End User License Agreement

This End User License Agreement (**"Agreement"**) governs the use of services or solutions (**"Services")** of Socure Inc. (**"Socure"**) that are sold by Carahsoft Technology Corp. or its affiliates (**"Carahsoft"** or "**Partner"**). Carahsoft and an entity purchasing Services (**"End User"**) will enter in an ordering document or other agreement for such purchase (**"Order"**) that references this Agreement. This Agreement will thereby be deemed incorporated within, and a part of, any such Order.

1. USE OF SERVICES. Partner hereby grants to End User a permission to access the Services and any data contained therein for its own internal business purposes, 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 the Socure Sample Code and Software Development Kit ("SDK") terms of use attached to this Agreement as Attachment SDK, 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. 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 Customer 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 the applicable schedule attached hereto, in addition to the terms of this Agreement. While the Services may be used to assist End User in its compliance with applicable laws and regulations, End User acknowledges and agrees that it is solely responsible for its own legal and regulatory compliance obligations. Without limiting the generality of the foregoing sentence, if End User is a regulated entity subject to the provisions of the U.S. Bank Secrecy Act and implementing regulations, including associated AML requirements, End User shall be solely responsible for its compliance with these laws and regulations and associated regulatory requirements.

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 Customer 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 handling and destruction policies and procedures to protect the security, confidentiality and integrity of all information obtained through Services; (g) not cache or store any information to avoid additional queries; (h) 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 (i) take all reasonable 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. 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 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 search inquiry data used to access the Services (in the past or future) for any business 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 and promptly with any and all audits. 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 Customer 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 not exceed the amounts paid by End User to Partner in the twelve months immediately preceding the event giving rise to the cause of action. 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.**. 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. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. 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 POLICY**. End User represents and warrants that it reviewed and shall fully comply with Socure's Acceptable Use Policy, in the form attached hereto as Schedule AU hereto.

10. **SERVICE LEVEL AGREEMENT.** Partner will provide the Services in a manner consistent with Socure's Service Availability Commitment attached as Schedule SLA.

Attachments

Schedule SDK:	**Socure Sample Code and Software Development Kit Terms of Use**
Schedule AU:	**Socure Acceptable Use Policy**
Schedule SLA:	**Socure Service Availability Commitment**

SCHEDULE SDK

Socure Sample Code and Software Development Kit Terms of Use

In connection with the Service provided pursuant to an Order between Partner and End User (also referred to herein as “Customer”), Socure may provide Customer with access to sample code ("Sample Code") or software development kits consisting of documentation, redistributable libraries ("Libraries"), and other materials provided by Socure and any upgrades, modified versions, additions, and improvements therefor, if any (collectively, the "SDK") designed to enable software developers to integrate the Service into Customer’s own branded applications and/or website (“Applications”).

These terms (the “Terms”), are incorporated into the agreement to which they are attached (**“Agreement”**) and, together with the terms of the Order, govern use of the SDK and, as applicable, related Services described below by Customer. By executing a written order to use of the Sample Code and/or SDK, customer agrees to be bound by the Terms, as may be modified from time to time upon notice to customer.

1. **License.** Subject to compliance with all the terms and conditions set forth in these Terms, the Agreement, and the Order solely during the term of the Order and in connection with Customer’s use of the Service, Socure grants Customer the following limited, non-exclusive, non-transferable, non-sublicensable, revocable licenses to:

   a. use, and (where applicable) authorize its employees to use, the documentation internally solely in connection with modifying Customer’s own branded Applications to incorporate functionalities provided by Socure Services.
   b. incorporate unmodified Libraries into Customer Applications, solely for the purpose of enabling interoperability with the Service, solely in accordance with all applicable documentation and applicable Terms; and
   c. use, modify, and redistribute the Sample Code pursuant to the applicable third-party license, as identified in the headers or associated documentation, solely for the purpose of enabling interoperability with the Service.

2. **Restrictions.** The SDK is owned by Socure or its third-party licensors and is licensed, not sold, to Customer, solely as part of the Services. Except as expressly provided above, the foregoing license does not include any right to (i) redistribute, sell, lease, license, publicly display or modify, make any derivative works to, any portion of the SDK, (ii) use or implement any undocumented feature or API, or use any documented feature or API other than in accordance with applicable documentation. Except if, and solely to the extent that, such a restriction is impermissible under applicable law or applicable Third Party Software (defined below) license terms, Customer may not (y) decompile, reverse engineer, or otherwise access or attempt to access the source code for the SDK not made available to Customer in source code form, or make or attempt to make any modification to the SDK; or (z) remove, obscure, interfere with or circumvent any feature of the SDK, including without limitation any copyright or other intellectual property notices, security, or access control mechanism. Customer may not use the SDK for any purpose other than integrating with the Service in a manner for which the SDK and Service are expressly designed. If Customer is prohibited under applicable law from using the SDK or the Services associated with them, Customer may not use them, and Customer will comply with all applicable laws and regulations (including without limitation laws and regulations related to consumer privacy and export controls) in connection with Customer’s use of the SDK.

3. **Third Party Software.** The SDK consists of a package of components, including certain third-party software ("Third Party Software") that are provided by their authors under separate license terms (the "Third Party Terms"), as described in more detail in the SDK.

4. **Confidentiality.** The SDK (including as embedded in or utilized by any Application) is the confidential and proprietary information of Socure and its licensors and subject to the confidentiality obligations set forth in the Agreement and the Order. Customer shall take all reasonable precautions to prevent unauthorized persons from obtaining access to or use of the SDK and shall notify Socure promptly of any such unauthorized access or use of which Customer becomes aware.

5. **Document Verification and Device Risk Services.** Customer acknowledges that any consumer information collected by Customer and its Applications in connection with Socure’s Document Verification and Device Risk services, including without limitation images, device ID, and device and interaction data, is (i) processed by Socure on the basis of the legitimate interests of Socure and Customer under applicable law; (ii) collected by consumer’s devices and transferred directly to Socure and/or its third party vendors; (iii) processed by Socure and/or its vendors for the purposes set forth in the Agreement, including but not limited to the purposes Socure deems necessary, appropriate or customary to perform the Services, and to operate the business of which the Services are a part, and (iv) retained by Socure after consumers terminate their accounts with Customer. Customer shall (a) ensure its privacy disclosures, including but not limited to website and mobile app privacy policies, accurately reflect and disclose the collection of personal information, including facial images, biometrics identity documents, device attributes, behavioral information and other data used for fraud detection via the Services, and Socure’s processing of consumer information as set forth herein; (b) shall obtain all consents (including express and/or affirmative consents as appropriate) which are or may be required by applicable laws and shall comply with all requirements of such applicable laws (including any consumer notification requirements) necessary; and (c) fully integrate, as reasonably

determined by Socure, with the latest version of each applicable SDK in accordance with applicable documentation to enable Socure's collection of legally required consents. Customers will not claim to consumers that Customer responds to Do Not Track signals as long as it uses the Service.

SCHEDULE AU
Acceptable Use Policy

Company agrees to comply with the following limitations on the use of data provided by the Services: (a) not to use the Services for any "permissible purpose" covered by the Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.) ("FCRA") or use any of the information it receives through the Services to take any "adverse action", as that term is defined in the FCRA; (b) not to use the Services in violation of the Driver's Privacy Protection Act (18 U.S.C. Section 2721 et seq.); (c) not to use the Services in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14 et seq. ("BIPA"), and similar and/or associated laws, whether state, local, foreign, or domestic; (d) not to use the Services other than pursuant to an exception to the privacy provisions of the Gramm-Leach-Bliley Act (15 U.S.C. Sec. 6801 et seq.); and (e) not to use the Services in violation of such other legislation that may be enacted in the future that Socure determines limits the use of the Services by Company. Company will not use the information gathered through the Services that include GLBA or DPPA governed data for marketing purposes. Customer shall provide all necessary notices and obtain all necessary consents and approvals required pursuant to applicable laws, including (i) the transfer of Customer Information to Socure and its vendors, (ii) the use of such Customer Information by Socure and its vendors in accordance with this Agreement, and (iii) the access by Socure or its vendors to Customer Proprietary Network Information. Neither Customer nor any of its shareholders, directors, officers or other principals is a citizen of, entity that is formed in, or has its principal place of business in, a country which is subject to any embargo, prohibition, or similar sanction under applicable laws, or is an individual who is identified on the Specially Designated Nationals or Blocked Persons list provided by the U.S. Treasury Department. Company agrees and acknowledges that at any time Socure may investigate and take appropriate steps to safeguard data provided by the Services and ensure that Company is in compliance with this policy. If at any time, Socure determines, in its sole and reasonable discretion, that Company is not using the data or Services provided in compliance with any of the foregoing, Socure may terminate its MSA with Company immediately without notice and without waiving any claim for damages.

A. GRAMM-LEACH-BLILEY ACT (GLBA) ACCEPTABLE USES

The information that Socure's service provides to the Company may contain consumer identification information governed by the Gramm-Leach-Bliley Act ("GLBA"). In accordance with the GLBA, you certify that such information will only be used for the following purposes:

- Fraud detection and prevention purposes including use to protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability.
- Completion of a transaction authorized by the consumer including but not limited to the collection of delinquent accounts.
- Application Verification including but not limited to (a) employment application verification (however, Socure data cannot be used to make an employment decision as outlined in the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.)), (b) property leasing application information verification (however, Socure data cannot be used for making a leasing decision as outlined in the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.)), and (c) insurance application information verification (however, Socure data cannot be used for making a decision to insure an individual or business as outlined in the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.)). Company represents and warrants that Socure data will not be used for purposes governed by the Fair Credit Reporting Act.
- Law firm and attorney functions including use by persons, or their representatives, holding a legal or beneficial interest relating to the consumer.
- Insurance purposes including (a) account administration, (b) reporting, (c) fraud prevention, (d) premium payment processing, (e) claim processing and investigation, (f) benefit administration, or (g) research projects.
- Required institutional risk control programs including complying with federal, state, or local laws, rules, and other applicable legal requirements.
- Dispute resolution for resolving customer disputes or Inquiries.

B. DRIVER'S PRIVACY PROTECTION ACT (DPPA) ACCEPTABLE USES

The information that Socure's service provides to the Company may contain driver's license and motor vehicle registration information subject to the protections of the Driver's Privacy Protection Act (DPPA). In accordance with DPPA, you certify that such information will only be used for the following purposes:

- Use in the normal course of business, to verify the accuracy of personal information submitted by the individual to the business and, if the submitted information is incorrect, to obtain correct information, but only for the purpose of preventing fraud by, or pursuing legal remedies against, or recovering on a debt or security interest against, the individual. 18 U.S.C. § 2721 (b)(3).
- Use by court or other government agency or entity, acting directly on behalf of a government agency. 18 U.S.C. § 2721 (b)(1).
- Use for any matter regarding motor vehicle or driver safety or theft; to inform an owner of a towed or impounded vehicle. 18 U.S.C. § 2721 (b)(2).
- Use in connection with a civil, criminal, administrative, or arbitral proceeding. 18 U.S.C. § 2721 (b)(4).
- Use by an employer or its agents or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under the Commercial Motor Vehicle Safety Act of 1986. 18 U.S.C. § 2721 (b)(9).
- Use by an insurer or insurance support organization, in connection with claims investigation activities, antifraud activities, rating or underwriting. 18 U.S.C. § 2721 (b)(6).
- Use by a licensed private investigative agency, or licensed security service, for a purpose permitted in items 1 through 6 above. 18 U.S.C. § 2721 (b)(8).
- For use in connection with the operation of private toll transportation facilities.

Data & Access Security Guidelines
In order to protect sensitive information, it is essential to implement and enforce effective information security processes and programs. For businesses that use Socure's API services, this includes but is not limited to the following:

- Implementing and adhering to information security policies that include administrative, physical, and technical safeguards and controls
- Annual security awareness training for all employees
- Implementing strong access controls for users and systems
- Having a security incident response plan, along with tools and procedures for monitoring, detecting, investigating, and reporting security-related events
- Anti-virus software with current definitions scanning employee workstations
- Regular testing of internal controls by third parties

SCHEDULE SLA
Service Availability Commitment

I.Service Availability

The Services will not be available during scheduled downtime and during the loading of new data. Scheduled outages for maintenance and data loading in whole or in part ("Scheduled Downtime") and data loading will occur whenever possible during Non-Business Hours, although some data extract files may not be available during Non-Business Hours and the data load process may occur during Business Hours. "**Business Hours**" means 8 a.m. to 6 p.m. Eastern Time, Monday-Friday, excluding holidays. "**Non-Business Hours**" means all hours that are not Business Hours. Socure will provide a minimum of sixty (60) days' advance notice to Partner in the event of any Scheduled Downtime. In certain circumstances, Partner and End User may agree that the minimum notice period can be less than sixty (60) days. Socure will use commercially reasonable efforts to minimize any disruption, inaccessibility and/or inoperability of the Services in connection with Scheduled Downtime.

All times at which the Services are not available to an End User will be considered "**Excess Downtime**" as to such End User, except downtime caused by Permitted Occurrences. "**Permitted Occurrences**" means: (a) Scheduled Downtime; (c) failure caused by delay or interruption in telecommunications provided by End User or by third party services outside the Socure-controlled network; (d) failure caused by a Force Majeure Event; (e) deficiencies or errors in the data provided by End User; or (f) failure of End User to develop interfaces sufficient for the receipt of the Services. To the extent that Socure's Services are not available to an End User due to End User's intentional or willful misconduct in breach of the Agreement, such unavailability is not considered Excess Downtime.

"Service Availability" means any time, in any given month, in which there is no Excess Downtime.

"Monthly Fee" means any Monthly Minimum Fee (or 1/12 any Annual Minimum Fee) stated in the Order for the Service that suffered Excess Downtime, plus any Transactional Pricing due under such Order for transactions in excess of the applicable Minimum Fee.

Service Availability	**Remedy**
99.90% - 100%	0% credit (calculated out of the Monthly Fee payable for the month in which there was Excess Downtime)
99.51% - 99.89%	1% credit (calculated out of the Monthly Fee payable for the month in which there was Excess Downtime)
< 99.51%	2.5% credit (calculated out of the Monthly Fee payable for the month in which there was Excess Downtime)

II. Terms Applicable to Remedies

For End User to be eligible for the remedy of a credit against the Services Fee, End User must request the credit in a written request to Partner submitted within 20 days after End User experiences the Excess Downtime and setting forth the dates and time of the failure (such that Partner will then be able to submit such written request to Socure within 30 days after End User experiences the Excess Downtime, as required by Socure). A failure to submit such credit request within such time period, time being of the essence, will constitute a waiver of such right. Any credit will be applied against the next applicable invoice, provided, however if there is a credit at the time of termination or expiration of the Agreement, Partner shall pay the credits due to End User hereunder no later than 60 days after such termination or expiration.

IN NO EVENT WILL THE TOTAL CREDITS DURING ANY CONTRACT QUARTER FOR FAILURE TO ACHIEVE SERVICE AVAILABILITY EXCEED A TOTAL OF 10% OF THE QUARTERLY (PRORATED) SERVICES FEE UNDER THE APPLICABLE SOCURE ORDER.

The remedies stated in this Schedule B will be the sole remedy of End User in the event of a failure to provide Service Availability as set forth on this Schedule B.

III. Support Services

During the Term, Partner (through Socure) will provide End User help desk support for the Service Platform and the other Services on a 24x7x365 basis. Partner (through Socure) will respond to bugs and issues reported by End User as provided below at any time and use reasonable commercial efforts to provide resolution as soon as is technically and operationally feasible.

Priority and escalation for all issues related to maintenance and upkeep of the Service Platform and related Services (Partner (through Socure) shall use reasonable commercial efforts to provide resolutions within the timeframes set forth below):

Severity Level	Impact	Definition	Initial response time frame from receipt of service call	Targeted service restoration
1	Major Outage	(i) A problem has been identified that makes the continued use of one of more systems impossible; or (ii) Problem may cause loss of data and/or restrict data availability and/or cause significant impact to the Customer.	30 minutes	5 hours
2	Service Disruption	(i) production system, or environment, or a major portion of the system or environment, is degraded, impeding critical business processing and/or causing disruption to normal production workflow; (ii) development is down, disrupting critical development; or (iii) a Severity 3 problem has remained unresolved for 48 hours.	2 hours	8 hours

3		(i) A problem that does not have a major effect on the Service Platform or Services used to support applicable business operations. (ii) A problem for which an acceptable work around exists is available and operations can continue in a restricted fashion.	2 hours if call is received prior to 12:00 p.m. Eastern Time	48 hours
4		(i) General user questions about usage of software or web reporting. (ii) Support Items that don’t affect processing	Next business day	Next scheduled release