

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 Process 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:

1. 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;
2. 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;
3. 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;
4. 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;
5. 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;
6. 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;
7. 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;
8. 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;
9. 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
10. 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.