SOCURE INC.
SERVICES TERMS OF USE

THIS SERVICES TERMS OF USE ("**Agreement**") is entered into by and between **Socure Inc.**, a Delaware corporation ("**Socure**") with its principal place of business at 885 Tahoe Blvd. Suite 1 Incline Village, Nevada 89451, and the Customer (as defined below).

A. Socure has developed a SaaS platform that provides fraud prevention, identity verification and KYC/AML compliance solutions.

B. The Prime Contractor identified below may, under an agreement between Socure and Prime Contractor (the **"Socure Partner Agreement"**), sell use of such platform and solutions to Customer. Any and all Socure services sold to Customer, directly or indirectly, by Prime Contractor, all of which include, as essential functions thereof, the collection, retention, use, analysis, testing and processing of Customer personal information in order to process individual transactions as well as to continually develop and improve the services and their underlying features, models and databases, are referred to herein as the **"Services**.**"** References herein to the **"Service Platform"** means Socure's SaaS platform through which it provides any such Services.

C. This Agreement shall govern Customer's use of any and all Services and the Service Platform.

D. A party shall be a **"Customer"** for the purposes of the Agreement, and this Agreement shall become effective and binding between such party and Socure, immediately upon the earlier of (1) such party's acceptance of an order referencing this Agreement or (2) such party accessing or utilizing the Services or the Service Platform. Customer fully accepts, and agrees to be bound by, this Agreement, and this Agreement shall become effective and binding between the parties, immediately upon such acceptance, access, or use, as applicable. The date this Agreement becomes effective under this paragraph is referred to herein as the **"Effective Date."**

Prime Contractor: _____ (or its permitted successor or assignee)

This Agreement consists of the attached Terms and Conditions and the following Schedules:

SCHEDULES

Schedule A:	Service Availability
Schedule B:	Socure Sample Code and Software Development Kit Terms of Use
Schedule AU:	Acceptable Use Policy
Schedule DPA:	Data Processing Agreement

TERMS AND CONDITIONS

1. **Services**. Nothing herein obligates Socure to provide Services or the Service Platform to Customer. To the extent Customer is provided Services and the Service Platform, this Agreement shall govern Customer's use thereof. Customer acknowledges and agrees that Customer's continued access to the Services and the Services Platform is contingent on the existence of the Socure Partner Agreement and the Prime Contractor's compliance therewith. In the event Socure or Prime Contractor terminates or suspends the Socure Partner Agreement, Customer's access shall be suspended until a new agreement is executed by Socure and Prime Contractor. Customer further acknowledges that it would not have access to the Services or the Service Platform but for its execution of this Agreement and its compliance herewith.

1.1 **Generally.** Any access to Services and the Service Platform provided to Customer shall be limited to the employees or agents of Customer ("**End Users**") for Customer's own internal business purposes. Any Customer access to Services and the Service Platform shall end at the end of the term of this agreement and may be suspended or terminated as provided under Section 1.1 and as otherwise provided in this Agreement. The Services will be provided remotely by Socure via the Internet, hosted from facilities determined by Socure. Customer may only utilize the Services with respect to individuals residing in the United States. Document Verification and Device Risk Services, shall be subject to the terms of Schedule B attached hereto, in addition to the terms of this Agreement.

1.2 **Service Availability.** Socure agrees to provide the Services to Customer in compliance with the service availability commitment set forth in Schedule A; provided, however, that any credits due thereunder will be credited from Socure to the Prime Contractor and Socure shall not be responsible for the Prime Contractor crediting the same to Customer.

1.3 **Performance.** Customer and End Users accept all information "AS IS" and acknowledge and agree that Socure obtains its data from third party sources, which may or may not be completely thorough and accurate, and that they shall not rely on Socure for the accuracy or completeness of information made available via the Services. Customer and End Users understand that not all services or data are available to all customers. Socure 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.

1.4. **Feedback Data.** Customer hereby agrees as a condition to using the Services that it will provide feedback data on the types and outcomes of historic transactions as detailed in the documentation. Customer will integrate with the feedback API, or at a minimum provide monthly files via Socure's SFTP, in accordance with the documentation.

1.5 **Acceptable Use Policy**. As a condition for accessing the Service Platform, Customer 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.

1.6 **License to API, SDK and Documentation.** Subject to the terms of this Agreement, Schedule A attached hereto and the specific terms of use associated with the applicable API and/or SDK made available by Socure from time to time, Socure grants to Customer a non-exclusive, non-transferable, revocable, personal license to use the API, applicable SDKs, and associated documentation, solely for internal use and solely in connection with Customer's access to the Service Platform, during the Term.

1.7 **Integration Updates**. The Customer shall ensure proper integration with the latest version of each component of the Services (e.g., Socure's Sigma models, APIs or applicable SDKs) promptly following Socure making them generally available and prior to submitting any transactions in the production environment, in accordance with the applicable documentation and with any implementation certification and approval process made available by Socure.

2. **Term and Termination.**

2.1 **Term.** Subject to this Section 2, this Agreement commences on the Effective Date and continues (i) for so long as Prime Contractor sells Services to Customer and (ii) thereafter until terminated by either Party by written notice to the other (the **"Term"**). For the avoidance of doubt, Socure may terminate and/or suspend Customer's access to the Services (and any related licenses) upon notice to Socure by Prime Contractor that Prime Contractor has terminated or suspended, as applicable, Services to the Customer. Notwithstanding anything to the contrary, prior to activating a Customer's account and access, Socure may at any time and in its sole discretion, terminate this Agreement and refuse to provide the Services, in which event Socure will refund any monies pre-paid by Customer.

2.2 **Termination for Breach.** If either party materially breaches this Agreement, the non-breaching party will have a right to terminate this Agreement, provided that, for breach capable of cure, the non-breaching party notifies the breaching party in writing of the breach, gives the breaching party 60 days to cure the breach, and the breach is not cured within the 60-day period. Socure may terminate this Agreement immediately in its sole discretion upon Customer's breach of Sections 3, 4 or 8 of this Agreement. Customer may terminate this Agreement immediately in its sole discretion upon Socure's breach of Section 3 of this Agreement.

3. **Proprietary Rights.**

3.1 **Socure Ownership and Permission to Use Content.**

3.1.1 Customer acknowledges that Socure and its licensors own the Services, associated documentation, API(s) and SDK(s), including the Content (as defined herein) and all rights related to or arising from the Service Platform. Subject to

Section 3.2, and except for the access permissions granted in this Agreement, this Agreement does not confer to Customer any right of ownership in the Services. Customer acknowledges that subject to Section 3.2, the Services and the Content (excluding Customer Information) are proprietary in nature and owned exclusively by Socure or Socure's licensors. Customer is welcome to provide suggestions, comments, instructions, ideas and report issues related to the Services or the Service Platform ("Suggestions"), which may influence how Socure prioritizes its development efforts provided, however, that any and all Suggestions shall be owned exclusively by Socure.

3.1.2 Socure hereby grants Customer permission to display, copy, distribute and download the content and the information that Socure provides through the Service Platform and its dashboard (collectively, the "Content") that reflects information generated by the Service Platform in connection with Customer Information, provided that: (a) the copyright notice pertaining to such Content remains on the Content and a permission notice (e.g., "Used with permission") is added to such Content; (b) the use of such Content is solely for Customer's internal business purposes; (c) such Content will be treated as Confidential Information and will not be copied or posted on any third party networked computer or published in any medium, except as explicitly permitted by Socure in a separate agreement or grant of permission that is separate from and in addition to the Agreement; and (d) no modifications are made to such Content. This permission will terminate automatically and without any notice if Customer breaches this Agreement, and Socure may revoke this permission at any time upon notice to Customer. Upon termination or revocation of this permission, Customer must immediately destroy any downloaded and/or printed Content (unless it constitutes solely Customer Information, or reports that refer specifically to Customer Information, in which events Customer may continue holding it).

3.1.3 Customer acknowledges that Socure owns exclusively all rights related to or arising from Socure's Marks (as defined below), and agrees that any use of Socure's Marks by Customer (to the extent permitted hereunder) will be solely for and will inure solely to Socure's benefit. Except as otherwise expressly stated in this Agreement, nothing in this Agreement will be construed as conferring any license to Socure's Marks. "Socure's Marks" means and includes all names, marks, brands, logos, designs, trade dress, slogans and other designations Socure uses in connection with its business, services and products.

3.2. Ownership of Customer Information.

3.2.1 As between Socure and the Customer, all data that is provided by Customer (including Customer's consumer data that Customer makes available hereunder) for analysis by the Service Platform ("**Customer Information**"), will remain the property of Customer. Any insights or data derived by Socure or the Services from Customer Information shall not be considered Customer Information.

3.2.2 Socure may process Customer Information in order to provide the Services, including, without limitation for the purposes set out in this Agreement. Customer hereby grants to Socure a non-exclusive license to collect, use, copy, store, transmit and display Customer Information as provided above. Customer shall provide all necessary notices and obtain all necessary consents and approvals required pursuant to applicable laws, including as to (i) the transfer of Customer Information to Socure and its vendors, (ii) the collection and 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 ("CPNI" as such term is defined in the Telecommunications Act).

3.3 License of Customer Marks. Customer hereby grants to Socure a non-exclusive, license to use the trademarks, trade names and service marks owned and used by Customer in the conduct of its business (the **"Customer Marks"**) to the extent necessary to provide the Services.

3.4 Display of Best Matched Entity. KYC transactions manually processed by a Customer End User via the dashboard available to Socure customers (operational parameters set forth in the documentation) may display personal information that Socure has determined to be the best available match for the identifiers submitted (information resulting from such transactions referred to as "BMEI"). Unless otherwise authorized in writing, this functionality may only be accessed on a manual, per-transaction basis by an End User (not via any automated means), solely for the purpose of internal quality assurance relating to the Services and shall otherwise be treated as a KYC transaction under the Agreement. BMEI (a) may comprise personal information and shall be used in accordance with all applicable laws; and (b) shall be considered Content, but may not be copied, downloaded, exported or disclosed to third parties.

4. <u>Customer Conduct</u>.

4.1 Access.

At Socure's request, Customer must identify the End Users who will be authorized by Customer to have access to and use the Services on behalf of Customer. Customer will only permit authorized End Users to access and use the Services. Customer will appoint one End User to be Customer's primary agent in authorizing End User access to the Services. Customer may also appoint secondary agents of Customer in authorizing End User access to the Services. Socure has no obligation to verify the identity of, and Customer is solely responsible for the acts of, any person who gains access to the Services by means of Customer's authorized access. Customer is solely responsible for monitoring End Users' access to and use of the Services, and for any failure by any End User to comply with the Agreement; a failure to comply with the Agreement by an End User is a failure by Customer. Customer must immediately take all necessary steps, including providing notice to Socure, to effect the termination of access for any End User (a) upon the End User's termination of access rights (whether through separation of employment or otherwise), (b) if there is any compromise in the security of passwords, or (c) if unauthorized use is suspected or has occurred. A unique API Key shall be required for each unique authorized source of transactions, such as independently operating affiliates, lines of business or third-party referral sources. Customer represents and warrants that it is a public sector entity, more specifically that it is an organization that is owned, operated, or substantially controlled by a government agency at the national, state, or local level.

4.2. Compliance.

4.2.1 Customer will use the Services pursuant to, and only for the purposes set forth in, this Agreement. Customer will not use, nor will Customer permit any End User to use, the Services for any unlawful purpose or in furtherance of any unlawful purpose, or any purpose that does not comply with Socure's Acceptable Uses, as identified in the Socure Acceptable Use Policy. 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 (the "SDN List"). If Socure has reasonable grounds to believe that Customer or any End User is using the Services for any improper purpose or appears on the SDN List, Socure may suspend or terminate the Services immediately upon notice to Customer.

4.2.2 Customer will not use the Services or the Content in any way that violates any applicable domestic or international law, regulation or rule, including, without limitations any of the following (to the extent they apply): (a) the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq. ("**FCRA**"); (b) the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq. ("**GLBA**"); (c) the Driver's Privacy Protection Act, 18 U.S.C. § 2721, et seq. ("**DPPA**"); (d) the Illinois Biometric Information Privacy Act, 740 ILCS 14 et seq. ("**BIPA**"); or (e) any other statute, regulation, rule or other governmental mandate that governs the use of the Services or Content. Socure is not a consumer reporting agency, does not prepare consumer reports, and does not intend nor permit any of its Services or Content to be used as or incorporated into a consumer report, as such terms are defined by the FCRA or any similar law or regulation. Customer agrees that it will not use any part of the Services or Content in any way that is regulated by the FCRA or any similar law or regulation. If and to the extent that the Content is transferred by Customer to its own customers or other third parties (in whole or in part), then Customer warrants that its agreement with such customers will have covenants and restrictions similar to the ones set forth in this Section 4.2.2.

4.2.3 While the Services may be used to assist Customer in its compliance with applicable laws and regulations, Customer 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 Customer is a regulated entity subject to the provisions of the U.S. Bank Secrecy Act and implementing regulations, including associated AML requirements, Customer shall be solely responsible for its compliance with these laws and regulations and associated regulatory requirements. Customer also acknowledges and agrees that it is solely responsible for its own personal information handling practices.

4.2.4 Intentionally Omitted.

4.3. Unauthorized Conduct.

4.3.1 Customer will not, directly or indirectly, transmit or permit End Users to transmit, directly or indirectly, to any of Socure's servers any Unauthorized Code. "**Unauthorized Code**" means any virus, software program or segment of code, or other programming design, instruction, or routine that permits unauthorized access to any Socure server, or the Services and is intended to damage, detrimentally interfere with, surreptitiously intercept, or expropriate any of the foregoing or any system, data, or personal information.

4.3.2 Customer will not use nor permit others to use the Services or the Content in a way that (a) violates, misappropriates or impairs any Socure or third party rights, including but not limited to property, intellectual property, privacy, publicity and treatment of personal information; (b) is abusive, deceptive, defamatory, offensive or obscene; (c) permits or seeks to permit the unauthorized use, disclosure or access of/to the Services or Content, including but not limited to (except as expressly permitted by applicable law or contract): data mining, copying, storing, transmitting, assigning, caching/storing to avoid additional queries (re)selling, (sub)licensing, distributing, displaying, publishing, benchmarking, scanning, monitoring, mirroring, framing, embedding, scraping, linking, modifying, translating, combining, creating derivative works, disassembling, decompiling, and reverse engineering; (d) violates/circumvents contractual usage restrictions or any monitoring, reporting or authentication mechanisms; or (e) has the goal or effect of: (i) circumventing, breaching, probing or compromising any privacy or security measures,(ii) gaining unauthorized access to any information, services or systems (including but not limited to phishing, pharming or spoofing), (iii) disrupting the integrity, availability or operation of any information, services or systems (e.g. DoS, DDoS).

4.3.3 Customer will not remove or alter any of Socure's Marks, or co-brand its own products, services or material with Socure's Marks, without Socure's prior written consent. Customer will not incorporate any of Socure's Marks into Customer's trademarks, service marks, company names, Internet addresses, domain names, or any other similar designations, for use on or in connection with Customer's business or any of Customer's products, services or technologies.

4.4 Audit. Socure, upon reasonable advance notice to Customer, at its sole cost and expense, shall have the rights to audit, inspect and otherwise monitor Customer's compliance with this Agreement or any other contractual obligations of Customer related to the Services, including, without limitation, compliance with all applicable laws and regulations, but no more frequently than once during a twelve (12) month period. Customer agrees to cooperate fully with respect to any and all audits and to respond to such audit inquiry within fifteen (15) business days, unless an expedited response is required. If any audit by Socure results in Socure being notified that Customer is not in compliance with a legal requirement or any of Customer's obligations to Socure, Socure, in its sole discretion, shall either (i) require Customer to take appropriate action to remedy the non-compliance and provide Socure with evidence of the steps taken to rectify the audit finding or (ii) suspend and/or terminate this Agreement immediately by providing written notice to Customer. Socure will provide Customer with copies of Socure's current security policies and procedures and a copy of all applicable current third-party data security audit reports, including, but not limited to, Socure's SOC 2 Type II report, provided that Socure shall only be obligated to provide such documentation

once in any twelve (12) month period. Customer and Socure agree this Agreement shall be deemed to be amended from time to time to the extent necessary to comply with all applicable federal and state laws and/or privacy and information security requirements and directives of regulators having jurisdiction over either Party.

5. Reserved

6. Warranty

6.1 Limited Warranty. Socure warrants solely to Customer that it has full authority to execute and perform this Agreement. Customer acknowledges that Socure may use third-party service providers in the performance of the Services.

6.2 Disclaimer of Warranties. THE PARTIES ACKNOWLEDGE THAT THE SERVICES ARE BASED, IN WHOLE OR IN PART, ON THIRD PARTIES' WEBSITES, SERVICES AND ANALYSIS, AND THAT NO WARRANTY MAY BE PROVIDED IN CONNECTION THERETO. FURTHERMORE, EXCEPT AS SET FORTH IN SECTION 6.1 AND SCHEDULE A (SERVICE LEVEL COMMITMENT), THE SERVICES (INCLUDING THE SERVICE PLATFORM) ARE PROVIDED TO CUSTOMER "AS IS", WITH NO WARRANTIES WITH RESPECT TO THE FUNCTIONALITY OF THE SERVICE PLATFORM, ITS OPERABILITY, USE OR ABILITY TO ACTUALLY DETECT IDENTITY THEFT OR FRAUD, AND SOCURE DOES NOT WARRANT THAT THE SERVICES (INCLUDING THE SERVICE PLATFORM) WILL MEET CUSTOMER'S REQUIREMENTS, THAT THE OPERATION OF THE SERVICE PLATFORM WILL BE UNINTERRUPTED OR THAT THE SERVICE PLATFORM IS ERROR-FREE. THE ENTIRE RISK REGARDING THE QUALITY AND PERFORMANCE OF THE SERVICES (INCLUDING THE SERVICE PLATFORM) IS WITH CUSTOMER. SOCURE HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SERVICES (INCLUDING THE SERVICE PLATFORM), INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

7. Limitation of Liability.

7.1 Aggregate Liability. IN NO EVENT WILL SOCURE'S AGGREGATE LIABILITY FOR ANY AND ALL CLAIMS, LOSSES OR DAMAGES ARISING OUT OF OR RELATING TO THIS AGREEMENT OR ANY SERVICES (WHETHER IN CONTRACT, EQUITY, NEGLIGENCE, TORT OR OTHERWISE) EXCEED THE AGGREGATE FEES PAID BY PRIME CONTRACTOR TO SOCURE, FOR SERVICES PROVIDED TO CUSTOMER, UNDER THE SOCURE PARTNER AGREEMENT, DURING THE TWELVE-MONTH PERIOD IMMEDIATELY PRECEDING THE DATE UPON WHICH THE APPLICABLE CAUSE OF ACTION ARISES, LESS ANY LIABILITY OF SOCURE TO THE PRIME CONTRACTOR UNDER THE SOCURE PARTNER AGREEMENT.

UNDER NO CIRCUMSTANCES WILL SOCURE OR ITS LICENSORS BE LIABLE FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFIT OR LOSS RESULTING FROM BUSINESS INTERRUPTION EVEN IF SOCURE HAS BEEN ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. SOCURE WILL NOT BE LIABLE FOR ANY DELAY, LOSS OR DAMAGE ATTRIBUTABLE TO ANY SERVICE, PRODUCT OR ACTION OF ANY PERSON OTHER THAN SOCURE OR ITS AGENTS.

THE FOREGOING LIMITATIONS REGARDING AGGREGATE LIABILITY AMOUNT SHALL NOT APPLY TO LIMIT LIABILITY RESULTING FROM FRAUDULENT OR WILLFUL BREACH OF ANY OBLIGATION HEREUNDER NOR TO ANY MATTERS FOR WHICH LIABILITY CANNOT BE LIMITED BY LAW.

The parties acknowledge that Socure has set its prices and entered into this Agreement in reliance upon the limitations of liability and the disclaimers of warranties and damages set forth in this Agreement. The parties acknowledge that the limitation and exclusions of liability and disclaimers specified in this Agreement will survive termination or expiration of this Agreement and apply even if found to have failed of their essential purpose.

8. Confidential Information.

8.1 Confidentiality. Each party will hold all Confidential Information received from the other party in strict confidence and shall not directly or indirectly use, copy, transfer or disclose any Confidential Information, other than for the purposes described in this Agreement, unless specifically authorized by the disclosing party in writing. The receiving party understands and acknowledges that all items of Confidential Information are valuable and material confidential information or trade secrets of the disclosing party and affect the successful conduct of the business of the disclosing party. **"Confidential Information"** means the confidential and proprietary information of the disclosing party, including any and all ideas, information, concepts, designs, logos, names, know how, techniques, processes, methods, inventions, products, works of authorship, discoveries, developments, source code and object code, other programming code, algorithms, innovations, improvements, and other proprietary property of a party of any kind, whether tangible or intangible, whether in written or other form (collectively, **"Intellectual Property"**), and its technical information, and operating procedures and production technologies, that is labeled or otherwise designated as confidential, or that by its nature would reasonably be expected to be kept confidential. Without limiting the generality of the above, Socure's Confidential Information shall also include (a) the terms and conditions of this Agreement, (b) the Services and all Intellectual Property embodied therein and all Intellectual Property rights relating thereto, and (c) any insights or data derived by Socure or the Services from Customer Information (excluding the Customer Information). Confidential Information shall not include information which (i) at the time of disclosure, was published, known publicly, or otherwise in the public domain through no fault of the receiving party; (ii) receiving party can demonstrate was in it's possession on a nonconfidential basis, (iii) was or is obtained by the recipient party from a third party, provided, that, such third party was not bound by a contractual, legal or fiduciary obligation of confidentiality to the any other party with respect to such information, or (iv) is independently developed by the receiving party without reference to the Confidential Information.

8.2 Deletion of Confidential Information. Whenever requested by the disclosing party following the termination of the Agreement, the receiving party will immediately destroy or permanently erase all manifestations of the Confidential Information. For avoidance of doubt, upon termination hereof, the Customer may continue holding any written reports generated by the Service Platform and which include specific information related to or analysis of the Customer Information. Customer agrees and acknowledges that Socure may retain Customer Information (including Customer Information provided to Socure under any previously executed proof-of-concept or evaluation agreement) as necessary for the purposes described in this Agreement, and for legal, regulatory, and compliance purposes, which includes retention of information reasonably necessary to evidence compliance with applicable laws, for a period of up to seven (7) years as set forth in Socure's data retention policy.

8.3 Compelled Disclosure. If the receiving party becomes legally compelled to disclose any Confidential Information of disclosing Party, receiving Party will provide disclosing party with prompt (but, in any event, no less than ten days prior to the legally compelled disclosure) notice of that request(s) so that disclosing party may seek an appropriate protective order or other appropriate remedy and/or waive receiving party compliance with the provisions of this Agreement. If that protective order or other remedy is not obtained by the date that receiving Party must comply with the request, or if disclosing party waives compliance with the provisions of this Agreement, receiving Party will provide only that portion of the Confidential Information of disclosing party which is legally required, and will exercise commercially reasonable efforts to obtain a protective order or other reliable assurance that confidential treatment will be accorded to that portion of the Confidential Information of disclosing party which is being furnished or disclosed.

9. Indemnification.

9.1 Indemnification by Customer.

9.1.1 Customer's obligations to indemnify and holding Socure harmless under this Agreement shall not apply to the extent Customer is prohibited from agreeing to such obligations under applicable law. Socure acknowledges that, if Customer is a government entity, some or all such obligations may be so prohibited.

9.1.2 Customer will indemnify Socure for, and hold Socure harmless from and against, any and all Liabilities (as defined herein) or Expenses (as defined herein) at any time due, owing, paid or incurred by, or assessed against, Socure arising out of (a) a breach, noncompliance or misrepresentation by Customer with respect to its obligations or representations at Sections 3.2.2 or 4 of this Agreement or Schedule AU; or (b) any third party claim related to Customer Information, Customer's use of the Service Platform or the Content, except to the extent the claim is attributable to the actions of Socure in violation of an obligation under law, regulation or this Agreement; provided however, that Socure must give Customer prompt notice in writing of the institution of the Proceeding (as defined herein), permit Customer to defend the same and give Customer all available information assistance and authority (at Customer's expense) in connection therewith. Customer will have control of the defense of any such Proceeding including appeals and of all negotiations therefor, including the right to effect the settlement or compromise thereof. **"Liabilities"** means all liabilities, losses and claims (including judgments, interest, fines, penalties, attorneys' fees due any other party, court costs, and amounts to be paid in settlement) reasonably incurred in connection with any Proceeding. **"Expenses"** includes all attorneys' fees and costs, retainers, court costs, transcripts, experts' fees, witness fees, travel expenses, computer costs, duplicating costs, printing and binding costs, telephone charges, postage, delivery service fees and all other disbursements or expenses reasonably incurred in connection with asserting or defending claims. **"Proceeding"** includes any threatened, pending or completed action, suit, arbitration, mediation, alternate dispute resolution mechanism, investigation, administrative hearing or any other proceeding, whether civil, criminal, administrative or investigative.

9.2 Indemnification by Socure. Socure will indemnify Customer for, and defend and hold Customer harmless from and against, any and all Liabilities or Expenses at any time due, owing, incurred by, or assessed against, Customer arising out of claims brought by third parties, relating to or connected with, directly or indirectly, any claim that Customer's use of the Services in accordance with this Agreement infringes or otherwise violates any, patent, trademark or copyright of any such third party; provided however, that Customer must give Socure prompt notice in writing of the institution of the Proceeding, permit Socure to defend the same and give Socure all available information assistance and authority in connection therewith. Socure will have control of the defense of any such Proceeding including appeals of and all negotiations therefor, including the right to effect the settlement or compromise thereof. In case the Services are in any such Proceeding alleged or held to constitute infringement, Socure will at its option and expense (a) procure for Customer the right to continue using the Services, (b) replace the same with materially equivalent or superior non-infringing Services, or (c) modify the same so that it becomes non-infringing without materially impairing or degrading its performance or functionality. Socure, however, will not have any liability whatsoever to Customer or End Users to the extent that any such infringement, or claim thereof, is based upon or arises out of (i) compliance with the design, plans or specifications furnished by or on behalf of Customer as to the Services, (ii) the use of the Services in combination with apparatus or devices not used or supplied by Socure if the action would have been avoided by use of other apparatus or devices, (iii) the use of the Services in a manner for which the same was neither designated nor contemplated, or (iv) the claimed infringement of any patent in which Customer or any subsidiary or affiliate of Customer has any direct or indirect interest, by license or otherwise. The foregoing states the entire liability of Socure for or resulting from such infringement or claim thereof with respect to the Services.

10. Miscellaneous.

10.1 Equitable Relief. Either party may enforce any provision of this Agreement by obtaining equitable relief in addition to all other remedies at law or under this Agreement. Each party agrees the remedies at law for a breach of any provision of this Agreement are inadequate and the nonbreaching party will suffer irreparable harm from any such breach. The rights and remedies of the parties under this Agreement are cumulative and not alternative and are in addition to any other right or remedy

set forth in any other agreement between the parties, or which may now or subsequently exist at law or in equity, by statute or otherwise.

10.2 Notice. Any written notice connected with this Agreement will be sufficiently made on the mailing date if sent by registered, certified or first class - postage prepaid mail or e-mail to the party at its address set forth on the cover page of this Agreement. All legal notices to Socure shall be made by e-mail to legal@socure.com, Attn: Head of Legal.

10.3 Force Majeure. Each party to this Agreement will be excused for delays in performing or from its failure to perform hereunder (other than payment delays or failures) to the extent that the delays or failures result from causes beyond the reasonable control of such party ("**Force Majeure Event**"); provided that, in order to be excused from delay or failure to perform, such party must act diligently to remedy the cause of the delay or failure.

10.4 Assignment. This Agreement will be binding upon Socure's or Customer's successors or assigns, as the case may be. However, neither this Agreement nor any of Customer's rights, privileges, duties or obligations under this Agreement may be assigned, sublicensed, sold, mortgaged, pledged or otherwise transferred or encumbered by Customer without the prior written consent of Socure.

10.5 Intentionally Omitted.

10.6 Waiver of Breach. No waiver by either party of any breach of this Agreement will constitute a waiver of any other breach of the same or other provisions of this Agreement. No waiver by either party will be effective unless made in writing and signed by an authorized representative of that party.

10.7 Severability. If any provision in this Agreement is invalid or unenforceable in any circumstance, its application in any other circumstances and the remaining provisions of this Agreement will not be affected thereby.

10.8 Entire Agreement. This Agreement, together with its Schedules, constitutes the entire agreement and understanding of the parties relating to the subject matter hereof. This Agreement supersedes all prior written and oral agreements and all other communications between Socure and Customer. Amendments to this Agreement will be effective only if written and signed by Socure and Customer.

10.9 No Third-Party Beneficiaries. Except as expressly provided in this Agreement, each party intends that this Agreement will not benefit, or create any right or cause of action in or on behalf of, any person or entity other than Customer and Socure.

10.10 Interpretation and Priority of Documents. In the case of conflicts or inconsistencies between the terms of this Agreement and any Schedule or Attachment hereto, the terms of this Agreement will prevail, except as specifically stated otherwise.

10.11 Authority; Counterparts. Customer's signature is by an authorized representative of Customer and constitutes Customer's acceptance of this Agreement and its agreement to be bound hereby. This Agreement may be executed and delivered by the parties in counterparts (each of which will be considered for all purposes an original) and by facsimile, electronic signature (i.e., DocuSign) or by e-mail transmission in PDF format, and when a counterpart has been executed and delivered by each of the parties, by facsimile, electronic signature or e-mail in PDF format or otherwise, all such counterparts and facsimiles will together constitute one agreement.

10.12 Headings; Interpretation. The Section headings in this Agreement are for identification purposes only and will not affect the interpretation of this Agreement. Unless business days are specified, all references to "days" means calendar days.

10.13 Survival. Sections 3, 6.2, 7, 8, 9 and 10 will survive the expiration or earlier termination of this Agreement.

10.14 Publicity. Subject to the confidentiality obligations of this Agreement, Socure may issue a press release regarding the Parties' relationship and the parties shall jointly issue a press release, case study or webinar. Socure will provide a draft of the press release to Customer for review of factual accuracy. Each Party may refer to the other Party as required by applicable law, or in its public filings and/or marketing materials as a customer or vendor, as applicable.

SCHEDULE A

Service Availability Commitment

I. Service Availability

The Services will not be available during scheduled downtime for maintenance ("Scheduled Downtime"). Socure will provide a minimum of thirty (30) days' advance notice to Customer in the event of any Scheduled Downtime. In certain circumstances, Socure and Customer may agree that the minimum notice period can be less than thirty (30) 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 Customer will be considered "**Excess Downtime**," except downtime caused by Permitted Occurrences. "**Permitted Occurrences**" means: (a) Scheduled Downtime; (b) failure caused by delay or interruption in telecommunications provided by Customer or caused by third party services outside the Socure-controlled network; (c) failure caused by a Force Majeure Event; (d) deficiencies or errors in the data provided by Customer; or (e) failure of Customer to develop interfaces sufficient for the receipt of the Services. To the extent that Socure's Services are not available to Customer due to Customer's 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 fees owed for usage of the Services (i.e. based on the Transactional Pricing in the applicable Order Form) that suffered Excess Downtime during the month such Excess Downtime occurred.

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 Customer to be eligible for the remedy of a credit against the Monthly Fee, Customer must request the credit in a written request to Socure submitted within 30 days after Customer experiences the Excess Downtime, and setting forth the dates and time of the failure. 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, Socure shall pay the credits due to Customer hereunder no later than 30 days after such termination or expiration.

If Customer chooses to terminate the Agreement because of Excess Downtime exceeding 24 hours in a calendar month, it must provide written notice to Socure within 30 days after the event of Excess Downtime specifying the dates and time of the Excess Downtime. Termination will be effective at 11:59 p.m. on the 15th day after such notice is made.

IN NO EVENT WILL THE TOTAL CREDITS DURING ANY CONTRACT QUARTER FOR FAILURE TO ACHIEVE THE SERVICE LEVELS SET FORTH IN THIS SCHEDULE A EXCEED A TOTAL OF 10% OF THE TOTAL MONTHLY FEES FOR THE QUARTER DURING WHICH THE FAILURE OCCURED.

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

III. Support Services

During the Term, Socure will provide Customer help desk support for the Services and the other Services on a 24x7x365 basis. Socure will respond to bugs and issues reported by Customer and shall 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 Services (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 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 Services used to support applicable business operations, (ii) A problem for which an acceptable work around exists and 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 issues that don't affect processing	Next business day	Next scheduled release

SCHEDULE B

Socure Sample Code and Software Development Kit Terms of Use

In connection with the services and solutions (the "Service") provided by Socure, Inc. ("Socure") pursuant to an agreement between Socure or its resellers (the "Agreement") and the customer named therein ("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 and together with the terms of the Agreement, govern use of the SDK and, as applicable, related Services described below by Customer. By downloading, installing, or otherwise accessing or using 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.

This Schedule B is subject to Section 9.1.1 of the Agreement.

1. License. Subject to compliance with all the terms and conditions set forth in these Terms and the Agreement, solely during the term of the Agreement 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. Customer agrees to indemnify, defend and hold Socure and its affiliates, officers, directors, suppliers, licensors, and other customers harmless from and against any and all liability and costs, including reasonable attorneys' fees incurred by such parties, in connection with or arising out of Customer's Applications, Customer's use or misuse of the SDK, or Customer's violation of these Terms.

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. 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 this 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 the applicable documentation to enable Socure's collection of legally required consents. Notwithstanding any other language to the contrary, Customer will without limitation, fully indemnify and hold Socure harmless from and against any and all claims, demands, actions, losses, liabilities, damages and expenses (including, attorneys' fees and costs of litigation), arising from or in any manner related to a breach of the foregoing warranty. Socure third-party licensors shall have the right to enforce the terms of the Agreement (including these Terms) on Customer. Customer will notify Socure of any requests by consumers relating to Socure's processing of consumers' information, including requests by consumers to access information or opt out. 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. 18 U.S.C. § 2721 (b)(10)

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 DPA
DATA PROCESSING AGREEMENT

The terms of this Data Processing Agreement (together with all attachments hereto, the "Schedule" or "DPA") are incorporated into the Agreement. Except as specifically stated herein, all of the terms, provisions, requirements and specifications contained in the Agreement remain in full force and effect, and the terms of this Schedule are in addition thereto. In the event of any conflict or inconsistency between the provisions of the Agreement and this Schedule with regard to the subject matter of this Schedule, the provisions of this Schedule shall control. Capitalized terms used but not herein defined shall have the same meanings as set forth in the Agreement. This Schedule shall survive termination of the Agreement for so long as any Customer Personal Data is retained.

1. **Definitions.** Unless otherwise set out in this DPA, any capitalized terms not defined in this DPA shall have the respective meanings given to them in the Agreement.

   a. "**Customer Personal Data**" means Personal Data contained within Customer Information (as defined in the Agreement).

   b. "**Data Protection Laws**" means all laws relating to the collection, use, retention, disclosure, processing, privacy, and protection of Customer Personal Data that are applicable to Customer, Socure, or the Services (as defined in the Agreement).

   c. "**Data Subject**" means an individual who is the subject of Customer Personal Data (or to whom the Customer Personal Data relates).

   d. "**Data Subject Request**" means a request made by a Data Subject to exercise a right conferred on them in relation to Customer Personal Data by Data Protection Laws.

   e. "**Personal Data**" means any information relating to an identified or identifiable individual. Where the applicable Data Protection Laws provide as such, "Personal Data" may also include any information relating to an identified or identifiable household or device.

   f. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data.

   g. "**Sub-processor**" means any sub-contractor engaged by and acting under the instructions of Socure that agrees to receive from and process on behalf of Socure any Customer Personal Data.

2. **Data Processing.**

. Socure will only process Customer Personal Data in accordance with: (i) the Agreement, to the extent necessary to provide the Services; and (ii) the Customer's written instructions contained in the Agreement, unless required by applicable laws.

a. The Agreement (subject to any changes to the Services agreed between the parties), including this DPA, shall be the Customer's complete and final instructions to Socure in relation to the processing of Customer Personal Data.

b. Socure shall promptly notify Customer if, in its opinion, an instruction of the Customer infringes Data Protection Laws or if applicable law requires it to process the Customer Personal Data other than in accordance with the Customer's instructions and this DPA.

c. If any modification to this Agreement is required to comply with a material change in Data Protection Law, then either Party may notify the other in writing and propose modifications, and the Parties may renegotiate the terms of this Agreement.

d. Each Party is solely responsible for its own compliance with the Data Protection Laws, including without limitation the lawfulness of any transfer of personal data required to obtain or provide the Services.

e. Customer shall have sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer acquired or obtained the Customer Personal Data, including providing any required notices, or obtaining any required consents, to Data Subjects. If Customer is using the services for UK residents:

i. Customer shall ensure that it makes available to such individual consumers a copy of the CRAIN located at https://www.socure.com/crain(which Customer may do via a URL link clearly presented to the consumer), and shall provide an appropriate written notification (the "CRAIN Notification") to consumers setting out that

1. the information is provided to Socure who may share it with a credit reference or fraud prevention agency which may keep a record of that information pursuant to Data Protection Law; and

2. the credit reference or fraud prevention agency may disclose that information, and the fact a search was made, to its other customers for the purposes of verifying identity, assessing the risk of giving credit, preventing fraud and tracing debtors.

ii. Upon Socure's written request, Customer shall promptly provide the CRAIN Notification to Socure, for the purpose of providing the CRAIN Notification to the credit reference or fraud prevention agency.

3. The California Consumer Privacy Act. The parties acknowledge and agree that, where Socure is a service provider for the purposes of the California Consumer Privacy Act of 2018 ("CCPA"): (a) Socure is receiving and utilizing Customer Personal Data for a Business Purpose, as defined in Cal. Civ. Code § 1798.140; (b) Socure shall not "sell" or "share" any Customer Personal Data, as those terms are defined by CCPA; and (c) Socure shall not retain, use, or disclose any Customer Personal Data, except as necessary for the purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or permitted by the CCPA.

4. Sub-Processors

. Customer agrees that Socure may engage Sub-processors to process Customer Personal Data in accordance with this DPA in connection with providing the Services.

a. Customer acknowledges that a list of Sub-processors shall be provided upon request. Socure may update such Sub-processors list from time to time as required to provide the Services. Socure shall notify Customer of any such updates using the means provided in the Agreement for providing notices and within a reasonable timeframe prior to the Sub-processors processing Customer Personal Data.

b. When engaging Sub-processors, Socure shall enter into agreements with the Sub-processors to bind them to obligations which are substantially similar to those set out in this DPA.

5. Data Security

. Socure will implement technical and organizational measures to ensure a level of security appropriate to the risk posed by the processing of Customer Personal Data, as follows: (i) Socure shall maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards that will: (A) ensure the security and confidentiality of the Customer Personal Data; (B) protect against any anticipated threats or hazards to the security or integrity of such Customer Personal Data; (C) protect against unauthorized access to or use of such Customer Personal Data; (D) limit access, use, and disclosure of such Customer Personal Data as expressly permitted herein; (E) ensure the proper disposal of Customer Personal Data upon termination or expiration of this Agreement; (F) ensure the encryption of Customer Personal Data at rest using a current industry acceptable encryption method (e.g., AES-256 or stronger encryption); (G) comply with applicable law regarding the handling of such Customer Personal Data; and (H) include control objectives that meet one or more of the following industry standards ISO 27002, FFIEC, OCC, or NIST.; (ii) Socure shall require its Sub-processors to maintain internal policies and procedures designed to: (A) secure any Customer Personal Data processed by Socure against accidental or unlawful loss, access or disclosure; (B) identify reasonably foreseeable and internal risks to security and unauthorized access to the Customer Personal Data processed by Socure; and (C) minimize security risks, including through risk assessment and regular testing; (iii) Socure will, and will use reasonable efforts to ensure that its Sub-processors periodically will: (A) conduct periodic reviews of the security of its network and the adequacy of its information security program as measured against industry security standards and its policies and procedures; and (B) evaluate the security of its network and associated services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

a. Socure may update such measures from time to time to reflect changes in operations, practices, and any new or increasing risks, provided that the level of security shall not be reduced or diminished.

b. Socure shall notify Customer within a reasonable timeframe and without undue delay of confirming that a Personal Data Breach has occurred and shall provide Customer with reasonable assistance to allow Customer to notify Data Subjects or applicable regulatory authorities of the Personal Data Breach where required by applicable Data Protection Laws.

6. Audits

. Upon Customer request, Socure will provide documentation and information (and where required by law allow for and contribute to audits) sufficient to demonstrate Socure's and its Sub-processors' compliance with their respective obligations under Data Protection Laws and this DPA ("Audit"). Where required by Data Protection Laws, Socure agrees to allow for and contribute to any such Audit requested under this section. Alternatively, Socure may arrange for a qualified, independent auditor to conduct an audit of Socure's policies and technical and organizational measures in support of the obligations under this DPA using an appropriate and accepted control standard or framework and audit procedure for the audits, as applicable.

a. Socure agrees to provide a report of the Audit to Customer upon request. Any information provided by Socure under this Section 6 is Socure Confidential Information.

b. Except as otherwise required by Data Protection Laws, Customer Audits under this Section 6 shall occur no more than once in any 12 month period.

7. Requests or Demands from Governmental or Regulatory Bodies. Customer acknowledges that any requests or demands from governmental or regulatory bodies that Socure may receive in connection with its processing of Customer's Personal Data are governed by the Compelled Disclosure section of the Agreement.

8. Data Subject Rights

. Customer shall not forward to Socure any Data Subject Request unless Customer has first verified that the Services were used in connection with the Data Subject. Customer shall notify Socure within 7 days of receipt of any applicable Data Subject Request by emailing the contact specified in Appendix 1 and shall encrypt any Customer Personal Data provided in connection therewith. Socure shall support Customer in responding to applicable Data Subject Requests.

a. Socure shall provide notice to Customer within 7 days of confirming that a Data Subject Request relates to Socure's provision of the Services to Customer. Customer's point of contact for communications related to Data Subject Requests is as specified in Appendix 1. Customer has validated that the contact channel for Data Subject Requests is monitored at all times during regular business hours.

b. Socure shall, except as required (or where prohibited) under applicable law, notify Customer within 7 days if it receives a Data Subject Request and, where possible and applicable, Socure shall provide Customer with commercially reasonable cooperation and assistance as is necessary for Customer to comply with its obligations under the Data Protection Laws in relation to any such Data Subject Request. Customer agrees that Socure's cooperation and assistance obligations may be satisfied by providing Customer with the means to delete, export, or otherwise retrieve Customer Personal Data from Socure systems.

c. Customer shall use its best efforts to respond to and resolve promptly all Data Subject Requests which Socure provides to Customer.

d. To the extent legally permitted, Customer shall be responsible for any reasonable costs arising from Socure's provision of assistance under this Section 9.

9. Data Deletion. Unless otherwise required by applicable laws to which Socure or its Sub-processors are subject, Customer Personal Data will be deleted at the same time and manner in which Customer Information is deleted pursuant to the Agreement.

10. Cross border transfers.

. **Global Applicability.** This DPA applies to Socure's processing of Customer Personal Data for the locations specified in the Order Form(s), regardless of whether the processing involves cross border transfers of such data. The Parties represent that they do not believe the laws and practices in any country to which Customer Personal Data is transferred for purposes of the Agreement will prevent Socure or Customer from fulfilling their obligations under this DPA or applicable Data Protection Laws.

a. **UK, EEA, and Switzerland**. If Socure's Processing of Personal Data involves the transfer of Personal Data of Customer's Data Subjects located in the European Economic Area ("EEA"), United Kingdom ("UK") and/or Switzerland to a country or territory outside of those regions, the Parties acknowledge that Socure is an active participant in the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and the Swiss-U.S. Data Privacy Framework, and hereby incorporate, and agree to comply with, the Standard Contractual Clauses of June 4, 2021 ("EU SCCs") approved by the European Commission and the UK International data transfer addendum to the EU SCCs (the "UK Addendum") issued by the UK Information Commissioner on February 2, 2022 to the EU SCCs. In such case: (i) Module 1 (Controller to Controller) of the EU SCCs shall apply if Socure is designated as a Controller for a particular processing activity, as set forth in Appendix 1. The Parties further agree that the competent supervisory authority where Module 1 applies is the Irish Data Protection Commission (DPC) for the EEA or the Information Commissioner's Office (ICO) for the UK; (ii) Module 2 (Controller to Processor) of the EU SCCs shall apply if Socure is designated as a Processor for a particular processing activity, as set forth in Appendix 1. The Parties further agree that, with respect to Clause 17, Option 1 is selected, and the governing law shall be the laws of Ireland for the EEA and the laws of England and Wales for the UK; (iii) The Parties agree that Appendix 1 to this DPA provides all relevant information to complete Annexes I & II to the EU SCCs and the Tables in Part 1 of the UK Addendum.

b. **Canada**. If Socure's Processing of Personal Data involves the transfer of Personal Data of Customer's Data Subjects located in Canada: (i) Customer acknowledges that it has assessed and found adequate the lawfulness, necessity, and proportionality of the processing of Personal Data in connection with the Services; (ii) Customer acknowledges and agrees that it is fully responsible for providing required notices and obtaining required consents from Data Subjects with regard to the processing of their Personal Data in connection with the Services. Customer will not deploy the Services if it deems any notices

of consents provided by Socure to be non-compliant with Canadian Data Protection Laws, unless it has first provided supplemental notices and consents to its customers; (iii) Customer is responsible for conducting all required privacy and data transfer compliance documentation, including Privacy Impact Assessments (PIAs) and Data Transfer Impact Assessments (DTIAs); and (iv) For any Services involving the processing of biometric data, Customer represents and warrants that it has: (a) provided its customers with a non-biometric based alternative means for identification, verification, or fraud prevention; (b) meaningfully informed its customers of the non-biometric alternative means before deploying the Services; and (c) notified any regulators required to receive information relating to its use of a biometric database.

APPENDIX 1 to Schedule DPA

Table 1: Parties

Start date	DPA Effective Date	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Socure Inc. Trading name (if different): N/A Main address (if a company registered address): 885 Tahoe Blvd Suite 1, Incline Village, NV 89451 Official registration number (if any) (company number or similar identifier):
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name: Alan Tse Job Title: Global Privacy Lead Contact details including email: privacy@socure.com

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	Yes	No	No	Option 2	14 days	No

2	Yes	No	No	N/A	N/A	Yes
3	No	N/A	N/A	N/A	N/A	N/A
4	No	N/A	N/A	N/A	N/A	N/A

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex I.A: List of Parties:

Importer: Socure

Activities relevant to the data transferred under these Clauses: Providing the Services, as that term is defined in the Agreement.

Role: Processor with respect to the Services, except where Data Protection Law provides that it shall be a Controller with respect to specific processing activities.

Exporter: Customer

Activities relevant to the data transferred under these Clauses: Procuring the Services, as that term is defined in the Agreement.

Role: Controller with respect to individual transactions. No role with respect to Socure machine learning or product development and improvements.

Annex I.B: Description of Transfer:

Categories of data subjects whose personal data is transferred: Data subjects whose personal data is transferred to Socure include Customer's customers and may also, from time to time, include Customer's employees or contractors.

Categories of personal data transferred: Personal data transferred may be any of the data described in the "Collection of Personal Information" section of Socure's Privacy Statement.

Annex I.B: Description of Transfer:

Categories of data subjects whose personal data is transferred: Data subjects whose personal data is transferred to Socure include Customer's customers and may also, from time to time, include Customer's employees or contractors.

Categories of personal data transferred: Personal data transferred may be any of the data described in the "Collection of Personal Information" section of Socure's Privacy Statement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: Sensitive data categories: data revealing racial or ethnic origin, biometric data, and criminal convictions and offenses. Restrictions and safeguards include encryption at rest and in transit, access restrictions, restrictions for onward transfers, and purpose limitation.

Frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): The data is transferred on a continuous basis in order for Socure to provide the Services.

Nature of the processing: Processing may include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Purpose(s) of the data transfer and further processing: The purpose of the data transfer is for Socure to provide the Services set forth in the Agreement. Any further processing is done in accordance with Customer's written instructions, and may include machine learning and product development or improvements.

Period for which the personal data will be retained, or, if not possible, the criteria used to determine that period: The personal data is retained in accordance with the Agreement, but in any event, not longer than 7 years from the date of collection. More information about Socure's data retention practices is available here.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: The nature of the processing is such that the personal data is transferred in order for Socure to perform the Services in accordance with the Agreement. The nature and duration of the processing is set forth in the relevant processor or sub-processor agreements.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Description of the technical and organizational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: Relevant Certifications include: SOC 2 Type 2, ISO 27001:2013 — for Information Security, ISO 27701:2019 — for Privacy Information Management, ISO 27017:2015 — for Information Security Controls within a Cloud Environment, and ISO 27018:2019 — for Privacy of PII held within a Cloud Environment. Additional Measures are described in [Security Addendum] to the Agreement.

For transfers to (sub-) processors, also describe the specific technical and organizational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter: Processors and sub-processors are subject to terms similar to those in this DPA.

Annex III: List of Sub processors (Modules 2 and 3 only):

To be provided upon request.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Importer may end this Addendum as set out in Section 19 of UK Addendum.