax terminates these Terms and Conditions due to the conditions in the preceding sentence, Qualified Subscriber (i) unconditionally releases and agrees to hold Equifax harmless and indemnify it from and against any and all liabilities of whatever kind or nature that may arise from or relate to such termination, and (ii) covenants it will not assert any claim or cause of action of any kind or nature against Equifax in connection with such termination.

8. California Law Certification. Qualified Subscriber will refer to Exhibit 1-A in making the following certification, and Qualified Subscriber agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act.

(QUALIFIED SUBSCRIBER'S AUTHORIZED REPRESENTATIVE MUST PLACE HIS/HER INITIALS NEXT TO THE APPLICABLE SPACE BELOW)

1. Are you, Qualified Subscriber a "retail seller," as defined in Section 1802.3 of the California Civil Code and referenced in Exhibit 1-A, intending to issue credit to consumers who appear in person on the basis of an application for credit submitted in person?

_____yes

___X__no

2. If "yes" to question 1 above, do you, Qualified Subscriber, certify that you will instruct Qualified Subscriber employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person Do you, Qualified Subscriber issue credit to consumers who appear in person on the basis of an application for credit submitted in person?

_____yes

_____no

9. Vermont Certification. Qualified Subscriber will refer to Exhibit 1-A in making the following certification, and Qualified Subscriber agrees to comply with all applicable provisions under Vermont law and Applicable Vermont rules, as referenced in Exhibit 1-A.

(QUALIFIED SUBSCRIBER'S AUTHORIZED REPRESENTATIVE MUST PLACE HIS/HER INITIALS NEXT TO THE APPLICABLE SPACE BELOW)

Do you, Qualified Subscriber, certify that you will order Equifax Information Services relating to Vermont residents consisting of credit reports as defined by the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e, as amended (the "VFCRA"), only after you have received prior consumer consent specific to the purpose for which such credit report is being ordered, in accordance with VFCRA Section 2480e and Applicable Vermont Rules, referenced in Exhibit 1-A?

___X__Yes

_____No

10. Qualified Subscriber Security.

10.1. This Paragraph 10 applies to any means through which Qualified Subscriber orders or accesses the Equifax Information Services including, without limitation, system-to-system, personal computer or the Internet.

For the purposes of this Paragraph 10, the term "Authorized User" means a Qualified Subscriber employee that Qualified Subscriber has authorized to order or access the Equifax Information Services and who is trained on Qualified Subscriber's obligations under these Terms and Conditions with respect to the ordering and use of the Equifax Information Services including Qualified Subscriber's FCRA and other obligations with respect to the access and use of consumer reports.

10.2. Qualified Subscriber will, with respect to handling Equifax Information:

(a) ensure that only Authorized Users can order or have access to the Equifax Information Services and take all necessary measures to prevent unauthorized ordering of or access to the Equifax Information Services by any person other than an Authorized User for permissible purposes, including, without limitation, limiting the knowledge of the Qualified Subscriber security codes, member numbers, User IDs, and any passwords Qualified Subscriber may use to those individuals with a need to know. In addition, the User IDs must be unique to each person, and the sharing of User IDs or passwords is prohibited,

(b) ensure that Authorized Users are trained not to order consumer reports for personal reasons or provide consumer reports to third parties except as permitted by this Agreement and that any unauthorized access or use of consumer reports may subject them to civil and criminal liability under the FCRA, punishable by fines and imprisonment,

(c) ensure that secure authentication practices are utilized when accessing the Equifax Information Services , including but not limited to restricting access based on Authorized User location and only permitting access to the Equifax Information Services through Qualified Subscriber approved devices,

(d) ensure that Equifax Information is encrypted in transit with Advanced Encryption Standard (AES)-256 or an equivalent or better National Institute of Standards and Technology (NIST) approved cypher,

(e) use commercially reasonable efforts to secure Equifax Information at rest, including: (i) encrypting all Equifax Information at rest in accordance with industry accepted encryption standards; (ii) separating Equifax Information from the Internet or other public networks by firewalls configured to meet industry accepted best practices; (iii) protecting Equifax Information through multiple layers of network security, including but not limited to, industry-recognized firewalls, routers, and intrusion detection/prevention devices (IDS/IPS), (iv) securing access (both physical and network) to systems storing Equifax Information; and (v) patching servers on a timely basis with appropriate security-specific system patches, as they are available,

(f) ensure that: (i) all hard copy Equifax Information is stored in a secure manner; (ii) Equifax Information, including electronic and hard copy information, is securely destroyed when no longer needed for the Equifax Information Services; and (iii) maintain documented policies to ensure compliance with the foregoing,

(g) not allow Equifax Information to be displayed via the Internet unless utilizing, at a minimum, a three-tier architecture configured in accordance with industry best practices,

(h) use commercially reasonable efforts to establish procedures and logging mechanisms for systems and networks that will allow tracking and analysis in the event there is a compromise, and maintain an audit trail history,

(i) provide prompt notification to Equifax of any change in address or office location where Equifax Information Services are or will be accessible, which location is subject to an onsite visit of the new location by Equifax or its designated representative, and

(j) in the event Qualified Subscriber has a Security Incident involving Equifax Information, Qualified Subscriber will notify Equifax as soon as possible, but in no event more than twenty-four (24) hours following the Security Incident, and: (i) fully cooperate with Equifax in a security assessment process; (ii) promptly remediate any finding; and (iii) take all necessary actions to prevent a recurrence.

For purposes of this Section “Security Incident” means any suspected or actual breach, theft or unauthorized access, use, misuse, theft, vandalism, modification or transfer of or to Equifax Information Services or Equifax Information.

11. Qualified Subscriber may access, use and store Equifax Credit Information only at or from locations within the territorial boundaries of the United States, Canada, and the United States territories of American Samoa, Guam, the Northern Mariana Islands, Puerto Rico, and the U. S. Virgin Islands (the “Permitted Territory”). Qualified Subscriber may not access, use or store Equifax Credit Information at or from, or send it to any location outside of the Permitted Territory without first obtaining Equifax’s prior written consent and entering into such written agreements as Equifax may require. Notwithstanding the foregoing, Qualified Subscriber is prohibited from Processing Equifax Information from an Embargoed Country. “Embargoed Country” means any country or geographic region subject to comprehensive economic sanctions or embargoes administered by OFAC or the European Union.

12. These Terms and Conditions will be governed by and construed in accordance with the laws of the State of Georgia, without giving effect to its conflicts of laws provisions. These Terms and Conditions constitute the entire agreement of the parties with respect to Qualified Subscriber receiving Equifax Information Services and no changes in these Terms and Conditions may be made except in writing by an officer of Equifax.

___X___ Qualified Subscriber has read and understands these Terms and Conditions. (To be initialed by the person signing on behalf of Subscriber.)

___X___ Qualified Subscriber has read the attached Exhibit 1-B “Notice to Users of Consumer Reports, Obligations of Users” which explains Qualified Subscriber’s obligations under the FCRA as a user of consumer report information. (To be initialed by the person signing on behalf of Qualified Subscriber.)

EXHIBIT 1-A to CRA Qualified Subscriber Terms and Conditions

State Compliance Matters

California Retail Seller Compliance. Provisions of the California Consumer Credit Reporting Agencies Act specifically, as amended effective July 1, 1998, will impact the provision of consumer reports to Qualified Subscriber if Qualified Subscriber is a “retail seller” under California law and Qualified Subscriber intends to request consumer reports from Equifax about consumers applying in person for credit. California Civil Code § 1802.3 defines a “retail seller” as (“a person engaged in the business of selling goods or services to retail buyers” ,” defined in §1802.4 as “a person who buys goods or obtains services from a retail seller in a retail installment sale and not principally for the purpose of resale”).

Under the foregoing circumstances, before delivering a consumer report to Qualified Subscriber, Equifax must match at least three items of a consumer’s identification within the file maintained by Equifax with the information provided to Equifax by Qualified Subscriber in connection with the in-person credit transaction. Compliance with this law further includes Qualified Subscriber’s inspection of the photo identification of each consumer who applies for in-person credit, mailing extensions of credit to consumers responding to a mail solicitation at specified addresses, taking special actions regarding a consumer’s presentment of a police report regarding fraud, and acknowledging consumer demands for reinvestigations within certain time frames.

If Qualified Subscriber is a “retail seller” and intends to request consumer reports from Equifax about consumers applying in person for credit, Qualified Subscriber certifies that it will instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person. If Qualified Subscriber is not currently, but subsequently becomes a “retail seller”, Qualified

Subscriber agrees to provide written notice to Equifax prior to ordering credit reports in connection with an in-person credit transaction, and agrees to comply with the requirements of the California law as outlined in this Section, and with the specific certifications set forth herein.

Qualified Subscriber certifies agrees that, as a "retail seller" who intends to request consumer reports from Equifax about consumers applying in person for credit, it will either (a) acquire a new customer number for use in processing consumer report inquiries that result from in-person credit applications covered by California law, with the understanding that all inquiries using this new customer number will require that Qualified Subscriber supply at least three items of identifying information from the applicant; or (b) contact Qualified Subscriber's Equifax sales representative to ensure that Qualified Subscriber's existing number is properly coded for these transactions.

Vermont Fair Credit Reporting Compliance. Provisions of the Vermont Fair Credit Reporting Statute, 9 V.S.A. § 2480e, as amended (the "VFCRA") and applicable Vermont Rules (specifically, CVR 06-031-012 Rule CF 112 - Fair Credit Reporting, CF

112.03 Consumer Consent ("Applicable Vermont Rules")), prohibit Qualified Subscriber from obtaining credit reports, as defined by the VFCRA, without prior consumer consent specific to the purpose for which such credit report is being ordered as specified in VFCRA § 2480e and Applicable Vermont Rules. If Qualified Subscriber designated in Section I.3 of the Agreement that Qualified Subscriber does not comply with these provisions of the VFCRA and Applicable Vermont Rules by obtaining the requisite consumer consent from Vermont consumers, then provision of credit reports, as defined by the VFCRA, to Qualified Subscriber will be impacted. If Qualified Subscriber designated in Section I.3 of this Agreement that Qualified Subscriber is in compliance with VFCRA § 2480e and Applicable Vermont Rules, Qualified Subscriber shall provide notice to Equifax should its ability to certify compliance with VFCRA § 2480e and Applicable Vermont Rules has changed. Reviews by Equifax pursuant to the section of this Agreement authorizing reviews or audits of Qualified Subscriber's permissible purpose to obtain consumer reports shall require, as applicable, evidence of specific consumer consent obtained from Vermont consumers as required by the VFCRA and Applicable Vermont Rules.

EXHIBIT 1-B to CRA Qualified Subscriber Terms and Conditions
NOTICE TO USERS OF CONSUMER REPORTS:
OBLIGATIONS OF USERS UNDER THE FCRA

All users of consumer reports must comply with all applicable regulations. Information about applicable regulation currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfainance.gov/learnmore.

The Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Consumer Financial Protection Bureau's (CFPB) website at www.consumerfinance.gov/learnmore. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the CFPB's website. Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If

you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 contains a list of the permissible purposes under the law. These are:

As ordered by a court or a federal grand jury subpoena. Section 604(a)(1)

As instructed by the consumer in writing. Section 604(a)(2)

For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)

For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Sections 604(a)(3)(B) and 604(b)

For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)

When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)

To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)

To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)

For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)

For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604 (a)(5)

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making "prescreened" unsolicited offers of credit or insurance. Section 604(c). The particular obligations of users of "prescreened" information are described in Section VII below.

B. Users Must Provide Certifications

Section 604(f) prohibits any person from obtaining a consumer report from a consumer reporting agency (CRA) unless the person has certified to the CRA the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers When Adverse Actions Are Taken

The term "adverse action" is defined very broadly by Section 603. "Adverse actions" include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact as defined by Section 603(k) of the FCRA – such as denying or canceling credit or insurance, or denying

employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action as defined by the FCRA that is based at least in part on information contained in a consumer report, Section 615(a) requires the user to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following:

The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.
A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days.
A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

2. Adverse Actions Based on Information Obtained From Third Parties Who Are Not Consumer Reporting Agencies

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within

60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained From Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure as set forth in I.C.1 above.

D. <u>Users Have Obligations When Fraud and Active Duty Military Alerts are in Files</u>

When a consumer has placed a fraud alert, including one relating to identity theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extended fraud

alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed. Federal regulations are available at www.consumerfinance.gov/learnmore.

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. Federal regulations have been issued that cover disposal.

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

If a person uses a consumer report in connection with an application for, or a grant, extension, or provision of, credit to a consumer on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person, based in whole or in part on a consumer report, the person must provide a risk-based pricing notice to the consumer in accordance with regulations prescribed by the CFPB.

Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) ("Notice to the Home Loan Applicant").

III. OBLIGATIONS OF USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

A. Employment Other Than in the Trucking Industry

If information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

· Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.

· Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.

· Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.

· Before taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of consumer's rights. (The user should receive this summary from the CRA.) A Section 615(a) adverse action notice should be sent after the adverse action is taken.

An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2)

The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry

Special rules apply for truck drivers where the only interaction between the consumer and the potential employer is by mail, telephone, or computer. In this case, the consumer may provide consent orally or electronically, and an adverse action may be made orally, in writing, or electronically. The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by an entity or person that is a consumer reporting agency. Consumers who are the subjects of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

• The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)

• The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure described below.

• Upon the written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed, or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with Federal, state or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long as the employer or its agent complies with the procedures set forth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes – or in connection with a credit transaction (except as provided in federal regulations – the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Sections 603(l), 604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain preestablished criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in a consumer's CRA file was used in connection with the transaction.

- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.

- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.

- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. The statement must include the address and toll-free telephone number of the appropriate notification system.

In addition, once the CFPB has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The relevant regulation is 12 CFR 1022.54.

VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

Section 607(e) requires any person who obtains a consumer report for resale to take the following steps:

- Disclose the identity of the end-user to the source CRA.

- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.

• Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:

(1) the identity of all end-users;

(2) certifications from all users of each purpose for which reports will be used; and

(3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

Under Section 611(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CRA for reinvestigation. When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

C. Fraud Alerts and Resellers

Section 605A(f) requires resellers who receive fraud alerts or active duty alerts from another consumer reporting agency to include these in their reports.

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCRA can result in state government or federal government enforcement actions, as well as private lawsuits. Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Section 619.

The CFPB's Web site, www.consumerfinance.gov/learnmore, has more information about the FCRA, including publications for businesses and the full text of the FCRA.

Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1681 et seq.:

Section 602	15 U.S.C. 1681	Section 604	15 U.S.C. 1681b
Section 603	15 U.S.C. 1681a	Section 605	15 U.S.C. 1681c
Section 605A	15 U.S.C. 1681cA	Section 617	15 U.S.C. 1681o
Section 605B	15 U.S.C. 1681cB	Section 618	15 U.S.C. 1681p
Section 606	15 U.S.C. 1681d	Section 619	15 U.S.C. 1681q
Section 607	15 U.S.C. 1681e	Section 620	15 U.S.C. 1681r
Section 608	15 U.S.C. 1681f	Section 621	15 U.S.C. 1681s
Section 609	15 U.S.C. 1681g	Section 622	15 U.S.C. 1681s-1
Section 610	15 U.S.C. 1681h	Section 623	15 U.S.C. 1681s-2
Section 611	15 U.S.C. 1681i	Section 624	15 U.S.C. 1681t
Section 612	15 U.S.C. 1681j	Section 625	15 U.S.C. 1681u
Section 613	15 U.S.C. 1681k	Section 626	15 U.S.C. 1681v
Section 614	15 U.S.C. 1681l	Section 627	15 U.S.C. 1681w
Section 615	15 U.S.C. 1681m	Section 628	15 U.S.C. 1681x
Section 616	15 U.S.C. 1681n	Section 629	15 U.S.C. 1681y

CRA Agreement for Service Consumer Reporting Agencies LRD 10.25.23 9
Templates/USIS/Broker and Reseller
RES-24-47832

VantageScore, v3,v4SM - is a tri-bureau credit risk model developed using one algorithm across sample data common to all three credit bureaus.

The following additional terms and conditions apply to Qualified Subscriber's receipt and use of VantageScore: End User Terms for VantageScore – Qualified Subscriber will request VantageScores only for Qualified Subscriber's exclusive use. Qualified Subscriber may store VantageScores solely for Qualified Subscriber's own use in furtherance of Qualified Subscriber's original purpose for obtaining the VantageScores. Qualified Subscriber shall not use the VantageScores for model development or model calibration, except in compliance with the following conditions: (1) the VantageScores may only be used as an independent variable in custom models; (2) only the raw archived VantageScore and VantageScore segment identifier will be used in modeling (i.e., no other VantageScore information including, but not limited to, adverse action reasons, documentation, or scorecards will be used); and (3) Qualified Subscriber's depersonalized analytics and/or depersonalized third party modeling analytics performed on behalf of Qualified Subscriber, using VantageScores, will be kept confidential and not disclosed to any third party other than as expressly provided for below in (ii), (iv), (v) and/or (vi) of this paragraph). Qualified Subscriber shall not reverse engineer the VantageScore. All VantageScores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any Person, except: (i) to those employees, agents, and independent contractors of Qualified Subscriber with a need to know and in the course of their employment; (ii) to those third party processing agents and other contractors of Qualified Subscriber who have executed an agreement that limits the use of the VantageScores by the third party only to the use permitted to Qualified Subscriber and contains the prohibitions at least as restrictive as those set forth herein regarding model development, model calibration, reverse engineering and confidentiality; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the VantageScore (provided, that, accompanying reason codes are not required to the extent permitted by law); (iv) to government regulatory agencies; (v) to ratings agencies, dealers, investors and other third parties for the purpose of evaluating assets or investments (e.g., securities) containing or based on obligations of the consumers to which the VantageScores apply (e.g., mortgages, student loans, auto loans, credit cards), provided that, as it relates to this subsection (v), (a) Qualified Subscriber shall not provide any information that would enable a recipient to identify the individuals to whom the VantageScores apply, and (b) Qualified Subscriber shall enter into an agreement with each recipient that limits the use of the VantageScores to evaluation of such assets or investments; or (vi) as permitted with the express, written authorization from VantageScore Solutions, LLC, or as otherwise required by law. Qualified Subscriber agrees that the trademarks, trade names, product names, brands, logos, and service marks ("Vantage Marks") for VantageScore credit scores and credit scoring models will remain the sole property of VantageScore Solutions, LLC. Qualified Subscriber obtains a limited, non-exclusive, non-transferable, royalty free license to use and display the Vantage Marks in connection with the activities solely permitted by this Agreement. The use of the Vantage Marks under the preceding license is limited to use only in connection with the Services covered by this Agreement, and the Qualified Subscriber expressly agrees not to use the Vantage Marks in connection with any products or services not covered by this Agreement. Any use of the Vantage Marks is subject to VantageScore Solutions, LLC's prior written authorization. Qualified Subscriber further agrees it will include the Vantage Marks in all advertising and marketing materials which reference the VantageScores or Vantage models and it will comply with the VantageScore Trademark Policy and Brand Guidelines, which may be changed from time to time upon written notice. All use of the Vantage Marks will accrue solely to the benefit of VantageScore Solutions, LLC

Additional Terms and Conditions Applicable for Credit Score Information Services, other than FICO Scores:

(a) Disclosure of Scores. Qualified Subscriber will hold all information received from Equifax in connection with any Score received from Equifax or CRA under the CRA Agreement for Service in strict confidence and will not disclose that information to the consumer or to others except as required by law or as explicitly permitted in the CRA Agreement for Service. Qualified Subscriber may provide the principal factors contributing to the Score to the subject of the report when those principal factors are the basis of Qualified Subscriber's adverse action against the subject consumer. Qualified Subscriber must describe the principal factors in a manner which complies with Regulation B of the ECOA.

(b) ECOA Statements. Subject to the terms below, Equifax reasonably believes that, (1) the scoring algorithms used in the computation of the Scores are empirically derived from consumer credit information from Equifax's consumer credit reporting database, and are demonstrably and statistically sound methods of rank ordering candidate records from the Equifax consumer credit database for the purposes for which the Score was designed particularly, and it is intended to be an "empirically derived, demonstrably and statistically sound credit scoring system" as defined in Regulation B. and (2) the scoring algorithms comprising the Score, except as permitted, do not use a "prohibited basis," as such phrase is defined in Regulation B. This section and Equifax's statements herein are contingent on Qualified Subscriber's use of the Score for the purpose for which it was designed, in compliance with the service definitions described in the CRA Agreement for Service. Qualified Subscriber must validate the Score on its own records. Qualified Subscriber will be responsible for meeting its requirements under the ECOA and Regulation B and will not use any Score in any manner that violates any fair lending laws.

(c) Release. Equifax does not guarantee the predictive value of the Score with respect to any individual, and does not intend to characterize any individual as to credit capability. Neither Equifax nor its directors, officers, employees, agents, subsidiary and affiliated companies, or any third-party contractors, licensors or suppliers of Equifax will be liable to Qualified Subscriber for any damages, losses, costs or expenses incurred by Qualified Subscriber resulting from any failure of a Score to accurately predict the credit worthiness of Qualified Subscriber's applicants or customers. In the event the Score is not correctly applied by Equifax to any credit file, Equifax's sole responsibility will be to reprocess the credit file through the Score at no additional charge.

Fee and Payment Authorization Agreement:

A. Generally. You may be required to pay fees to access or use certain features of the SaaS for your "Transactions." **All fees are in U.S. dollars and are non-refundable**. If we change the fees for all or part of any of the SaaS, including by adding fees or charges, we will provide you advance notice of those changes. If you do not accept the changes, we may discontinue providing the applicable part of the SaaS to you. Our authorized third-party payment processors will charge the payment method you specified at the time of purchase or as agreed to as part of the selected SaaS. You authorize us to charge all fees as described on your checkout screen in the SaaS and in the Terms of Service, which includes the Payments SaaS requirements and the SaaS and Area Specific Requirements for the SaaS you select to that payment method. If you pay any fees with a credit card, we may seek pre-authorization of your credit card account before your purchase to verify that the credit card is valid and has the necessary funds or credit available to cover your purchase.

B. Subscriptions. The SaaS may include features that allow for automatically recurring payments for periodic charges ("Subscription SaaS"). If you decide to activate a Subscription SaaS, you authorize us to periodically charge, on a going-forward basis and until cancellation of either the recurring payments or your account, all accrued sums on or before the payment due date for the accrued sums. The subscription will continue unless and until you cancel your subscription, or we terminate it. You must cancel your Subscription SaaS before it renews in order to avoid billing of the next periodic subscription fee to your account. We will bill the periodic subscription fee to the payment method you provide to us during registration (or to a different payment method if you change your payment information). We may change the subscription fee for any subsequent subscription period but will provide you advance notice of any increase before it applies. Unless otherwise stated in the Terms of Service, you may cancel a Subscription SaaS through the settings page in your account, or by contacting us at support@withoneapp.com.

C. Transactions with Consumers. At Merchant's sole discretion, Merchant may charge Consumer a one-time "Application Fee" for facilitating the formation of an application to lease an apartment or housing unit between a Consumer and a housing provider. Your Application Fee can vary, depending on a variety of factors. **Consumer will be charged the Application Fee shown and communicated to the Consumer on the oneapp platform before the Consumer elects to accept the Transaction.** The Application Fee is not refundable.

D. Chargebacks. Merchant assumes sole and exclusive responsibility for Transactions. Merchants are solely responsible for verifying the identity of End Users, which include Consumers, and of the eligibility of a presented payment card used to purchase Merchant's services, and oneapp does not guarantee or assume any liability for Transactions authorized and completed that may later be reversed or charged back (see Payments SaaS section 25 (Your Liability and Indemnification Concerning Liabilities)). **Merchant is solely responsible for all reversed or charged back transactions regardless of the reason for, or timing of the reversal or chargeback**. oneapp or Stripe Inc. ("the Processor") may add or remove one or more types of Payment Networks or Cards, in their sole discretion, at any time, without prior notice to you.

E. Authorization for ACH Debits and Credits and Other Transactions. If and to the extent permitted by oneapp in its sole discretion, End Users may pay Fees owed from their designated bank accounts. Subject to oneapp's eligibility requirements, if you elect to pay Fees or any other amounts owed via ACH transfers from your designated bank account, you hereby authorize us to electronically debit and, if necessary, electronically credit your designated bank account via ACH for such amounts pursuant to the Terms of Service, which includes the Payments SaaS and your SaaS and Area Specific Requirements, and you agree to comply with the ACH rules issued by the National Automated Clearing House ("NACHA") and all applicable laws, including, but not limited to, the federal Bank Secrecy Act, the U.S.A. Patriot Act, and economic sanctions overseen by the Office of Foreign Assets Control (OFAC). Your authorization for ACH transfers contained in this Section E will remain in full force and effect until you notify us that you wish to revoke your authorization by removing your bank account information from your account settings page or by contacting customer support at support@withoneapp.com.

You must notify us of any change in your designated bank account's information at least five (5) business days before any such change by updating your bank account information in your Profile or by contacting customer support. If we do not receive notice at least five (5) days before any such change, we may attempt, in our sole discretion, to implement such change prior to any ACH debit or credit transfer performed pursuant to your authorization provided in this Section E. However, we assume no responsibility for our failure to do so.

You are solely responsible for promptly reconciling your Transaction history with the transaction records for your bank account. You must notify us of any errors or discrepancies in your account transaction history (each, an "Error") within 30 days of when the Error could be viewed in your Account transaction history on the Site. If you do not notify us of an Error within 30 days of when the Error could be viewed in your Account transaction history on the Site, you will forfeit the right to contest the Error, except to the extent such forfeiture is prohibited by applicable law or the NACHA rules.

Subject to the foregoing notice requirement: (a) if and to the extent an Error is caused by us, we will correct the Error and (b) if an Error is caused by you, we may, but are under no obligation to, attempt to correct the Error and will offset any costs we incur from any funds returned to your bank account or your Escrow Account, as applicable. If an Error results in your receipt of more funds than you are entitled, we may recover the extra funds from you.

Refund Policy

Charges paid by Consumer for completed orders, or for orders confirmed by a Customer, are final and non-refundable. oneapp has no obligation to provide refunds or credits but may grant them gratuitously at oneapp's sole discretion in each case. In order to make a claim for a refund, please email oneapp at support@withoneapp.com. If oneapp grants your request for a refund, you will receive an email from oneapp confirming your refund request has been approved, and please follow the procedures set out below:

1. Issue Reported;
2. Refund Processed; and
3. Charge Dropped or Refund Received.

The timing of your refund depends on when it was issued as well as your bank's processing time. If a charge is still shown as "Pending" on your statement, it may take one to three business days to be removed.

"Pending" means the funds are authorized but not yet withdrawn. For partial refunds, the pending charge will be replaced with a new charge for the adjusted amount.

If the charge is no longer “Pending," this means it has been posted to your account. It can then take five to seven business days to be refunded.

Once your refund is issued, you will receive an email confirmation that details the refund issue date and refunded amount.

If it has been more than seven business days from the date listed in the refund email, please contact support@withoneapp.com for assistance.

Security Overview

This oneapp Security Overview (“*Security Overview*”) is incorporated into and made a part of the agreement between oneapp and Merchant covering Merchant’s use of the SaaS (as defined below) (“*Agreement*”).

1. Definitions

“*SaaS*” means any services or application programming interfaces branded as “oneapp”.

Any capitalized term not defined in this Section 1 will have the meaning provided in the Agreement, this Security Overview, or the Data Protection Addendum. The then-current terms of the Data Protection Addendum are available at https://legal.withoneapp.com.

2. Purpose. oneapp maintains data security policies and procedures in accordance with Applicable Data Protection Law, which includes the New York "Stop Hacks and Improve Electronic Data Security Act (“SHIELD Act”). This Security Overview describes oneapp’s security program, security certifications, and technical and organizational security controls to protect (a) Merchant Data from unauthorized use, access, disclosure, or theft and (b) the SaaS. As security threats change, oneapp continues to update its security program and strategy to help protect Merchant Data and the SaaS. As such, oneapp reserves the right to update this Security Overview from time to time; provided, however, any update will not materially reduce the overall protections set forth in this Security Overview. The then-current terms of this Security Overview are available at https://legal.withoneapp.com This Security Overview does not apply to any (a) SaaS that are identified as alpha, beta, not generally available, limited release, developer preview, or any similar SaaS offered by oneapp or (b) services provided by third party vendors.

3. Security Organization and Program. oneapp maintains a risk-based assessment security program. The framework for oneapp’s security program includes administrative, organizational, technical, and physical safeguards reasonably designed to protect the

SaaS and confidentiality, integrity, and availability of Merchant Data. oneapp's security program is intended to be appropriate to the nature of the SaaS and the size and complexity of oneapp's business operations. oneapp has separate and dedicated Information Security teams that manage oneapp's security program. There is a team that facilitates and supports independent audits and assessments performed by third parties. oneapp's security framework is based on the ISO 27001 Information Security Management System and includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Disaster Recovery Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, and Security Monitoring and Incident Response. Security is managed at the highest levels of the company, with oneapp's Chief Information Officer ("CIO") meeting with executive management regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are reviewed and approved by management at least annually and are made available to all oneapp employees for their reference.

4. Confidentiality. oneapp has controls in place to maintain the confidentiality of Merchant Data in accordance with the Agreement. All oneapp employees and contract personnel are bound by oneapp's internal policies regarding maintaining the confidentiality of Merchant Data and are contractually obligated to comply with these obligations.

5. People Security

5.1 Employee Background Checks. oneapp performs background checks on all new employees at the time of hire in accordance with applicable local laws. oneapp currently verifies a new employee's education and previous employment and performs reference checks. Where permitted by applicable law, oneapp may also conduct criminal, credit, immigration, and security checks depending on the nature and scope of a new employee's role.

5.2 Employee Training. At least once (1) per year, oneapp employees must complete a security and privacy training which covers oneapp's security policies, security best practices, and privacy principles. Employees on a leave of absence may have additional time to complete this annual training. oneapp's dedicated security team also performs phishing awareness campaigns and communicates emerging threats to employees. oneapp has also established an anonymous hotline for employees to report any unethical behavior where anonymous reporting is legally permitted.

6. Third Party Vendor Management

6.1 Vendor Assessment. oneapp may use third party vendors to provide the SaaS. oneapp carries out a security risk-based assessment of prospective vendors before working with them to validate they meet oneapp's security requirements. oneapp periodically reviews each vendor in light of oneapp's security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal or regulatory requirements. oneapp ensures that Merchant Data is returned and/or deleted at the end of a vendor relationship. For the avoidance of doubt, telecommunication providers are not considered subcontractors or third-party vendors of oneapp.

6.2 Vendor Agreements. oneapp enters into written agreements with all of its vendors which include confidentiality, privacy, and security obligations that provide an appropriate level of protection for Merchant Data that these vendors may process.

7. Security Certifications and Attestations. oneapp holds the following security-related certifications and attestations from third party vendors: ISO/IEC 17001, ISO/IEC/ 170017 & 27018, SOC 2 Type 2, PCI DSS Level 1, and PCI DSS Level 4.

8. Hosting Architecture and Data Segregation

8.1 Amazon Web Services.The SaaS are hosted on Amazon Web Services ("*AWS*") in the United States of America and protected by the security and environmental controls of Amazon. The production environment within AWS where the SaaS and Merchant Data are hosted are logically isolated in a Virtual Private Cloud (VPC). Merchant Data stored within AWS is encrypted at all times. AWS does not have access to unencrypted Merchant Data. More information about AWS security is available at https://aws.amazon.com/security/ and https://aws.amazon.com/compliance/shared-responsibility-model/. For AWS SOC Reports, please see https://aws.amazon.com/compliance/soc-faqs/.

8.2 Google Cloud Platform. oneapp uses Google Workspace for internal and external office productivity and communications, hosted on Google Cloud Platform ("*GCP*") in the United States of America. More information about GCP security is available at https://cloud.google.com/architecture#security.

8.3 SaaS. For the SaaS, all network access between production hosts is restricted, using access control lists to allow only authorized services to interact in the production network. Access control lists are in use to manage network segregation between different security zones in the production and corporate environments. Access control lists are reviewed regularly. oneapp separates Merchant Data using logical identifiers. Merchant Data is tagged with a unique customer identifier that is assigned to segregate Merchant Data ownership. The oneapp APIs are designed and built to identify and allow

authorized access only to and from Merchant Data identified with customer specific tags. These controls prevent other customers from having access to Merchant Data.

9. Physical Security. AWS data centers are strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication (2FA) a minimum of two (2) times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions. Each data center has redundant electrical power systems that are available twenty-four (24) hours a day, seven (7) days a week. Uninterruptible power supplies and on-site generators are available to provide back-up power in the event of an electrical failure. In addition, oneapp headquarters and office spaces have a physical security program that manages visitors, building entrances, closed circuit televisions, and overall office security. All employees, contractors, and visitors are required to wear identification badges.

10. Security by Design. oneapp follows security by design principles when it designs the SaaS. oneapp also applies the oneapp Secure Software Development Lifecycle (Secure SDLC) standard to perform numerous security-related activities for the SaaS across different phases of the product creation lifecycle from requirements gathering and product design all the way through product deployment. These activities include, but are not limited to, the performance of (a) internal security reviews before deploying new SaaS or code; (b) penetration tests of new SaaS by independent third parties; and (c) threat models for new SaaS to detect potential security threats and vulnerabilities.

11. Access Controls

11.1 Provisioning Access. To minimize the risk of data exposure, oneapp follows the principles of least privilege through a team-based-access-control model when provisioning system access. oneapp personnel are authorized to access Merchant Data based on their job function, role, and responsibilities, and such access requires Merchant approval. Access rights to production environments that are not time-based are reviewed at least semi-annually. An employee’s access to Merchant Data is promptly removed upon termination of their employment. In order to access the production environment, an authorized user must have a unique username and password and multi-factor authentication enabled. Before an engineer is granted access to the production environment, access must be approved by management and the engineer is required to complete internal training for such access including training on the relevant team’s systems. oneapp logs high risk actions and changes in the production environment. oneapp leverages automation to identify any deviation from

internal technical standards that could indicate anomalous/unauthorized activity to raise an alert within minutes of a configuration change.

11.2 Password Controls. oneapp's current policy for employee password management follows the NIST 800-63B guidance, and as such, our policy is to use longer passwords, with multi-factor authentication, but not require special characters or frequent changes. When a customer logs into its account, oneapp hashes the credentials of the user before it is stored.

12. Change Management. oneapp has a formal change management process it follows to administer changes to the production environment for the SaaS, including any changes to its underlying software, applications, and systems. Each change is carefully reviewed and evaluated in a test environment before being deployed into the production environment for the SaaS. All changes, including the evaluation of the changes in a test environment, are documented using a formal, auditable system of record. A rigorous assessment is carried out for all high-risk changes to evaluate their impact on the overall security of the SaaS. Deployment approval for high-risk changes is required from the correct organizational stakeholders. Plans and procedures are also implemented in the event a deployed change needs to be rolled back to preserve the security of the SaaS.

13. Encryption. For the SaaS, (a) the databases that store Merchant Data are encrypted using the Advanced Encryption Standard and (b) Merchant Data is encrypted when in transit between Merchant's software application and the SaaS using TLS v1.2.

14. Vulnerability Management. oneapp maintains controls and policies to mitigate the risk of security vulnerabilities in a measurable time frame that balances risk and the business/operational requirements. oneapp uses a third-party tool to conduct vulnerability scans regularly to assess vulnerabilities in oneapp's cloud infrastructure and corporate systems. Critical software patches are evaluated, tested, and applied proactively. Operating system patches are applied through the regeneration of a base virtual-machine image and deployed to all nodes in the oneapp cluster over a predefined schedule. For high-risk patches, oneapp will deploy directly to existing nodes through internally developed orchestration tools.

15. Penetration Testing. oneapp performs penetration tests and engages independent third-party entities to conduct application-level penetration tests. Security threats and vulnerabilities that are detected are prioritized, triaged, and remediated promptly. oneapp maintains a Bug Bounty Program through Bug Crowd, which allows independent security researchers to report security threats and vulnerabilities on an ongoing basis.

16. Security Incident Management. oneapp maintains security incident management policies and procedures in accordance with NIST SP 800-61. oneapp's Security Incident Response Team ("T-SIRT") assesses all relevant security threats and vulnerabilities and establishes appropriate remediation and mitigation actions. oneapp retains security logs for one hundred and eighty (180) days. Access to these security logs is limited to T-SIRT. oneapp utilizes third-party tools to detect, mitigate, and prevent Distributed Denial of Service (DDoS) attacks.

17. Discovery, Investigation, and Notification of a Security Incident. oneapp will promptly investigate a Security Incident upon discovery. To the extent permitted by applicable law, oneapp will notify Merchant of a Security Incident in accordance with the Data Protection Addendum. Security Incident notifications will be provided to Merchant via email to the email address designated by Merchant in its account.

18. Resilience and Service Continuity

18.1 Resilience. The hosting infrastructure for the SaaS (a) spans multiple fault-independent availability zones in geographic regions physically separated from one another and (b) is able to detect and route around issues experienced by hosts or even whole data centers in real time and employ orchestration tooling that has the ability to regenerate hosts, building them from the latest backup.

18.2 Service Continuity. oneapp also leverages specialized tools available within the hosting infrastructure for the SaaS to monitor server performance, data, and traffic load capacity within each availability zone and colocation data center. If suboptimal server performance or overloaded capacity is detected on a server within an availability zone or colocation data center, these specialized tools increase the capacity or shift traffic to relieve any suboptimal server performance or capacity overload. oneapp is also immediately notified in the event of any suboptimal server performance or overloaded capacity.

19. Merchant Data Backups. oneapp performs regular backups of Merchant Data, which is hosted on AWS's data center infrastructure. Merchant Data that is backed up is retained redundantly across multiple availability zones and encrypted in transit and at rest using the Advanced Encryption Standard.

Data Protection Addendum

This Data Protection Addendum ("*Addendum*") forms part of the agreement between Merchant and oneapp covering Merchant's use of the SaaS (as defined below) ("*Agreement*").

I. Introduction

1. Definitions

- "*Applicable Data Protection Law*" means all laws and regulations applicable to oneapp's processing of personal data under the Agreement.
- "*controller*" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "*Merchant Account Data*" means personal data that relates to Merchant's relationship with oneapp, including the names or contact information of individuals authorized by Merchant to access Merchant's account, and billing information of individuals that Merchant has associated with its account. Merchant Account Data also includes any personal data oneapp may need to collect for the purpose of identity verification (including providing the Multi-Factor Authentication SaaS, as defined below), or as part of its legal obligation to retain Subscriber Records (as defined below).
- "*Merchant Content*" means (a) personal data exchanged as a result of using the SaaS (as defined below), such as text message bodies, voice and video media, images, email bodies, email recipients, sound, and, where applicable, details Merchant submits to the SaaS from its designated software applications and services and (b) data stored on Merchant's behalf such as communication logs within the SaaS or marketing campaign data that Merchant has uploaded to the SaaS (as defined below).
- "*Merchant Data*" has the meaning given in the Agreement. Merchant Data includes Merchant Account Data, Merchant Usage Data, Merchant Content, and Sensitive Data, each as defined in this Addendum.
- "*Merchant Usage Data*" means data processed by oneapp for the purposes of transmitting or exchanging Merchant Content utilizing phone numbers either through the public switched telephone network or by way of other communication networks. Merchant Usage Data includes data used to identify the source and destination of a communication, such as (a) individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the SaaS, and the date, time, duration and the type of communication and (b) activity logs used to identify the source of Service requests, optimize and maintain performance of the SaaS, and investigate and prevent system abuse.

- "*Multi-Factor Authentication SaaS*" means the provision of a portion of the SaaS under which Merchant adds an additional factor for verification of Merchant's end users' identity in connection with such end users' use of Merchant's software applications or services.

- "*personal data*" means any information relating to an identified or identifiable natural person ("*data subject*"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- "*processor*" means the entity which processes personal data on behalf of the controller.

- "*processing*" (and "*process*") means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

- "*Security Incident*" means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Merchant Data.

- "*Sensitive Data*" means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), financial information, banking account numbers or passwords; (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords, mother's maiden name, or date of birth; (f) criminal history; or (g) any other information or combinations of information that falls within the definition of "special categories of data" under GDPR (as defined below) or any other applicable law or regulation relating to privacy and data protection.

- "*SaaS*" means the products and services provided by oneapp or its affiliates, as applicable, that are (a) used by Merchant, including, without limitation, products and services that are on a trial basis or otherwise free of charge or (b) ordered by Merchant under an order form.

- "*Subscriber Records*" means Merchant Account Data containing proof of identification and proof of physical address necessary for oneapp to provide Merchant or Merchant's end users with services in certain areas. When required by law or regulation, Subscriber Records are shared with local service providers, or local government authorities.

- "*sub-processor"* means (a) oneapp, when oneapp is processing Merchant Content and where Merchant is a processor of such Merchant Content or (b) any third-party processor engaged by oneapp to process Merchant Content in order to provide the SaaS to Merchant. For the avoidance of doubt, telecommunication providers are not sub-processors.

- "*Third Party Request*" means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.

- "*oneapp Privacy Notice"* means the privacy notice for the SaaS, the current version of which is available at https://legal.withoneapp.com.

Any capitalized term not defined in this Section 1 will have the meaning provided in this Addendum or the Agreement.

II. Controller and Processor

2. Relationship

2.1 oneapp as a Processor. Merchant and oneapp agree that with regard to the processing of Merchant Content, Merchant may act either as a controller or processor and oneapp is a processor. oneapp will process Merchant Content in accordance with Merchant's instructions as set forth in Section 5 (Merchant Instructions).

2.2 oneapp as a Controller of Merchant Account Data. Merchant and oneapp acknowledge that, with regard to the processing of Merchant Account Data, Merchant is a controller and oneapp is an independent controller, not a joint controller with Merchant. oneapp will process Merchant Account Data as a controller in order to (a) manage the relationship with Merchant; (b) carry out oneapp's core business operations, such as accounting and filing taxes; (c) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the SaaS; (d) perform identity verification; (e) comply with oneapp's legal or regulatory obligation to retain Merchant Records; and (f) as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the oneapp Privacy Notice.

2.3 oneapp as a Controller of Merchant Usage Data. The parties acknowledge that, with regard to the processing of Merchant Usage Data, Merchant may act either as a controller or processor and oneapp is an independent controller, not a joint controller

with Merchant. oneapp will process Merchant Usage Data as a controller in order to carry out the necessary functions as a SaaS provider, such as: (a) oneapp's accounting, tax, billing, audit, and compliance purposes; (b) to provide, optimize, and maintain the SaaS, platform and security; (c) to investigate fraud, spam, wrongful or unlawful use of the SaaS; (d) as required by applicable law or regulation; or (e) as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the oneapp Privacy Notice.

3. Purpose Limitation. oneapp will process personal data in order to provide the SaaS in accordance with the Agreement. Schedule 1 (Details of Processing) of this Addendum further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of personal data and categories of data subjects.

4. Compliance. Merchant is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Law in its use of the SaaS and its own processing of personal data and (b) it has, and will continue to have, the right to transfer, or provide access to, personal data to oneapp for processing in accordance with the terms of the Agreement and this Addendum.

III. oneapp as a Processor – Processing Merchant Content

5. Merchant Instructions. Merchant appoints oneapp as a processor to process Merchant Content on behalf of, and in accordance with, Merchant's instructions (a) as set forth in the Agreement, this Addendum, and as otherwise necessary to provide the SaaS to Merchant, and which includes investigating security incidents and preventing spam, fraudulent activity, and violations of the oneapp Acceptable Use Policy, the current version of which is available at https://legal.withoneapp.com, and detecting and preventing network exploits or abuse; (b) as necessary to comply with applicable law or regulation, including Applicable Data Protection Law; and (c) as otherwise agreed in writing between Merchant and oneapp ("*Permitted Purposes*").

5.1 Lawfulness of Instructions. Merchant will ensure that its instructions comply with Applicable Data Protection Law. Merchant acknowledges that oneapp is neither responsible for determining which laws or regulations are applicable to Merchant's business nor whether oneapp's provision of the SaaS meets or will meet the requirements of such laws or regulations. Merchant will ensure that oneapp's processing of Merchant Content, when done in accordance with Merchant's instructions, will not cause oneapp to violate any applicable law or regulation, including Applicable Data Protection Law. oneapp will inform Merchant if it becomes aware, or reasonably believes, that Merchant's instructions violate any applicable law or regulation, including Applicable Data Protection Law.

5.2 Additional Instructions. Additional instructions outside the scope of the Agreement or this Addendum will be agreed to in writing between Merchant and oneapp, including any additional fees that may be payable by Merchant to oneapp for carrying out such additional instructions.

6. Confidentiality

6.1 Responding to Third Party Requests. In the event any Third Party Request is made directly to oneapp in connection with oneapp's processing of Merchant Content, oneapp will promptly inform Merchant and provide details of the same, to the extent legally permitted. oneapp will not respond to any Third Party Request without Merchant's prior consent, except as legally required to do so or to confirm that such Third Party Request relates to Merchant.

6.2 Confidentiality Obligations of oneapp Personnel. oneapp will ensure that any person it authorizes to process Merchant Content has agreed to protect personal data in accordance with oneapp's confidentiality obligations in the Agreement.

7. Sub-processors

7.1 Authorization for Onward Sub-processing. Merchant provides a general authorization for oneapp to engage onward sub-processors that is conditioned on the following requirements:

(a) oneapp will restrict the onward sub-processor's access to Merchant Content only to what is strictly necessary to provide the SaaS, and oneapp will prohibit the sub-processor from processing the personal data for any other purpose;

(b) oneapp agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Merchant Content to the standard required by Applicable Data Protection Law, including the requirements set forth in Schedule 2 (Jurisdiction Specific Terms) of this Addendum; and

(c) oneapp will remain liable for any breach of this Addendum that is caused by an act, error, or omission of its sub-processors.

7.2 Current Sub-processors and Notification of Sub-processor Changes. Merchant consents to oneapp engaging third party sub-processors to process Merchant Content within the SaaS for the Permitted Purposes provided that oneapp maintains an up-to-date list of its sub-processors at https://legal.withoneapp.com. If Merchant subscribes to such notifications, oneapp will provide details of any change in sub-processors as soon as reasonably practicable. With respect to changes in infrastructure providers, oneapp will endeavor to give written notice sixty (60) days prior

to any change, but in any event will give written notice no less than thirty (30) days prior to any such change. With respect to oneapp's other sub-processors, oneapp will endeavor to give written notice thirty (30) days prior to any change, but will give written notice no less than ten (10) days prior to any such change.

7.3 Objection Right for new Sub-processors. Merchant may object to oneapp's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection. In such an event, Merchant and oneapp agree to discuss commercially reasonable alternative solutions in good faith. If Merchant and oneapp cannot reach a resolution within ninety (90) days from the date of oneapp's receipt of Merchant's written objection, Merchant may discontinue the use of the affected SaaS by providing written notice to oneapp. Such discontinuation will be without prejudice to any fees incurred by Merchant prior to the discontinuation of the affected SaaS. If no objection has been raised prior to oneapp replacing or appointing a new sub-processor, oneapp will deem Merchant to have authorized the new sub-processor.

8. Data Subject Rights. oneapp provides Merchant with a number of self-service features via the SaaS, including the ability to delete, obtain a copy of, or restrict use of Merchant Content. Merchant may use such self-service features to assist in complying with its obligations under Applicable Data Protection Law with respect to responding to Third Party Requests from data subjects via the SaaS at no additional cost. Upon Merchant's request, oneapp will provide reasonable additional and timely assistance to Merchant in complying with Merchant's data protection obligations with respect to data subject rights under Applicable Data Protection Law to the extent Merchant does not have the ability to resolve a Third Party Request from a data subject through self-service features made available via the SaaS.

9. Impact Assessments and Consultations. oneapp will provide reasonable cooperation to Merchant in connection with any data protection impact assessment (at Merchant's expense only if such reasonable cooperation will require oneapp to assign significant resources to that effort) or consultations with regulatory authorities that may be required in accordance with Applicable Data Protection Law.

10. Return or Deletion of Merchant Content. oneapp will, in accordance with Section 3 (Duration of the Processing) of Schedule 1 (Details of Processing) of this Addendum, delete or return to Merchant any Merchant Content stored within the SaaS.

10.1 Extension of Addendum. Upon termination of the Agreement, oneapp may retain Merchant Content in storage for the time periods set forth in Schedule 1 (Details of Processing) of this Addendum, provided that oneapp will ensure that Merchant Content (a) is processed only as necessary for the Permitted Purposes and (b) remains

protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

10.2 Retention Required by Law. Notwithstanding anything to the contrary in this Section 10, oneapp may retain Merchant Content, or any portion of it, if required by applicable law or regulation, including Applicable Data Protection Law, provided such Merchant Content remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

IV. Security and Audits

11. Security

11.1 Security Measures. oneapp has implemented and will maintain the technical and organizational security measures as set forth in the Agreement.

11.2 Determination of Security Requirements. Merchant acknowledges the SaaS include certain features and functionalities that Merchant may elect to use which impact the security of Merchant Data processed by Merchant's use of the SaaS, such as, but not limited to, encryption of voice recordings, availability of multi-factor authentication on Merchant's account, or optional Transport Layer Security (TLS) encryption. Merchant is responsible for reviewing the information oneapp makes available regarding its data security, including its audit reports, and making an independent determination as to whether the SaaS meet the Merchant's requirements and legal obligations, including its obligations under Applicable Data Protection Law. Merchant is further responsible for properly configuring the SaaS and using features and functionalities made available by oneapp to maintain appropriate security in light of the nature of Merchant Data processed as a result of Merchant's use of the SaaS.

11.3 Security Incident Notification. oneapp will provide notification of a Security Incident in the following manner:

(a) oneapp will, to the extent permitted by applicable law or regulation, notify Merchant without undue delay, but in no event later than seventy-two (72) hours after oneapp's discovery of a Security Incident impacting Merchant Data of which oneapp is a processor;

(b) oneapp will, to the extent permitted and required by applicable law or regulation, notify Merchant without undue delay of any Security Incident involving Merchant Data of which oneapp is a controller; and

(c) oneapp will notify Merchant of any Security Incident via email to the email address(es) designated by Merchant in Merchant's account.

oneapp will make reasonable efforts to identify a Security Incident, and to the extent a Security Incident is caused by oneapp's violation of this Addendum, remediate the cause of such Security Incident. oneapp will provide reasonable assistance to Merchant in the event that Merchant is required under Applicable Data Protection Law to notify a regulatory authority or any data subjects impacted by a Security Incident.

12. Audits. Merchant and oneapp acknowledge that Merchant must be able to assess oneapp's compliance with its obligations under Applicable Data Protection Law and this Addendum, insofar as oneapp is acting as a processor on behalf of Merchant.

12.1 oneapp's Audit Program. oneapp uses external auditors to verify the adequacy of its security measures with respect to its processing of Merchant Content. Such audits are performed at least once annually at oneapp's expense by independent third-party security professionals at oneapp's selection and result in the generation of a confidential audit report ("*Audit Report*").

12.2 Merchant Audit. Upon Merchant's written request at reasonable intervals, and subject to reasonable confidentiality controls, oneapp will make available to Merchant a copy of oneapp's most recent Audit Report. Merchant agrees that any audit rights granted by Applicable Data Protection Law will be satisfied by these Audit Reports. To the extent that oneapp's provision of an Audit Report does not provide sufficient information or Merchant is required to respond to a regulatory authority audit, Merchant agrees to a mutually agreed-upon audit plan with oneapp that: (a) ensures the use of an independent third party; (b) provides written notice to oneapp in a timely fashion; (c) requests access only during business hours; (d) accepts billing to Merchant at oneapp's then-current rates; (e) occurs no more than once annually; (f) restricts its findings to only data relevant to Merchant; and (g) obligates Merchant, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

13. Jurisdiction Specific Terms. To the extent oneapp processes personal data originating from and protected by Applicable Data Protection Law in one of the jurisdictions listed in Schedule 2 (Jurisdiction Specific Terms) of this Addendum, the terms specified in Schedule 2 with respect to the applicable jurisdiction(s) apply in addition to the terms of this Addendum.

V. Miscellaneous

15. Cooperation and Data Subject Rights. In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable) or (b) any Third Party Request relating to the processing of Merchant Account Data or Merchant Usage Data conducted by the other party, such

party will promptly inform such other party in writing. Merchant and oneapp agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Law.

16. Conflict. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms set forth in Schedule 2 (Jurisdiction Specific Terms) of this Addendum; (2) the terms of this Addendum outside of Schedule 2 (Jurisdiction Specific Terms); (3) the Agreement; and (4) the oneapp Privacy Notice. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including, without limitation, the exclusions and limitations set forth in the Agreement.

17. Updates. oneapp may update the terms of this Addendum from time to time; provided, however, oneapp will provide at least thirty (30) days prior written notice to Merchant when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing SaaS. The then-current terms of this Addendum are available at https://legal.withoneapp.com.

Schedule 1

Details of Processing

1. Nature and Purpose of the Processing. oneapp will process personal data as necessary to provide the SaaS under the Agreement. oneapp does not sell Merchant's personal data or Merchant end users' personal data and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

1.1 Merchant Content. oneapp will process Merchant Content as a processor in accordance with Merchant's instructions as set forth in Section 5 (Merchant Instructions) of this Addendum.

1.2 Merchant Account Data. oneapp will process Merchant Account Data as a controller for the purposes set forth in Section 2.2 (oneapp as a Controller of Merchant Account Data) of this Addendum.

1.3 Merchant Usage Data. oneapp will process Merchant Usage Data as a controller for the purposes set forth in Section 2.3 (oneapp as a Controller of Merchant Usage Data) of this Addendum.

2. Processing Activities

2.1 Merchant Content. Personal data contained in Merchant Content will be subject to the following basic processing activities:

(a) the provision of programmable communication products and services, primarily offered in the form of application programming interfaces, to Merchant, including transmittal to or from Merchant's software applications or; services and designated third parties as directed by Merchant, from or to the publicly-switched telephone network or by way of other communications networks. Storage of personal data on oneapp's network;

(b) the provision of products and services which allow the transmission and delivery of email communications on behalf of Merchant to its recipients. oneapp will also provide Merchant with analytic reports regarding the email communications it sends on Merchant's behalf. Storage of personal data on oneapp's network; and

(c) the provision of products and services which allows Merchant to integrate, manage and control its data relating to end users. Storage of personal data on oneapp's network.

2.2 Merchant Account Data. Personal data contained in Merchant Account Data will be subject to the processing activities of providing the SaaS.

2.3 Merchant Usage Data. Personal data contained in Merchant Usage Data will be subject to the processing activities of providing the SaaS.

3. Duration of the Processing. The period for which personal data will be retained and the criteria used to determine that period is as follows:

3.1 Merchant Content.

SaaS. Prior to the termination of the Agreement, (x) oneapp will process stored Merchant Content for the Permitted Purposes until Merchant elects to delete such Merchant Content via the SaaS and (y) Merchant agrees that it is solely responsible for deleting Merchant Content via the SaaS. Upon termination of the Agreement, oneapp will (i) provide Merchant thirty (30) days after the termination effective date to obtain a copy of any stored Merchant Content via the SaaS; (ii) automatically delete any stored Merchant Content thirty (30) days after the termination effective date; and (iii) automatically delete any stored Merchant Content on oneapp's back-up systems sixty (60) days after the termination effective date. Any Merchant Content archived on oneapp's back-up systems will be securely isolated and protected from any further processing, except as otherwise required by applicable law or regulation.

3.2 Merchant Account Data. oneapp will process Merchant Account Data as long as required (a) to provide the SaaS to Merchant; (b) for oneapp's legitimate business

needs; or (c) by applicable law or regulation. Merchant Account Data will be stored in accordance with the oneapp Privacy Notice.

3.3 Merchant Usage Data. Upon termination of the Agreement, oneapp may retain, use, and disclose Merchant Usage Data for the purposes set forth in Section 1.3 (Merchant Usage Data) of this Schedule 1, subject to the confidentiality obligations set forth in the Agreement. oneapp will anonymize or delete Merchant Usage Data when oneapp no longer requires it for the purposes set forth in Section 1.3 (Merchant Usage Data) of this Schedule 1.

4. Categories of Data Subjects

4.1 Merchant Content. Merchant's end users.

4.2 Merchant Account Data. Merchant's employees and individuals authorized by Merchant to access Merchant's oneapp account or make use of the Multi-Factor Authentication SaaS received from oneapp.

4.3 Merchant Usage Data. Merchant's end users.

5. Categories of Personal Data. oneapp processes personal data contained in Merchant Account Data, Merchant Content, and Merchant Usage Data.

6. Sensitive Data or Special Categories of Data

6.1 Merchant Content. Sensitive Data may, from time to time, be processed via the SaaS where Merchant or its end users choose to include Sensitive Data within the communications that are transmitted using the SaaS. Merchant is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Merchant's end users to transmit or process, any Sensitive Data via the SaaS.

6.2 Merchant Account Data and Merchant Usage Data.

(a) Sensitive Data may be found in Merchant Account Data in the form of Subscriber Records containing passport or similar identifier data necessarily processed in order to receive services.

(b) Merchant Usage Data does not contain Sensitive Data.

Schedule 2

Jurisdiction Specific Terms

1. United States of America:

1.1 “*US State Privacy Laws*” means all state laws relating to the protection and processing of personal data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“*CCPA*”), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

1.2 The definition of “Applicable Data Protection Law” includes US State Privacy Laws.

1.3 The following terms apply where oneapp processes personal data subject to the CCPA:

(a) The term “*personal information*”, as used in this Section 11.3, will have the meaning provided in the CCPA;

(b) oneapp is a service provider when processing Merchant Content. oneapp will process any personal information contained in Merchant Content only for the business purposes set forth in the Agreement, including the purpose of processing and processing activities set forth in this Addendum (“*Purpose*”). As a service provider, oneapp will not sell or share Merchant Content or retain, use, or disclose Merchant Content (i) for any purpose other than the Purpose, including retaining, using, or disclosing Merchant Content for a commercial purpose other than the Purpose, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Merchant and oneapp;

(c) oneapp will (i) comply with obligations applicable to it as a service provider under the CCPA and (ii) provide personal information with the same level of privacy protection as is required by the CCPA. Merchant is responsible for ensuring that it has complied, and will continue to comply, with the requirements of the CCPA in its use of the SaaS and its own processing of personal information;

(d) Merchant will have the right to take reasonable and appropriate steps to help ensure that oneapp uses personal information in a manner consistent with Merchant’s obligations under the CCPA;

(e) oneapp will notify Merchant if it makes a determination that it can no longer meet its obligations as a service provider under the CCPA;

(f) Upon notice, Merchant will have the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of personal information;

(g) oneapp will provide reasonable additional and timely assistance to assist Merchant in complying with its obligations with respect to consumer requests as set forth in the Agreement;

(h) For any sub-processor used by oneapp to process personal information subject to the CCPA, oneapp will ensure that oneapp's agreement with such sub-processor complies with the CCPA, including, without limitation, the contractual requirements for service providers and contractors;

(i) oneapp will not combine Merchant Content that it receives from, or on behalf of, Merchant, with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, unless such combination is required to perform any business purpose as permitted by the CCPA, including any regulations thereto, or by regulations adopted by the California Privacy Protection Agency; and

(j) oneapp certifies that it understands and will comply with its obligations under the CCPA.

1.4 oneapp acknowledges and confirms that it does not receive Merchant Content as consideration for any SaaS provided to Merchant.

Privacy Notice

Privacy is oneapp's code: oneapp has built our global privacy program, which serve as our code of conduct that governs our global processing of personal data. No matter where you are in the world, where you reside, where your citizenship lies, or where your data comes from, we offer the same high standards of privacy protection to all end users. We hope our Privacy Notice will provide clear, detailed, and easy-to-read information about oneapp's privacy practices and how we process personal data.

In addition, we provide in-time and in-context information about how you can control the data you collect and retain in our API documentation. Because we offer many different products — and end users can configure them in many different ways — we provide privacy-specific information in our documentation to enable end users to make choices when using our products. Please check the documentation for the product you're using to learn more about the data elements it collects and how you can make decisions about that information.

When we refer to oneapp, we mean the oneapp entity with which you have contracted. If there are any capitalized terms in this Privacy Notice that are not defined, then those terms will have the meaning defined in your agreement with us.

Contents of this Notice

Summary: How oneapp processes your personal data

oneapp collects personal data such as Merchant Account Data directly from you — as a end user or a visitor — when you visit oneapp's website, request a product, service or access to an event, or when you contact a member of the oneapp team or sign up for a oneapp account to use our software as a service. oneapp also indirectly collects the personal data of yend users called Merchant Usage Data (e.g., communications metadata) and Merchant Content (e.g., communications content).

Summary: Data about end users

We process end user contact details such as your name, email, and phone number directly from you when you make a request, contact a member of our team, or sign-up for a oneapp account. Read this section to learn more about the types of data we collect about you, why we collect it, and how we store it.

Summary: Data about end users' end users

We process yend users' communications-related data such as phone numbers, email addresses, friendly names that you create for yend users. We also process the content of communications sent by you or your end users to provide services to you and to carry out necessary functions of our business as a communications service provider. Please read this section to learn more about the types of data we collect about your end users, why we collect it, and how we store it.

Summary: How oneapp shares personal data

First things first: we do not sell your personal data, or the personal data of your end users. We also do not allow any personal data to be used by third parties for their own marketing purposes (except in cases where you explicitly request or provide consent for us to do so, such as at a conference when you direct us to share your information with a sponsor).

However, we do need to share it in some circumstances. These may be to provide you services (e.g., to route a call or send an email), or when necessary for our suppliers to provide services to us, or for another reason listed here.

Summary: How to make choices about your data

oneapp provides you with many ways to make choices about your data and your end users' data, such as accessing it, correcting it, deleting it, or updating your choices about how it is used.

Summary: Cookies and tracking technology

oneapp uses common information-gathering tools such as cookies, web beacons, pixels and other similar tracking technologies to automatically collect information as you navigate our websites, our services or when you interact with emails we sent to you. You can manage these technologies easily on our websites.

Summary: Global privacy compliance at oneapp

oneapp is a global company that is committed to complying with privacy laws around the world. Read this section to learn more about our global privacy compliance and how we protect the personal data of specific groups, such as employees and applicants.

Summary: International data transfers

oneapp relies on our Data Protection Addendum as our primary data transfer mechanism.

Summary: Security information

While there is no such thing as perfect security, we are committed to maintaining reasonable and appropriate security measures to ensure that your personal data is protected both online and offline. Read this section to learn more about our security measures and how you can better protect your account.

Summary: Handling privacy disputes

In the unlikely event that we are unable to resolve a privacy concern quickly and thoroughly, we provide a path of dispute resolution.

Summary: Other information you may find useful

Here you'll find other useful information about our data protection practices and about this notice. Our use of automated decision making is minimal; we use it primarily for anti-fraud purposes. Finally, we may update our Privacy Notice from time to time, and we will notify end users in advance of material changes.

How oneapp Processes Your Personal Data

When we talk about "personal data," we're talking about a broad range of information. Data protection laws around the world define this concept in different ways, but in general, we mean any information that relates to an identifiable, living individual person. In other words, a person's phone number is personal data, while a business's phone number is not.

In addition, some data protection laws and privacy laws in certain jurisdictions differentiate between “controllers” and “processors” of personal data. A controller decides why and how to process personal data. A processor does not make decisions about personal data; it only processes personal data on behalf of a controller based on the controller’s instructions.

With this background, let’s take a high level look at the personal data oneapp collects and how we process it.

If you are a end user of ours, oneapp processes personal data in different ways when you use our software as a service.

- We process your personal data as a end user (or potential end user) of oneapp’s services — information that we refer to as Merchant Account Data (e.g., your contact information) — when you visit a oneapp public-facing website like withoneapp.com; sign up for a oneapp event; reach out to our Sales team; or sign up for a oneapp account and use our software as a service.

- We process the personal data of your end users who use or interact with your application that you’ve built on oneapp’s platform, like the people you communicate with by way of that application. This includes information we use to route messages and metadata about messages — we refer to this information as Merchant Usage Data — and it also includes the contents of communications, which we refer to as your Merchant Content. You can see a more detailed definition of “Merchant Content” in our Data Protection Addendum, which is part of our agreement with you.

oneapp processes these categories of personal data differently because the direct relationship we have with you, end user, is different from the indirect relationship we have with your end users.

When oneapp processes your Merchant Account Data and your Merchant Usage Data, oneapp is acting as a controller. We are also a controller for our employees’ personal data. When oneapp processes your Merchant Content, we are acting as a processor.

If you are a visitor to our website (by which we mean any website that links back to this Privacy Notice in its footer, such as to withoneapp.com, or if you are not a oneapp user and you are attending one of our events, we collect a minimal amount of data about you (depending on how much you’ve chosen to share with us). This might be as little as an IP address or a cookie, and it might be your contact information. We also consider this Merchant Account Data. You can read below about how we process visitors’ Merchant Account Data.

If you are an end user of a oneapp end user, this Privacy Notice does not apply to the services that merchants using the oneapp platform provide to their consumers on or through the oneapp platform. Merchant users have their own policies regarding the collection, use, and disclosure of the personal data of their consumer users. If you are consumer user of one of our merchant users and want to learn about how that merchant handles your personal data, we encourage you to read the merchant's privacy policy. Only the merchant can assist you with requests for access or deletion.

Data about end users

In short, oneapp requires the minimal amount of data necessary to provide services to you, and the amount or type of data we collect depends on the product or service you choose or how you use it. If you choose to share additional information with us so that we can better customize your account and our services, we'll process that with the same care and respect. We do not sell your personal data and we do not share your information with third parties for those third parties' own business interests. This Privacy Notice describes the data we collect from end users at a high level, but you can always learn more by reading our API documentation.

We use the information we collect and share it with our service providers primarily to provide the services you've requested from us, and as needed for our operational purposes (e.g., to do the things we need to do to function as a business, such as to collect payment). In addition, we may use data about end users to detect, prevent, or investigate security incidents, fraud, or abuse and misuse of our platform and services.

Data we process during account creation and account usage

When you sign up for an account with us, we ask for certain information like your contact details and billing information to facilitate payment and communication. We also collect some information automatically, like your IP address, when you log in to your account or when your software application built on oneapp makes requests to our APIs. We use this to understand who is using our services and how, and to detect, prevent and investigate fraud, abuse, or security incidents.

Information You Share Directly:

Name and contact information. When you sign up for a oneapp account with us, we will ask you to give us your name, email address, and optionally, your company name, and to create a password. You can also name your account (or accounts, if you have more than one). We collect this information so we know who you are — this helps us communicate with you by email, text or voice call about your account(s), service-related

information, recognize you when you communicate with us through the account portal or otherwise, bill you correctly, and provide other services.

Telephone number. When you first sign up for an account, we may also ask you for a telephone number (where it's relevant to the service you're using) so we can communicate a verification code to that telephone number and have you enter the code into our website. This helps us verify that you're actually a human being. A oneapp team member may also contact you at this number to help you with onboarding unless you choose not to be contacted.

When you set up two-factor authentication for your account, we may ask you to enter a telephone number to set up the process. You have the option to use that telephone number as the method for us to communicate verification codes to you to verify that it is you logging into your account. We don't use this two-factor authentication phone number for purposes other than providing verification codes; however, if you've given us your phone number in another context, such as in connection with your oneapp account, we may contact you that way.

Payment information. When you upgrade your trial account, we'll ask you to provide our payment processor with your payment method information like a credit card or your Paypal account and your billing address. Our payment processor, acting on our behalf, gathers this so we can bill you for your use of our software as a service. Our payment processor will share your billing address with oneapp. We'll also use your billing address for tax calculation and audit purposes.

Subscriber records. For some products, we may also obtain proof of identity from you that includes a proof of address, name, physical address, or other identification information. For example, to use our Trust Hub or to obtain a phone number in certain countries, local law may require us to have a physical service address on file for the individual who will be using that oneapp number, whether that's you or your end user. We may also need proof of identity and physical service address. We call these "subscriber records."

We may have to share subscriber records with local government authorities or with the local telecommunications carrier that provides connectivity services. We may also use this physical service address for tax purposes. However, we don't share subscriber records for purposes other than this, and we treat these records with our highest confidentiality.

Personalization details. Some of our products, such as our short code service, may require you to complete an application form by providing details about your company and your intended use of the product. We'll use this information for the purpose of

determining eligibility for these products. We may also use it in connection with improving our own internal processes and services or to train our team members.

Information We Generate or Collect Automatically:

SIDs. When you sign up for an account with oneapp, we'll automatically assign you and each of your accounts a unique ID and we'll automatically generate an API token for each of your accounts. These are used like a username and password to make API requests. Instead of using these API tokens, you can provision API Keys and use your API key for authentication when making requests to our APIs. We keep a record of these credentials so we know it is you making the requests when your application makes requests to our API using these credentials.

Merchant Proprietary Network Information. When you use certain voice-based communications services, oneapp may collect information associated with your usage of the services. This includes information such as number of phone calls, call destinations, call locations, type, and service configuration, and is known as Merchant Proprietary Network Information (CPNI). CPNI does not include information such as your name, address, phone number, or the content of phone calls. We use this information to market related oneapp products or services to which you are not already subscribed unless you have exercised your right to opt out. For information about your choices, see the section titled How to make choices about your data below.

Device information and IP addresses. When you use our account portal, we collect your IP address and other data through tracking technologies like cookies, web beacons, and similar technologies. We also collect IP addresses when you make requests to our APIs and in our server logs. We use this information to understand how end users are using our platform, who those end users are (if they are a company and the IP address is associated with that company), what country they are logging in from (for analytics and export control purposes), and to help improve the navigation experience. You can learn more about cookies in the section titled "Cookies and Tracking Technologies" below.

When you use our account portal, we also collect information about your device, such as your computer or mobile device operating system type and version number, manufacturer and model, browser type, screen resolution, unique identifiers, and general location information such as city or town. We do not collect precise geographical information.

Data we process from our website, events, and interactions

When you visit our website, sign up for a oneapp event or request more information about oneapp, we collect information automatically using tracking technologies, like

cookies, and through web forms where you type in your information. We collect this information to provide you with what you request through the web form, to learn more about who is interested in our software as a service, and to improve navigation experience on our pages. You can learn more about cookies in the section titled “Cookies and Tracking Technologies” below.

Information You Share Directly:

In some places on oneapp’s public-facing websites, you can fill out web forms to ask to be contacted by our Sales Team, sign up for a newsletter, register for a oneapp event, or take a survey. The specific personal data requested on these forms will vary based on the purpose of the form. We will ask you for information necessary for us to provide you with what you request through the form (for example, we will ask you for your email address if you want to sign up for an email newsletter and for your phone number if you want a member of our Sales Team to call you). We may also ask you for additional information to help us understand you better as a end user, such as your oneapp use case, your company name, or your role at your company. If you sign up to receive ongoing marketing communications from oneapp, like a newsletter, you can always choose to opt out of further communications through a preferences page which will be linked from any marketing email you receive from oneapp. You can also contact our Merchant Support Team to communicate your choice to opt out.

If you contact our Sales or Merchant Support Teams, those teams keep a record of that communication, including your contact details and other information you share during the course of the communication. We store this information to help us keep track of the inquiries we receive from you and from end users generally so we can improve our software as a service and provide training to team members. This information also helps our teams manage our ongoing relationships with end users. Because we store a record of these communications, please be thoughtful about what information you share with our Sales and Merchant Support Teams. While we will take appropriate measures to protect any sensitive information you share with us, it is best to avoid sharing any personal or other sensitive information in these communications not necessary for these teams to assist you.

Information We Collect Automatically:

When you visit oneapp websites, including our web forms, we and our service providers acting on our behalf automatically collect certain information using tracking technologies like cookies, web beacons, and similar technologies. We use this information to understand how visitors to our websites are using them and which pages and features of the websites are most popular. This helps us understand how we can improve our websites and track performance of our advertisements. In addition, we use tracking

technologies to help improve the navigation experience on oneapp websites. We don't sell this information to third parties. For more details on our use of cookies and other tracking technologies, please read the below section titled "Cookies and Tracking Technologies."

Marketing information

We use your email address to send you information about other oneapp products, services or events in which we think you may be interested. You can opt out of receiving marketing communications from us at any time through your marketing preferences page by clicking the "unsubscribe" link at the bottom of any marketing email you receive from oneapp. You can also update your communication preferences using our online form or contact our Merchant Support Team to communicate your choice to opt out. Please note that it may take up to three days to remove your contact information from our marketing communications lists, so you may receive correspondence from us for a short time after you make your request. You will not be able to opt out of service emails from us, such as password reset emails, billing emails, or notifications of updates to our terms, unless you deactivate your account.

We may also use publicly-available information about you that we have gathered through services like LinkedIn, or we may obtain information about you or your company from third party providers. We use this information to help us understand end users better, such as your industry, the size of your company, and your company's website URL. We also use this information to reach out to potential candidates for roles at oneapp.

When you visit a oneapp website, we process your information to market our services to you on other websites. You are able to opt out of targeted advertisements by using the cookie consent management tool, TrustArc. To learn more about how we process this information and how to make choices about what is collected, please see the "Cookies and Tracking Technologies" Section below.

How Long We Store Your Merchant Account Data

oneapp will store your Merchant Account Data as long as needed to provide you with our services and to operate our business. If you ask oneapp to delete specific personal data from your Merchant Account Data (see 'Choices About Your Merchant Account Data' below), we will honor this request unless deleting that information prevents us from carrying out necessary business functions, such as billing for our services, calculating taxes, or conducting required audits.

More specifically, within 60 days following closure of your account, we will either delete other Merchant Account Data or transform it such that it can no longer be used to identify you, with the following exceptions, depending on and in accordance with applicable law:

- Merchant Account Data is stored for up to seven years following closure of your account. However, we may retain invoice records, including their digital equivalent, for longer periods for accounting, tax, and audit purposes.
- Where we collect subscriber records, we will retain this data for such time as needed for legal, security and anti-fraud purposes.
- We may retain your communications with oneapp's Merchant Support Teams for up to three years after your account is closed.
- We may need to retain data due to special circumstances (such as due to an open investigation, audit, or other legal matter).

Data about end users' end users

What Merchant Usage Data and Merchant Content oneapp Processes and Why

We use Merchant Usage Data and Merchant Content to provide services to you and to carry out necessary functions of our business as a communications service provider. We do not sell your end users' personal data and we do not share your end users' information with third parties for those third parties' own business interests or cross-context behavioral advertising.

The particular end user personal data oneapp processes when you, the end user, use our software as a service, and the reasons oneapp processes end user personal data, depends on how you use our software as a service and which oneapp products and services you use. For that reason, our API docs for each of our software as a service are the best place to find information about our processing of personal data when you use that oneapp product and service. In many cases, you can opt to store records of your communications or other activities in your oneapp account, and these records may include your end users' personal data. You may also have the option to use additional features or tools within oneapp's products or services that allow you to do things such as analyze the records, including end user personal data, in your oneapp account. In those cases, oneapp will process this information to provide you with the service you request.

For oneapp's end users, our Data Protection Addendum describes more about how we process Merchant Content in accordance with your instructions. That Data Protection Addendum is a part of your agreement with us by default.

How Long We Store Merchant Usage Data and Merchant Content

Details regarding how long your end user personal data may be stored on oneapp systems will depend on which oneapp products and services you are using and how you are using them. For that reason, our API docs for each of our software as a service are the best place to find more detailed information about managing end user data collected and stored in connection with your use of our software as a service. We also provide an overview of our retention periods in our support documentation.

As a oneapp end user, if the oneapp product or service you use enables you to store records of your usage on oneapp, including personal data contained within those records, and you choose to do so, then oneapp will retain these records for as long as you instruct, up until termination of your account. In some cases, use of extended storage may cost more. If you later instruct us to delete those records (please see below for information on how to delete your records), we will do so. Please note that it may take up to 30 days for the data to be completely removed from all systems.

How oneapp shares personal data

We do not sell your personal data or the personal data of your end users. We also do not allow any personal data to be used by third parties for their own marketing purposes (except in cases where you explicitly request or provide consent for us to do so, such as at a conference when you direct us to share your information with a sponsor) or share personal data for cross-context behavioral advertising. However, we do need to share personal data in order to provide our software as a service to you, such as to route a call you send through us or to store data you ask us to store. Below are the different scenarios under which we may share your data with third parties.

Telephony operators as necessary for proper routing and connectivity:

oneapp provides applications that make use of the publicly switched telephone network (PSTN) to send communications. Therefore, communications-related data is shared with and received from telephony operators as necessary to route and connect those communications from the sender to the intended recipient. How those telephony operators handle this data is generally determined by those operators' own policies and local regulations.

Other communications service providers for proper routing and connectivity:

oneapp also enables sending or receiving communications through communications service providers that do not use the PSTN, such as Over-the-Top (OTT) communications service providers. If you choose to use oneapp to send or receive communications by way of these providers, oneapp will share communications data with these providers as necessary to route and connect those communications from the sender to the intended recipient. How those OTT communications service providers handle this data is determined by their own policies.

Third-party service providers or consultants:

oneapp engages certain third-party vendors and service providers to carry out certain data processing functions on our behalf. These providers are limited to only accessing or using this data to provide services to us and must provide reasonable assurances they will appropriately safeguard the data.

Sub-processors:

A sub-processor is a vendor that is permitted to process data for which we are a processor — in other words, Merchant Content. We share Merchant Content with sub-processors who assist in providing the oneapp services, like our infrastructure provider, or as necessary to provide optional functionality like transcriptions. An up-to-date list of oneapp sub-processors is located below.

Compliance with Legal Obligations:

We may disclose your or your end users' personal data to a third party if (i) we reasonably believe that disclosure is compelled by applicable law, regulation, legal process, or a government request (including to meet national security, emergency services, or law enforcement requirements), (ii) to enforce our agreements and policies, (iii) to protect the security or integrity of our services and products, (iv) to protect ourselves, our other end users, or the public from harm or illegal activities, or (v) to respond to an emergency which we believe in good faith requires us to disclose data to assist in preventing a death or serious bodily injury. For more details, please see the procedure laid out in our Binding Corporate Rules.

If oneapp is required by law to disclose any personal data of you or your end user, we will notify you of the disclosure requirement, unless we are prohibited by law. Further, we object to requests we do not believe were issued properly.

Business transfers:

If we go through a corporate sale, merger, reorganization, dissolution or similar event, data we gather from you may be part of the assets transferred or shared in connection with the due diligence for any such transaction. In that situation, and that situation only,

we might transfer your data in a way that constitutes a sale under applicable law. If we do, we'll let you know ahead of time, and we will require any acquirer or successor of oneapp to continue to process data consistent with this Privacy Notice.

Aggregated or de-identified data:

We might also share data about end users with third parties if the data has been de-identified or aggregated in a way so it cannot be used to identify you or your end users.

How to make choices about your data

Choices About Your Merchant Account Data

Accessing and Controlling Account Data. As part of the services we provide to end users, we provide you with a number of self-service features at no additional cost within the oneapp console itself, including the ability to access your data, update any incorrect data, download a copy of your data, delete your data, or restrict the use of your data. You can make various choices about your Merchant Account Data through the account portal when you log into your oneapp account or through the marketing preferences center. Any other requests about your data you cannot make through these self-service tools, you can contact Merchant Support.

Closing Your Account and Deletion. To request closure or deletion of your oneapp account, you can contact Merchant Support. Please be aware that closure or deletion of your oneapp account will result in you permanently losing access to your account and the data in the account. After closure of your account, certain information associated with your account may remain on oneapp's servers in an aggregated form that does not identify you or your end users. Similarly, after you close your account, we will retain data — including personal data — associated with your account that we are required to maintain for legal purposes or for necessary business operations (see "How Long We Store Your Merchant Account Data" section above) until it's no longer needed.

Our Support portal provides documentation regarding how to delete the data you control and how long we retain it.

Merchant Proprietary Network Information (CPNI). As an individual oneapp account owner or as an authorized representative of a oneapp end user, you have the right to restrict oneapp's use of CPNI. To opt-out of the use of CPNI data related to your oneapp account to market other oneapp products and services based on your usage of our products, click here. Please note that, if you have subscribed for the services on behalf of an organization, the CPNI relates to the service usage by that organization and not

you individually. Opting-out of the use of CPNI for marketing will not unsubscribe you from other types of marketing contacts from oneapp and will not affect the status of the services you currently have with us. Your approval or opt-out of the use of your CPNI outside of the services to which you are already subscribed is valid until you affirmatively revoke or limit such approval.

Other Choices About Your Merchant Account Data. In addition, you can express other choices about your Merchant Account Data (e.g., accessing it, deleting it, restricting its use, porting it, or withdrawing consent for its use) by contacting Merchant Support.

Choices About Your End Users' Data

We also offer you the ability to delete, access, or exercise other choices about end user data, namely Merchant Usage Data and Merchant Content. Your ability to make choices about this data depends on the oneapp product or service you use and how you use the product or service. For that reason, our API docs for each of our software as a service are the best place to find more detailed information about managing end user data collected and stored in connection with your use of our software as a service.

In some cases, we may retain a copy of your usage records, including the personal data contained in them, to carry out necessary functions like billing, invoice reconciliation, troubleshooting, along with detecting, preventing, and investigating spam, fraudulent activity, and network exploits and abuse. Sometimes legal matters arise that also require us to preserve records, including those containing personal data. These matters include litigation, law enforcement requests, or government investigations. If we have to do this, we will delete the impacted records when we are no longer legally obligated to retain them. We may, however, retain or use records after they have been anonymized, if the law allows.

Cookies and Tracking Technologies

oneapp uses common information-gathering tools such as cookies, web beacons, pixels and other similar tracking technologies to automatically collect information as you navigate our websites, your account or when you interact with emails we sent to you.

Cookies

A cookie is a piece of data contained in a very small text file that is stored in your browser or elsewhere on your hard drive. Cookies allow oneapp to identify your device as you navigate our websites or your account. This makes navigating and interacting with our websites or your account more efficient, easy and meaningful for you.

By themselves, cookies do not identify you specifically. Rather, they recognize your web browser. So, unless you identify yourself specifically to oneapp, like signing into your account, we don't know who you are just because you visited our website.

oneapp uses both session and persistent cookies. Session cookies are cookies that disappear from your computer or browser when you turn off your computer. Persistent cookies stay on your computer even after you've turned it off. Additionally, the cookies on our websites fall into three categories: (1) Required Cookies, (2) Functional Cookies, and (3) Advertising Cookies. To learn more about each category of cookie, you can visit our cookie consent tool by clicking on the "Cookie Preferences" link on the bottom right of the oneapp website you are visiting.

How to Control & Delete Cookies

Using Your Browser. You can use your browser settings to opt out of Functional Cookies and Advertising Cookies. For more information on how to do that, click here. To manage privacy and storage settings for cookies, click here.

Do Not Track. Some browsers allow a "do not track" (DNT) setting that requests that a web application disable its tracking of an individual user. When you choose to turn on the DNT setting in your browser, your browser will send a special signal to websites, analytics companies, ad networks, plug-in providers, and other web services you encounter while browsing and stop tracking your activity. To set up DNT, you can visit the All About DNT page. If you do choose to set up DNT, we will automatically turn off all non-required cookies on oneapp's websites for you. Please note that this may impact the functionality of our websites or your account.

Global Privacy Control. Global Privacy Control (GPC) is a technical specification that you can use to inform websites of your privacy preferences in regard to ad trackers. To set up GPC, you can visit the Global Privacy Control page. If you do choose to set up GPC, we will automatically turn off all non-required cookies on oneapp's websites for you. Please note that this may impact the functionality of our websites or your account.

Opting out of Advertising Cookies. To learn more about how to opt out of targeting and advertising cookies, you can go to the Your Online Choices page, the Network Advertising Initiative page, and the Digital Advertising Alliance's Consumer Choice page. These opt-out tools are provided by third parties, not oneapp. We do not control or operate these tools or the choices that advertisers and others provide through these tools.

Web Beacons

oneapp also uses web beacons to gather data about your use of our websites, your account, and how you interact with emails we have sent to you. Web beacons are clear electronic images that can recognize certain types of data on your computer, like when you view a particular website tied to the web beacon, and a description of a website tied to the web beacon. Additionally, we may put web beacons in marketing emails that notify us when you click on a link in the email that directs you to a oneapp website. We use web beacons to operate and improve our websites and email communications to you.

Global Privacy Compliance at oneapp

oneapp is a global company with end users all around the world. As such, our approach to privacy compliance is a global one. No matter where you are located, we remain committed to abiding by all applicable data protection laws.

Regions Requiring a Legal Basis for Processing Personal Data

If you are from a region that requires a legal basis for processing personal data, our legal basis for collecting and using the personal data described above will depend on the personal data concerned and the specific context in which we collect it.

However, we will normally collect personal data from you only where we need the personal data to perform a contract with you, or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms, or where we have your consent to do so. In some cases, we may also have a legal obligation to collect personal data from you or may otherwise need the personal data to protect your vital interests or those of another person, such as in the case where we request personal data from you in the context of a government audit or in response to a request from law enforcement.

If you have questions about or need further information concerning the legal basis on which we collect and use your personal data, please contact us using the contact information provided below.

Broadly speaking, we use Merchant Account Data to further our legitimate interests to:

- understand who end users and potential end users are and their interests in oneapp’s product and services;
- manage our relationship with you and other end users;
- carry out core business operations such as accounting, filing taxes, and fulfilling regulatory obligations; and

- help detect, prevent, or investigate security incidents, fraud and other abuse or misuse of our software as a service.

United States

State Consumer Access and Deletion Rights

For those end users that would like more information about our use of Merchant Account Data or Merchant Usage Data, you have the ability to request:

- that we provide details about the categories of personal data that we collect about you, including how we collect and share it;
- that we provide you access to, and a copy of, the personal data we collect about you;
- that we update or correct any inaccurate personal data we have about you; and
- that we delete the personal data we have about you.

Please scroll up to our section above on How to make choices about your data for more information about how to make a request.

Please be aware that when you ask us for these things, we will take steps to verify that you are authorized to make the request. You do not have to be from any specific state, such as California, Colorado, Utah, or Virginia, to make this request. We won't discriminate against you or change the price of our services if you make a request, but if you ask us to delete your data, it may affect your ability to use our service.

If you're a Californian interested in what personal data we have shared lately for our business purposes, here's a list:

- Identifiers
- Commercial information
- Financial information
- Internet or other electronic activity information
- Geolocation information
- Professional or employment information

By “our business purposes,” we mean that we only share personal data as we describe in the section above (in other words, with telephony operators, communications providers, and so on).

Other regions

If you are in a region other than the United States, we aren’t forgetting you! Some regions also have specific privacy notice requirements, and we address those requirements in our general privacy sections above. If there are specific changes we need to make to our legal language to comply with a country’s privacy or data protection laws, you can find those changes in our Data Protection Addendum.

Privacy Compliance for Specific Individuals

Information from Children. We do not knowingly permit children to sign up for a oneapp account. If we discover someone who is underage has signed up for a oneapp account, we will take reasonable steps to promptly remove that person’s personal data from our records. If you believe a person who is underage has signed up for a oneapp account, please contact us at support@withoneapp.com.

International data transfers

As a global organization, we may need to transfer your personal data to oneapp affiliates, contractors, service providers, and to third parties in various countries and jurisdictions around the world. In each case, we take care to use appropriate safeguards to ensure your personal data remains protected.

Data transfers to the United States and elsewhere. When you use our account portal, or our other products and services, personal data of you and your end users processed by oneapp may be transferred to the United States, where our primary processing facilities are located, and possibly to other countries where we or our service providers operate. These transfers will often be made in connection with routing your communications in the most efficient way.

Safeguards for data transfers. oneapp employs appropriate safeguards for cross-border transfers of personal data, as required by applicable local law. Where we must transfer end users’ personal data to a third country, we conduct a transfer impact assessment, which we make available on our support pages. Our Data Protection Addendum, which we provide to all end users, includes more detailed information about our cross-border data transfers.

Security Information

How We Secure Personal Data

Our security measures. We use appropriate security measures to protect the security of your personal data both online and offline. These measures vary based on the sensitivity of the personal data we collect, process and store and the current state of technology. We also take measures to ensure service providers that process personal data on our behalf also have appropriate security controls in place. When we transfer data across borders, we also take supplementary measures to ensure that data is protected. You may read more about our security measures in our Security Overview, and if you are located in a country that requires you to obtain information about our supplemental measures, you may read more about those measures here.

Please note that no service is completely secure. While we strive to protect your data, we cannot guarantee that unauthorized access, hacking, data loss or a data breach will never occur.

Security measures you can take. To protect the confidentiality of your account and protect against unauthorized use of your account, we recommend enabling two-factor authentication for your account. Additionally, you must keep your account password and Auth Token confidential and not disclose them publicly or to unauthorized individuals — this includes accidentally distributing them in a binary or checking them into source control. Please let us know right away if you think your password or Auth Token was compromised or misused. For instructions on changing your password, click here. For instructions on changing your Auth Token, click here.

Similarly, if you provision an API Key, you should keep your secret, well... secret. You should store your API Key, Account ID, and secret in a secure location. Information on provisioning and revoking API Keys can be found here.

If you have any oneapp service on your mobile device, you should take measures to protect your device. First, you should set a password and activate biometrics (like Touch ID), where available, for all devices on which you have downloaded your oneapp app.

If you have multiple devices associated with your account and one of your devices is lost or stolen, you can remove that device from your circle of trusted devices by going into one of the other devices associated with your account, and over which you still control, and remove the lost or stolen device under Settings > Devices. If you only have a single device that is associated with your account and that device is lost or stolen, you can alert us by contacting our Merchant Support Team.

How we use personal data for security purposes

We may collect and use Merchant Account Data or Merchant Usage Data to detect, prevent, or investigate security incidents, fraud, or abuse and misuse of our platform and services. In addition, we also use records containing end user personal data to debug, troubleshoot, or investigate security incidents; to detect and prevent spam or fraudulent activity; and to detect and prevent network exploits and abuse. Specifically, we monitor text message content to detect spam, fraudulent activity, and violations of our Acceptable Use Policy. We may anonymize personal data and use it for our legitimate business needs, and, where allowed by law, this may include records containing end user personal data.

Other information you may find useful

Automated decision making and machine learning

oneapp may use automated decision making leveraging a variety of signals derived from records we collect to help monitor, identify, and suspend accounts sending spam or engaging in other abusive or fraudulent activity. Holders of accounts suspended under these circumstances are notified of the suspension and given an opportunity to request human review of the suspension decision.

Changes to our Privacy Notice

We may change this Privacy Notice from time to time, and if we do, the most current version will be available at https://legal.withoneapp.com with the date indicating when it was last updated. These changes might be minor, such as updating an address or fixing a typo, or they might be material, such as making a change that affects your rights. If we make changes that affect your rights, we will provide advance notice to you, such as by posting a message in the oneapp console, or we'll send an email via the address we have on file for you. We will comply with applicable law with respect to any changes we make to this notice and seek your consent to any material changes if this is required by applicable law.

Sub-Processors

Third Party Sub-Processors

oneapp uses the third party companies below (each, a “sub-processor”) to process personal data (i) on behalf of oneapp customers; (ii) in accordance with customer instructions as communicated by oneapp; and (iii) in strict accordance with the terms of a written contract between oneapp and the sub-processor.

oneapp imposes obligations on its sub-processors to implement appropriate technical and organizational measures ensuring that the sub-processing of personal data is protected to the standards required by applicable data protection laws. Further information relating to sub-processor security measures can be found via the external links below.

Where the engagement of a sub-processor requires the cross-border transfer of personal data, oneapp has performed Transfer Impact Assessments for such data transfer.

oneapp maintains an up-to-date list of the names and locations of all sub-processors below. oneapp customers may subscribe to notifications of sub-processor changes to receive updates.

Duration of processing: For each sub-processor below, processing of personal data will be for the duration that the customer uses and continues to use the applicable service(s), and for the retention periods as set out in customer’s agreement with oneapp.

Sub-Processor

Applicable Service(s)

Subject matter

Nature and purpose of processing

Location(s) of processing

External links for additional information relating to security

---

AWS

All services

Personal data contained in communications sent through or uploaded to the services.

Infrastructure Provider providing hosting services and storage.

USA*

Compliance Program; GDPR Centre; Supplementary Measures Addendum; Blog

---

With oneapp Inc.

All Services

If oneapp Inc. is not the oneapp party to the agreement, then oneapp Inc. is acting as a sub-processor for that oneapp party. (For example. If you are contracting with oneapp Ireland Ltd, then oneapp Inc. is acting as a sub-processor for the provision of the services.)

Provision of the oneapp Services

USA*

Data Privacy; Data Security

Service Level Agreements

The table below outlines each service level agreement (“*SLA*”) and the specific services that are covered by the corresponding SLA (“*Covered Services*”). Any capitalized term used but not defined below will have the meaning provided in the corresponding SLA.

SLA:	**Covered Services:**
oneapp APIs Service Level Agreement	Application programming interfaces branded as “oneapp”.

oneapp Trademark Usage Guidelines

These Trademark Usage Guidelines are for oneapp and its affiliates' licensees, authorized resellers, developers, customers, and other parties who wish to use oneapp's trademarks, names, and logos ("oneapp Trademarks") for their own purposes, including in promotional, advertising, instructional, or reference materials, or in or on

websites, products, labels, or packaging. Note that any use of oneapp logos and/or use of any oneapp Trademarks outside of these guidelines requires permission and without such permission may constitute trademark infringement under federal and state laws.

oneapp Trademarks
The oneapp Trademarks are valuable assets oneapp needs to protect. We ask that you help us by properly using and crediting the oneapp Trademarks in accordance with these guidelines.

oneapp Do’s and Don'ts
Below is a list of Do’s and Don’ts that will help guide you in using the oneapp Trademarks correctly:

General Uses of oneapp Trademarks

Do's

- Use the oneapp Trademarks to refer to the associated oneapp products or services. Example: An authorized developer may note in their advertisements and products that they utilize the oneapp software. Similarly, such a developer may issue a press release stating that they have built their product on the oneapp platform.

Don'ts

- Do not use the oneapp Trademarks as the most noticeable or most pronounced aspect in any materials.

- Do not manufacture, sell, or give-away merchandise items, such as T-shirts and mugs, bearing any of the oneapp Trademarks or any other oneapp marks or names, including symbols, logos, or icons, except pursuant to an express written trademark license from oneapp.

Use oneapp Trademarks as Adjectives

Do's

- Use the oneapp Trademarks as adjectives. Example: "oneapp platform's benefits"

- Use a generic term in association with each oneapp Trademark the first time the mark appears in text, and as often as possible after that. You need not include generic names in headlines, package titles and documentation titles. Example: "oneapp platform"

Don'ts

- Do not use the oneapp trademarks as nouns, verbs, or in the possessive or plural form. “oneapp’s benefits” = ✖
- Do not vary the oneapp Trademarks by changing their spelling or abbreviating them. "oneappVBX" or similar = ✖

Truthful and Accurate Use

Do's

- Use or reference the oneapp Trademarks in a truthful and accurate manner.

Don'ts

- Do not use or reference the oneapp Trademarks in a misleading manner.
- Do not use any name or trademark confusingly similar to the oneapp Trademarks or any other trademark or trade name owned by oneapp for which oneapp has not given you permission.
- Do not use the oneapp Trademarks or potentially confusing variations in your Internet domain name. This helps prevent Internet users from being confused as to whether you or oneapp is the source of the web site. Example: www.oneappDomainName.com
- Do not imitate oneapp’s trade dress, type style or logos.
- Do not copy oneapp's layout or styling of its web pages for use with your product, or display your product name in the distinctive logotype associated with the oneapp logo.
- See oneapp’s Logo Usage below for more information.

Relationship with Your Products or Services

Do's

- Indicate the relationship of your products or services to oneapp’s products or services by using accurate, descriptive taglines. Within text or body copy, such tag lines may appear in the same type as your product or service name. Example: You can use "with oneapp technology," or "built on the oneapp platform" in connection with your product or service name

- Make sure that the tag line appears in significantly smaller type than your name on product, packaging, advertising, and any other collateral where your product or service name is displayed apart from body copy.
- Distinguish the tag line from your mark by using a different font or color.
- If using a oneapp Trademark in your product name, please use the oneapp Trademark as an adjective and in a manner that would not cause confusion as to oneapp sponsorship, affiliation or endorsement. Example: XYZ for oneapp Platform NOTE: Please contact the oneapp Legal Department at trademark@oneapp.com if you wish to use a oneapp Trademark in your product name.
- If you are using a tag line or including a oneapp Trademark in your product name, please include the following disclaimer: “This product is not endorsed by or affiliated with oneapp Inc.” unless you do have some official endorsement or affiliation with oneapp Inc.

Don'ts

- Do not use the oneapp Trademarks in such proximity to any of your own trademarks or trade names or third party trademarks so as to create a combination or composite mark.
- Do not use any of the oneapp Trademarks in a manner that could cause confusion as to oneapp sponsorship, affiliation or endorsement; or in a manner that shows oneapp or its products in a false or derogatory light.
- Do not use the oneapp Trademarks or potentially confusing variations as all of your company, product or service names. If you wish to note the relationship of your products or services to oneapp’s products or services, please use an appropriate tag line or product name as detailed in this section. "XYZ [AKA your company or product name] with oneapp technology [AKA the appropriate tag line]" = ✓ “XYZ for oneapp Platform” = ✓ "TwiXYZ or XYZ oneapp" = ✖ “XYZ for oneapp” = ✖
- Do not use the oneapp Trademarks in a manner that would be in violation of our Acceptable Use Policy.

User Groups/Social Media

Do's

- oneapp generally permits use of its marks in a group's name that include phrases such as "user group," "special interest group," etc., that clarifies the relationship between oneapp and the group and does not create confusion about the source of the products or services. NOTE: This applies only to user groups that are not formally doing business as commercial entities.

Relationship of Products or Services

Don'ts

- Do not claim any trademark rights in the name or attempt to register the name or your logo with a trademark office if you are administering a user group that includes a oneapp Trademark in its name.
- Do not register the name as a trade name or business name, or conduct any business under the name if you are administering a user group that includes a oneapp Trademark in its name.
- Do not use oneapp Trademarks in any social media account handles or names, avatars, profile photos, icons, favicons, or banners. Example: @oneappImpersonator

You may indicate the relationship of your products or services to oneapp products or services by using accurate, descriptive tag lines such as "with oneapp technology," "built on the oneapp platform" in connection with your product or service name. Within text or body copy, such tag lines may appear in the same type as your product or service name. On product, packaging, advertising and other collateral where your product or service name is displayed apart from body copy, make sure that the tag line appears in significantly smaller type than your name. You should also distinguish the tag line from your mark by using a different font or color.

Trademark Symbols

Proper trademark attribution through trademark symbols and credit lines helps make others aware of our rights, and helps prevent them from becoming generic terms. Credit lines also help clarify that they belong to oneapp. Accordingly, you should attribute ownership of the oneapp Trademarks to oneapp Inc. by using trademark symbols (^{TM} or ^{SM}) and credit lines as detailed below.

Do's

- Use the ^{TM} symbol with the most prominent appearance of the "oneapp" mark on products, packaging, manuals, advertisements, promotional materials and Web page (for example, in the headline of an advertisement).

- Use the ™ symbol in the first use of the mark in text or body copy. This includes situations where "oneapp" is a part of a product or service name (for example, oneapp™ platform). Example: “XYZ Develops New Product on the oneapp™ Platform. XYZ Corporation has developed the ABC app based on the oneapp™ platform. The ABC app is one of numerous products XYZ has developed using oneapp software.” * Explanation: "oneapp" receives a trademark symbol in the headline because this is the most prominent appearance, and when it appears as part of the "oneapp platform" name because this is the first appearance in text. While there is no trademark symbol after "oneapp" when it appears in front of the term "software" since this is not the first time that the term "oneapp" appeared in body copy. That said, it is always acceptable to continue using the ™ after "oneapp" throughout the document.

Open Source Software

Most open source licenses do not grant, and many exclude, a license of trademark rights. Do not assume you can use the name of a source code base in the name of your distribution developed from that code base. Without a license or permission, you may not incorporate oneapp Trademarks in the name of your distribution or other products that incorporate open source elements. Truthful statements incorporating a trademark are generally allowed (for example, in the format "MyImplementation, derived from Trademarked ProductName"), but you should check the terms of the license for the original source code or any posted trademark guidelines for the project.

“oneapp” as a Trade Name

Trade names are the actual business names of companies. Trademarks and trade names are not the same, even though many companies use their trade names as trademarks. If you are using "oneapp" as a substitute for With One App, Inc., you are using it as a trade name. Because they are nouns, trade names can be used in the possessive and do not require a generic term or a trademark symbol. Thus, you should not use a ™ after "oneapp" when it appears as part of the full corporate name or as a trade name.

Examples:
Corporate Name: This software was developed by With One App, Inc. Trade Name: This software was developed by oneapp. Trade Name: oneapp's latest software developments are outstanding. Trademark: The oneapp™ platform leads the industry.

oneapp Logo Usage

Proper use of oneapp Trademarks reinforces their role as brands for our products and services, and helps prevent them from becoming generic names that can be used by anyone. Examples of former trademarks that became generic terms are "aspirin," "cellophane," and "escalator." By adhering to the following rules, you help protect oneapp's investment in its trademarks.

Request Permission - Logo Usage

The oneapp corporate logo is the most recognizable expression of oneapp's brand. We ask that you help us protect this important asset.

We understand and appreciate that oneapp’s licensees, authorized resellers, developers, customers, as well as outside parties, may want to show affiliation with oneapp. However, use of the oneapp corporate logo to imply affiliation with or endorsement by oneapp without express written permission by oneapp is strictly prohibited. Affiliation with oneapp or oneapp programs does not imply the right to use the oneapp corporate logo.

Please contact the oneapp Legal Department using the contact information below. You will be asked a few questions to help us determine your intended use of the material and your relationship to oneapp. We will respond to you based on our policy and may ask you to provide additional information in order to review your request.

Correct Use

Proper use of the oneapp Trademarks reinforces their role as brands for our products and services, and helps prevent them from becoming generic names that can be used by anyone. Examples of former trademarks that became generic terms are "aspirin," "cellophane," and "escalator." By adhering to the following rules, you help protect oneapp's investment in its trademarks.

Credit Line

Include the following trademark credit line in all products, packaging, manuals, advertisements, promotional materials, and web pages bearing oneapp Trademarks: "oneapp is a registered trademark of oneapp Inc. and/or its affiliates. Other names may be trademarks of their respective owners."

If you are using any oneapp Trademarks in a tag line or your product name, please also include the following disclaimer, unless you do have some official endorsement or

affiliation with oneapp Inc. (as mentioned in the Relationship with your Products or Services section):
“This product is not endorsed by or affiliated with oneapp Inc.”

The credit line and disclaimer may appear anywhere on the collateral, but typically is displayed on a copyright page, the back of a package or at the end of a document or web page.

Ownership

Nothing in these guidelines gives you any right, title, or interest in the oneapp Trademarks, or any other trademark or trade name of oneapp, except the right to use the trademarks solely to identify your actual use of oneapp's software and platform. You agree that the oneapp Trademarks are solely owned by oneapp, and that all uses of the oneapp Trademarks, and all goodwill derived therefrom, whether or not done pursuant to written agreement, shall inure solely to the benefit of oneapp.

Additional Resources

In addition to these Trademark Usage Guidelines, please review the following policies and guidelines to ensure that you use the oneapp Trademarks correctly:

- https://legal.withoneapp.com

Changes to Guidelines

These Trademark Usage Guidelines are not expected to be a complete list of how to use the oneapp Trademarks. oneapp reserves the right to cancel, modify, or change these guidelines at any time. Please contact the oneapp Legal Department at trademark@withoneapp.com if you have any further questions.

Report Usage Violations

Please report suspected misuse of oneapp’s logos, trademarks, or copyrighted material to trademark@oneapp.com.

Questions Or Requests

If you have any questions regarding oneapp Trademarks or to request permission for use, please contact the oneapp Legal Department at:

- support@withoneapp.com

Customer Research and User Experience Acknowledgement and Waiver

By participating in any research and user experience sessions (individually, a "*Session*" and collectively, "*Sessions*") and providing any feedback, observations, comments, criticisms, suggestions, or other information ("*Feedback*") to With One App Inc. (*"oneapp*") in connection therewith, I acknowledge that I understand and agree to the following terms ("*Feedback Terms*"):

- I agree that oneapp has the right to use the Feedback at oneapp's sole discretion, for any reason or purposes, including incorporating any portion of the Feedback into oneapp's products or services, without notice to, payment to or consent from me.
- I hereby irrevocably and unconditionally assign to oneapp all right, title, and interest in and to Feedback and any products or services contemplated thereby or derived therefrom.
- I agree that my name, image, likeness, title, and company/organization affiliation, trademarks, may be used in oneapp's internal business activities to identify me as the source of any statements made during a Session.
- During the Session, I will not disclose to oneapp any confidential information or trade secrets of any current or former employer or other third party and I represent that my participation in the Session does not and will not cause me to breach any agreement or obligation I may have with any current or former employer or other third party.
- I acknowledge that oneapp may provide me with a financial incentive for a Session, which shall be my sole monetary compensation for agreeing to these Feedback Terms, along with the consideration of the opportunity to provide Feedback and potentially benefit from such Feedback as a customer of oneapp.
- **Confidentiality:**
    - Applicability. This language in this provision will apply to the extent that, oneapp and I and/or oneapp and my company/organization are not bound by pre-existing confidentiality obligations through an agreement in effect between the parties, including without limitation, a Non-Disclosure

Agreement, oneapp Terms of Service, or oneapp Platform Agreement (“*Agreement*”).

- Definition. Confidential Information” means any information or data, regardless of whether it is in tangible form, disclosed by either party (“*Disclosing Party*”) to the other party (“*Receiving Party*”) that is marked or otherwise designated as confidential or proprietary or that should otherwise be reasonably understood to be confidential given the nature of the information and the circumstances surrounding the disclosure, including, without limitation, security reports and attestations, audit reports, customer lists, pricing, concepts, processes, plans, designs and other strategies, “know how”, inventions, financial, and other business and/or technical information and materials of Disclosing Party and its affiliates. Confidential Information does not include any information which: (a) is publicly available through no breach of these Feedback Terms or fault of Receiving Party; (b) was properly known by Receiving Party, and to its knowledge, without any restriction, prior to disclosure by Disclosing Party; (c) was properly disclosed to Receiving Party, and to its knowledge, without any restriction, by another person without violation of Disclosing Party's rights; or (d) is independently developed by Receiving Party without use of or reference to the Confidential Information of Disclosing Party.
- Use and Disclosure. Except as otherwise authorized by Disclosing Party in writing, Receiving Party will not (a) use any Confidential Information of Disclosing Party for any purpose outside of exercising Receiving Party’s rights or fulfilling its obligations under these Feedback Terms and (b) disclose or make Confidential Information of Disclosing Party available to any party, except to its, its affiliates’, and their respective employees, legal counsel, accountants, contractors, and in oneapp’s case, subcontractors (collectively, “*Representatives*”) who have a “need to know” as necessary for Receiving Party to exercise its rights or fulfill its obligations under these Feedback Terms. Receiving Party is responsible for its Representatives’ compliance with this confidentiality provision. Representatives will be legally bound to protect Confidential Information of Disclosing Party under terms of confidentiality that are at least as protective as the terms of this provision. Receiving Party will protect the confidentiality of Confidential Information of Disclosing Party using the same degree of care that it uses to protect the confidentiality of its own confidential information but in no event less than reasonable care.

    - Compelled Disclosure. Receiving Party may disclose Confidential Information of Disclosing Party if so required pursuant to a regulation, law, subpoena, or court order (collectively, "*Compelled Disclosures*"), provided Receiving Party gives Disclosing Party notice of a Compelled Disclosure (to the extent legally permitted). Receiving Party will provide reasonable cooperation to the Disclosing Party in connection with a Compelled Disclosure at the Disclosing Party's sole expense.
    - Injunctive Relief. The parties expressly acknowledge and agree that no adequate remedy may exist at law for an actual or threatened breach of this confidentiality provision and that, in the event of an actual or threatened breach of the provisions of this confidentiality provision, the non-breaching party will be entitled to seek immediate injunctive and other equitable relief, without waiving any other rights or remedies available to it.
- **Order of Precedence**
    - In the event of any conflict or inconsistency between the terms relating to the use of Feedback set forth in the Agreement and these Feedback Terms, these Feedback Terms will prevail.

Updates to oneapp Legal Terms and Conditions

Please visit the Terms of Service to review the updates or modifications we make to our legal terms and conditions from time to time, the current version of which is available at https://legal.withoneapp.com.