SOCURE END USER AGREEMENT

1.   **USE OF SERVICES.** Partner hereby grants to End User a permission to access the Services and any data contained therein, subject to the restrictions and limitations set forth below:

(i)   **Generally.** Partner hereby grants to End User permission to use the Services solely for End User's own internal business purposes. In addition, subject to the terms of use associated with the applicable API and/or SDK made available by Socure from time to time, including Schedule G attached to this Agreement, End User shall have a non-exclusive, non-transferable, revocable, personal license to use the API, SDK and associated documentation, solely for internal use and solely in connection with End User access to the Services, during the Term. End User will integrate with the SDK in accordance with the applicable documentation to enable collection of device risk data by Socure. End User represents and warrants that all of End User's use of the Services shall be for only legitimate business purposes, including those specified by End User in connection with a specific information request, relating to its business and as otherwise governed by the Agreement. End User shall not use the Services for marketing purposes or resell or broker the Services to any third party and shall not use the Services for personal (non-business) purposes. End User shall not use the Services to provide data processing services to third-parties or evaluate the data of or for third-parties. End User agrees that if Partner determines or reasonably suspects that continued provision of Services to End User entails a potential security risk, or that End User is engaging in marketing activities, reselling, brokering or processing or evaluating the data of or for third-parties, or using the Services for personal (non-business) purposes or using the Services' information, programs, computer applications, or data, or is otherwise violating any provision of this Agreement, or any of the laws, regulations, or rules described herein, Partner may take immediate action, including, without limitation, terminating the delivery of, and the license to use, the Services. End User shall not access the Services from Internet Protocol addresses located outside of the United States and its territories without Partner's prior written approval. End User may not use the Services to create a competing product. End User shall comply with all laws, regulations and rules which govern the use of the Services and information provided therein and has the sole responsibility to implement and use the Services in compliance with all applicable United States and international laws. Partner may at any time mask or cease to provide End User access to any Services or portions thereof which Partner may deem, in Partner's sole discretion, to be sensitive or restricted information. End User shall obtain all necessary consents and approvals required pursuant to applicable laws, (i) for the transfer of consumer information included in a search inquiry to Socure and its vendors, (ii) the use of such information by Socure and its vendors in accordance with this Agreement and (iii) the access by Socure or its vendors to Partner Proprietary Network Information ("CPNI" as such term is defined in the Telecommunications Act). Document Verification and Device Fingerprint Services, to the extent applicable, shall be subject to the terms of Schedule G attached hereto, in addition to the terms of this Agreement.

(ii)   **GLBA Data.** Some of the information contained in the Services is "nonpublic personal information," as defined in the Gramm-Leach-Bliley Act (15 U.S.C. § 6801, et seq.) and related state laws, (collectively, the "GLBA"), and is regulated by the GLBA ("GLBA Data"). End User shall not obtain and/or use GLBA Data through the Services, in any manner that would violate the GLBA, or any similar state or local laws, regulations and rules. End User acknowledges and agrees that it may be required to certify its permissible use of GLBA Data falling within an exception set forth in the GLBA at the time it requests information in connection with certain Services and will recertify upon request by Partner. End User certifies with respect to GLBA Data received through the Services that it complies with the Interagency Standards for Safeguarding End User Information issued pursuant to the GLBA.

(iii)   **DPPA Data.** Some of the information contained in the Services is "personal information," as defined in the Drivers Privacy Protection Act (18 U.S.C. § 2721, et seq.) and related state laws, (collectively, the "DPPA"), and is regulated by the DPPA ("DPPA Data"). End User shall not obtain and/or use DPPA Data through the Services in any manner that would violate the DPPA. End User acknowledges and agrees that it may be required to certify its permissible use of DPPA Data at the time it requests information in connection with certain Services and will recertify upon request by Partner.

(iv)   **Social Security and Driver's License Numbers**. Partner may in its sole discretion permit End User to access full social security numbers (nine (9) digits) and driver's license numbers (collectively, "QA Data"). If End User is authorized by Partner to receive QA Data, and End User obtains QA Data through the Services, End User certifies it will not use the QA Data for any purpose other than as expressly authorized by Partner policies, the terms and conditions herein, and applicable laws and regulations. In addition to the restrictions on distribution otherwise set forth in Paragraph 2 below, End User agrees that it will not permit QA Data obtained through the Services to be used by an employee or contractor that is not an Authorized User with an Authorized Use. End User agrees it will certify, in writing, its uses for QA Data and recertify upon request by Partner. End User may not, to the extent permitted by the terms of this Agreement, transfer QA Data via email or ftp without Partner's prior written consent. However, End User shall be permitted to transfer such information so long as: 1) a secured method (for example, sftp) is used, 2) transfer is not to any third party, and 3) such transfer is limited to such use as permitted under this Agreement. Partner may at any time and for any or no reason cease to provide or limit the provision of QA Data to End User.

(v)   **Fair Credit Reporting Act.**   The Services provided pursuant to this Agreement are not provided by "consumer reporting agencies," as that term is defined in the Fair Credit Reporting Act, (15 U.S.C. §1681, et seq.), (the "FCRA"), and do not constitute "consumer reports" as that term is defined in the FCRA. Accordingly, the Services may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or another purpose in connection with which a consumer report may be used under the FCRA or any similar law or regulatory requirement. Further, (A) End User certifies that it will not use any of the information it receives through the Services to determine, in whole or in part an individual's

eligibility for any of the following products, services or transactions: (1) credit or insurance to be used primarily for personal, family or household purposes; (2) employment purposes; (3) a license or other benefit granted by a government agency; or (4) any other product, service or transaction in connection with which a consumer report may be used under the FCRA or any similar statute, including without limitation apartment rental, check-cashing, or the opening of a deposit or transaction account; (B) by way of clarification, without limiting the foregoing, End User may use, except as otherwise prohibited or limited by this Agreement, information received through the Services for the following purposes: (1) to verify or authenticate an individual's identity; (2) to prevent or detect fraud or other unlawful activity; (3) to locate an individual; (4) to review the status of a legal proceeding; (5) to collect a debt, provided that such debt collection does not constitute in whole or in part, a determination of an individual consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; or (6) to determine whether to buy or sell consumer debt or a portfolio of consumer debt in a commercial secondary market transaction, provided that such determination does not constitute in whole or in part, a determination of an individual consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; (C) specifically, if End User is using the Services in connection with collection of a consumer debt on its own behalf, or on behalf of a third party, End User shall not use the Services: (1) to revoke consumer credit; (2) to accelerate, set or change repayment terms; or (3) for the purpose of determining a consumer's eligibility for any repayment plan; provided, however, that End User may, consistent with the certification and limitations set forth in this section (viii), use the Services for identifying, locating, or contacting a consumer in connection with the collection of a consumer's debt or for prioritizing collection activities; and (D) End User shall not use any of the information it receives through the Services to take any "adverse action," as that term is defined in the FCRA or any similar law or regulatory requirement.

(vi)   MVR Data. If End User is permitted to access Motor Vehicle Records ("MVR Data") from Partner, without in any way limiting End User's obligations to comply with all state and federal laws governing use of MVR Data, the following specific restrictions apply and are subject to change:

(a) End User shall not use any MVR Data provided by Partner, or portions of information contained therein, to create or update a file that End User uses to develop its own source of driving history information.

(b) As requested by Partner, End User shall complete any state forms that Partner is legally or contractually bound to obtain from End User before providing End User with MVR Data.

(c) Partner (and certain third-party vendors) may conduct reasonable and periodic audits of End User's use of MVR Data. Further, in response to any audit, End User must be able to substantiate the reason for each MVR Data order.

(vii)   Retention of Records. For uses of GLB Data, DPPA Data and MVR Data, End User shall maintain for a period of five (5) years a complete and accurate record (including consumer identity, purpose and, if applicable, consumer authorization) pertaining to every access to such data. End User agrees and acknowledges that Socure may retain any data submitted by Partner to the Socure System as necessary for business, legal, regulatory and compliance purposes for a period of at least seven (7) years as set forth in Socure's data retention policy, as amended from time to time, provided such End User data is treated as confidential information so long as held by Socure.

2.   **SECURITY.** End User acknowledges that the information available through the Services may include personally identifiable information and it is End User's obligation to keep all such accessed information confidential and secure. Accordingly, End User shall (a) restrict access to Services to those employees who have a need to know as part of their official duties; (b) ensure that none of its employees shall (i) obtain and/or use any information from the Services for personal reasons, or (ii) transfer any information received through the Services to any party except as permitted hereunder; (c) keep all user identification numbers, and related passwords, or other security measures (collectively, "User IDs") confidential and prohibit the sharing of User IDs; (d) immediately deactivate the User ID of any employee who no longer has a need to know, or for terminated employees on or prior to the date of termination; (e) in addition to any obligations under Paragraph 1, take all commercially reasonable measures to prevent unauthorized access to, or use of, the Services or data received therefrom, whether the same is in electronic form or hard copy, by any person or entity; (f) maintain and enforce data destruction procedures to protect the security and confidentiality of all information obtained through Services as it is being disposed; (g) unless otherwise required by law, purge all information received through the Services and stored electronically or on hard copy by End User within ninety (90) days of initial receipt; (h) be capable of receiving the Services where the same are provided utilizing "secure socket layer," or such other means of secure transmission as is deemed reasonable by Partner; (i) not access and/or use the Services via mechanical, programmatic, robotic, scripted or other automated search means, other than through batch or machine-to-machine applications approved by Partner; and (j) take all steps to protect their networks and computer environments, or those used to access the Services, from compromise. End User agrees that on at least a quarterly basis it will review searches performed by its User IDs to ensure that such searches were performed for a legitimate business purpose and in compliance with all terms and conditions herein. End User will implement policies and procedures to prevent unauthorized use of User IDs and the Services and will immediately notify Partner, in writing to the Partner if End User suspects, has reason to believe or confirms that a User ID or the Services (or data derived directly or indirectly therefrom) is or has been lost, stolen, compromised, misused or used, accessed or acquired in an unauthorized manner or by any unauthorized person, or for any purpose other than legitimate business reasons. End User shall remain solely liable for all costs associated therewith and shall further reimburse Partner for any expenses it incurs due to End User's failure to prevent such impermissible use or access of User IDs and/or the Services, or any actions required as a result thereof. Furthermore, in the event that the Services provided to the End User include personally identifiable information (including, but not limited to, social security numbers, driver's license numbers or dates of birth), the following shall apply: End User acknowledges that, upon unauthorized acquisition or access of or to such personally identifiable information, including but not limited to that which is due to use by an unauthorized person or due to

unauthorized use (a "Security Event"), End User shall, in compliance with law, notify the individuals whose information was potentially accessed or acquired that a Security Event has occurred, and shall also notify any other parties (including but not limited to regulatory entities and credit reporting agencies) as may be required in Partner's reasonable discretion. End User agrees that such notification shall not reference Partner or the product through which the data was provided, nor shall Partner be otherwise identified or referenced in connection with the Security Event, without Partner's express written consent. End User shall be solely responsible for any other legal or regulatory obligations which may arise under applicable law in connection with such a Security Event and shall bear all costs associated with complying with legal and regulatory obligations in connection therewith. End User shall remain solely liable for claims that may arise from a Security Event, including, but not limited to, costs for litigation (including attorneys' fees), and reimbursement sought by individuals, including but not limited to, costs for credit monitoring or allegations of loss in connection with the Security Event, and to the extent that any claims are brought against Partner, shall indemnify Partner from such claims. End User shall provide samples of all proposed materials to notify consumers and any third-parties, including regulatory entities, to Partner for review and approval prior to distribution. In the event of a Security Event, Partner may, in its sole discretion, take immediate action, including suspension or termination of End User's account, without further obligation or liability of any kind.

3.   **PERFORMANCE.** Partner will use commercially reasonable efforts to deliver the Services requested by End User and to compile information gathered from selected public records and other sources used in the provision of the Services; provided, however, that End User accepts all information "**AS IS**." End User acknowledges and agrees that Partner obtains its data from third-party sources, which may or may not be completely thorough and accurate, and that End User shall not rely on Partner for the accuracy or completeness of information supplied through the Services. Without limiting the foregoing, the criminal record data that may be provided as part of the Services may include records that have been expunged, sealed, or otherwise have become inaccessible to the public since the date on which the data was last updated or collected. End User understands that End User may be restricted from accessing certain Services which may be otherwise available. Partner reserves the right to add materials and features to, and to discontinue offering any of the materials and features that are currently a part of, the Services. In the event that Partner discontinues a material portion of the materials and features that End User regularly uses in the ordinary course of its business, and such materials and features are part of a flat fee subscription plan to which End User has subscribed, Partner will, at End User's option, issue a prorated credit to End User's account.

4.   **INTELLECTUAL PROPERTY**. End User agrees that End User shall not reproduce, retransmit, republish, or otherwise transfer for any commercial purposes the Services' information, programs or computer applications. End User acknowledges that Socure (and/or its third-party data providers) shall retain all right, title, and interest under applicable contractual, copyright, patent, trademark, Trade Secret and related laws in and to the Services, the API, SDK and related documentation provided by Socure and the data and information that they provide. End User shall use such materials in a manner consistent with Partner's interests and the terms and conditions herein and shall notify Partner of any threatened or actual infringement of Partner's rights. Notwithstanding anything in this Agreement to the contrary, Socure may use End User's search inquiry data used to access the Services (in the past or future) for any purpose consistent with applicable federal, state and local laws, rules and regulations.

5.   **AUDIT.** End User understands and agrees that, in order to ensure compliance with the FCRA, GLBA, DPPA, other similar state or federal laws, regulations or rules, regulatory agency requirements, this Agreement, and Partner's obligations under its contracts with its data providers and Partner's internal policies, Partner may conduct periodic reviews of End User's use of the Services and may, upon reasonable notice, audit End User's records, processes and procedures related to End User's use, storage and disposal of Services and information received therefrom. End User agrees to cooperate fully with any and all audits and to respond to any such audit inquiry within ten (10) business days, unless an expedited response is required. Violations discovered in any review and/or audit by Partner will be subject to immediate action including, but not limited to, suspension or termination of the license to use the Services, reactivation fees, legal action, and/or referral to federal or state regulatory agencies.

6.   **WARRANTIES/LIMITATION OF LIABILITY.** Neither Partner, nor its subsidiaries and affiliates, nor any third-party data provider (for purposes of indemnification, warranties, and limitations on liability, Partner, its subsidiaries and affiliates are hereby collectively referred to as "Partner") shall be liable to End User (or to any person claiming through End User to whom End User may have provided data from the Partner Services) for any loss or injury arising out of or caused in whole or in part by Partner's acts or omissions in procuring, compiling, collecting, interpreting, reporting, communicating, or delivering the Services. If, notwithstanding the foregoing, liability can be imposed on Partner, then End User agrees that Partner's aggregate liability for any and all losses or injuries arising out of any act or omission of Partner in connection with anything to be done or furnished under this Agreement, regardless of the cause of the loss or injury, and regardless of the nature of the legal or equitable right claimed to have been violated, shall never exceed One Hundred Dollars ($100.00); and End User covenants and promises that it will not sue Partner for an amount greater than such sum even if End User and/or third parties were advised of the possibility of such damages and that it will not seek punitive damages in any suit against Partner. Partner does not make and hereby disclaims any warranty, express or implied with respect to the Services. Partner does not guarantee or warrant the correctness, completeness, merchantability, or fitness for a particular purpose of the Services or information provided therein. In no event shall Partner be liable for any indirect, incidental, or consequential damages, however arising, incurred by End User from receipt or use of information delivered hereunder or the unavailability thereof. Due to the nature of public record information, the public records and commercially available data sources used in Services may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. Services are not the source of data, nor are they a comprehensive compilation of the data. Before relying on any data, it should be independently verified.

7.   **INDEMNIFICATION.** End User hereby agrees to protect, indemnify, defend, and hold harmless Partner from and against any and all costs, claims, demands, damages, losses, and liabilities (including attorneys' fees and costs) arising from or in any way related to (a) use of information received by End User (or any third party receiving such information from or through End User) furnished by or through Partner; (b) breach of any terms, conditions, representations or certifications in this Agreement; and (c) any Security Event. Partner hereby agrees to protect, indemnify, defend, and hold harmless End User from and against any and all costs, claims, demands, damages, losses, and liabilities (including attorneys' fees and costs) arising from or in connection with any third-party claim that the Services or data contained therein, when used in accordance with this Agreement, infringe a United States patent or United States registered copyright, subject to the following: (i) End User must promptly give written notice of any claim to Partner; (ii) End User must provide any assistance which Partner may reasonably request for the defense of the claim (with reasonable out of pocket expenses paid by Partner); and (iii)Partner has the right to control the defense or settlement of the claim; provided, however, that the End User shall have the right to participate in, but not control, any litigation for which indemnification is sought with counsel of its own choosing, at its own expense. Notwithstanding the foregoing, Partner will not have any duty to indemnify, defend or hold harmless End User with respect to any claim of infringement resulting from (1) End User's misuse of the Services; (2) End User's failure to use any corrections made available by Partner; (3) End User's use of the Services in combination with any product or information not provided or authorized in writing by Partner; or (4) any information, direction, specification or materials provided by End User or any third party. If an injunction or order is issued restricting the use or distribution of any part of the Services, or if Partner determines that any part of the Services is likely to become the subject of a claim of infringement or violation of any proprietary right of any third party, Partner may in its sole discretion and at its option (A) procure for End User the right to continue using the Services; (B) replace or modify the Services so that they become non-infringing, provided such modification or replacement does not materially alter or affect the use or operation of the Services; or (C) terminate this Agreement and refund any fees relating to the future use of the Services. The foregoing remedies constitute End User's sole and exclusive remedies and Partner's entire liability with respect to infringement claims or actions.

8.   **FEEDBACK DATA**.   End User hereby agrees as a condition to using the Services that it will provide feedback data on historic transactions. End User will integrate with the feedback API, or at a minimum provide monthly files via Socure's SFTP, in accordance with the documentation provided by Socure.

9.   **ACCEPTABLE USE APPLICATION FORM**. As a condition for accessing the Services, End User shall fully complete an Acceptable Use Application Form, in a form attached as Schedule F hereto, which is incorporated herein by reference, as may be amended by Socure from time to time.