Arkose Labs

(https://www.arkoselabs.com)

Master Service Terms and Conditions

ARKOSE LABS, INC.

MASTER SERVICE TERMS AND CONDITIONS

These Master Service Terms and Conditions (the "**Agreement**") are effective as of ________________, 2023 by and between Arkose Labs, Inc., a Delaware corporation, located at 2 W 5th Avenue Floor 3, San Mateo, California 94402 ("**Arkose Labs**") and _________________, a __________, located at ____ ("**Client**" as further defined below). The parties hereby agree as follows:

1. **DEFINITIONS.**

"**Arkose Labs API**" means the Arkose Labs application programming interface and any related scripts, widgets, embeddable snippets, and other tools provided in connection therewith.

"**Arkose Labs Data**" means any information, materials or content provided or generated by or on behalf of Arkose Labs in the provision or operation of the Services, including without limitation, any data or content provided by Arkose Labs through or in connection with the Arkose Labs API.

"**Arkose Labs Technology**" means the Services, including without limitation, the Arkose Labs API, all Arkose Labs Data, all Documentation, and all ideas, concepts, inventions, systems, platforms, software, interfaces, tools, utilities, templates, forms, techniques, methods, processes, algorithms, know-how, trade secrets and other technologies, implementations and information that are used by Arkose Labs in providing the Services and the Arkose Labs API.

"**Client**" means the named entity that is party to this Agreement with Arkose Labs.

"**Client Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Client, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

"**Client Content**" means all materials displayed or performed on or accessible through the Client Websites, including, but not limited to, text, graphics, articles, photographs, images, illustrations, audio clips and video clips, excluding any Arkose Labs Technology.

"**Client Data**" means information that will be provided by or on behalf of Client to or through the Services, or otherwise to Arkose Labs in connection with Client's use of the Services.

"**Client Technology**" means the intellectual property rights of Client created independently of this Agreement.

"**Client Websites**" are the websites or other online services (including any internet-enabled mobile applications) owned or operated by Client for which Client uses the Services pursuant to this Agreement.

"**Digital Marketplace**" means an online or electronic marketplace operated or controlled by a third party through which Arkose Labs has authorized the marketing, distribution, and sale of its Services, including but not limited to AWS Marketplace.

"**Documentation**" means the documentation provided by or on behalf of Arkose Labs in connection with the Services.

“**End Users**” means the individuals who use the Services on any of the Client Websites.

“**End User Information**” means the information supplied by the End User when they encounter the Services on the Client Websites and may include, without limitation, geolocation, device or browser identifiers (e.g. cookies and IP addresses) and other demographic information. End User Information may or may not include Personally Identifiable Information.

“**Feedback**” means any and all suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Client or any third party relating to any Arkose Labs Technology, including, but not limited to, general knowledge described more fully in Section 6.5.

“**Named Users**” means any employee, officer, agent, contractor, or professional adviser of Client that is designated by Client as having the right to access a Dashboard Account (defined below) and to use the Services on behalf of Client.

“**Personally Identifiable Information**” means information that can be used to identify, or may reasonably identify, a specific individual and includes such things as name, address, phone number, and email address.

“**Services**” means (a) access to the Arkose Labs API, Arkose Labs Data and the Documentation, and (b) any other services (including, without limitation, professional services) provided by Arkose Labs to Client as set forth in an applicable Order Form.

2. SERVICES.

2.1 Order Forms. Subject to this Agreement, Arkose Labs will use commercially reasonable efforts to provide the Services set forth on one or more written or electronic orders that reference this Agreement and has been executed by the parties (each, an “**Order Form**”). An Order Form will generally include an itemized list of the Services to be rendered, as well as the Subscription Term for each of the Services. Any change to the terms of this Agreement within an Order Form will apply only to the Services described therein. Termination of an Order Form will not terminate or affect any other Order Forms between the parties or this Agreement.

2.2 Client Account. As part of the registration process, Arkose Labs will provide Client with the quantity of Dashboard Accounts (defined below) identified on an Order Form. Client will identify an administrative username(s) and password for Client's Arkose Labs account through which Client may access its Arkose Labs dashboard as well as the public and private keys used to authenticate the Arkose Labs API (“**Dashboard Account**”). Client may reasonably request additional Dashboard Accounts to be created for Named Users subject to the terms of the applicable Order Form. Client may only use the Services in accordance with the quantities and limits set forth in this Agreement and the applicable Order Form; any excess usage shall be subject to Arkose Labs' then-current fees for the applicable services or portions thereof. Arkose Labs may deliver the Services directly, or indirectly using contractors or other third party vendors or service providers (collectively, “**Third Party Providers**”).

2.3 Service Availability. Subject to Section 9.2 of this Agreement, Arkose will use commercially reasonable efforts to provide Services in accordance with the service availability terms set forth in Attachment 1.

2.4 Support Services. Arkose Labs will provide Client with one of three tiers of support services indicated on an Order Form and further set forth in the support service terms and automated abuse SLA set forth in Attachment 2.

2.5 Modifications. Arkose Labs reserves the right to modify the Services (in whole or in part) at any time, provided that Arkose Labs will not materially reduce the functionality of the Services without providing Client of at least thirty (30) days' notice thereof (unless such modification is required for Arkose Labs to comply with applicable law, rule or regulation).

2.6 Limitations. Arkose Labs will not be responsible or liable for any failure in the Services resulting from or attributable to (a) usage in excess of the Services or limits for which Client has ordered pursuant to an applicable Order Form, (b) Client's modification of Client's systems in a manner that changes the integration of the Services, (c) Client's products, services, negligence, acts or omissions, (d) scheduled maintenance, (e) Client Data, Client Websites or Client Content, (f) unauthorized access to the Dashboard Account, breach of firewalls, or other hacking by third parties, or (g) Client's delay in or failure to provide Client Data or Client Technology required hereunder.

2.7 Purchasing through Authorized Reseller and Digital Marketplaces. If Client purchases the Services through an Arkose Labs authorized reseller or Digital Marketplace, this Agreement will govern those Services. Client's payment obligations for the Services will be with the authorized reseller or Digital Marketplace, as applicable, not Arkose Labs. Client will have no direct fee payment obligations to Arkose Labs for those Services. However, in the event that Client fails to pay the Digital Marketplace for the Services, Arkose Labs retains the right to enforce Client's payment obligations and collect directly from Client. Any terms agreed to between Client and the authorized reseller or Digital Marketplace that are in addition to this Agreement are solely between Client and the authorized reseller or Digital Marketplace, as applicable. No agreement between Client and an authorized reseller or Digital Marketplace is binding on Arkose Labs or will have any force or effect with respect to the rights in, or the operation, use or provision of, the Services.

3. CLIENT DATA AND CLIENT TECHNOLOGY.

3.1. Client Data License. Client grants Arkose Labs a world-wide, non-exclusive, royalty-free, non-transferable (except in accordance with Section 14) license during the term of this Agreement to use, access, reproduce, copy and distribute Client Data in connection with the Services (e.g. to analyze and draw conclusions about the data and applicable services, and to produce reports to provide to Client related to the Services). Client represents and warrants that it owns all right, title and interest in and to the Client Data or otherwise has sufficient rights to the Client Data to permit its use as contemplated hereunder. Furthermore, Client grants Arkose Labs a non-exclusive, non-transferable, worldwide, royalty free license to use Client Technology to the extent necessary to provide the Service to Client and its End Users.

3.2 Client Websites. In order to receive the Services, Client must make the Client Websites available to receive and display the Services and to receive cookies from Arkose Labs and its Third Party Providers. Client grants Arkose Labs and such Third Party Providers the right during the Term (defined below) to place such cookies on the Client Websites and to access, index and cache requests made from the Client Websites to the Services, including by automated means in connection with Arkose Labs' provision of Services. On termination or expiration of this Agreement or the applicable Order Form, the right of access granted to Arkose Labs in accordance with this Section 3.2 shall cease.

3.3 Personal Data. Arkose Labs will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of End User Information, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of End User Information (other than by Client or End Users). The terms of the data processing addendum included in Attachment 3 ("**DPA**") are hereby incorporated by reference and shall apply to the extent End User Information includes Personal Data, as defined in the DPA. To the extent Personal Data from the European Economic Area (EEA), the United Kingdom and Switzerland are processed by Arkose Labs, the Standard Contractual Clauses shall apply, as further set forth in the DPA. For the purposes of the Standard Contractual Clauses, Client and its applicable Affiliates are each the data exporter, and Client's acceptance of this Agreement, and an applicable Affiliate's execution of an Order Form, shall be treated as its execution of the Standard Contractual Clauses and Appendices.

4. OTHER CLIENT OBLIGATIONS.

4.1 Cooperation. Client will cooperate with Arkose Labs in connection with the performance of this Agreement by making available such personnel, information and materials as may be reasonably required and taking such other actions as Arkose Labs may reasonably request. Client will also cooperate with Arkose Labs in establishing a password or other procedures for verifying that only Named Users have access to any administrative functions of the Services. Client shall ensure that any Client identification details used to access the Dashboard Account and the Services are kept secure and are not disclosed or transferred to any other person. Client will take reasonable steps to (a) ensure that Named Users are suitably trained on how to use the Services, (b) employ and implement the correct use and application of the Services in accordance with any manuals, Documentation or instructions supplied by Arkose Labs, and (c) comply with any other reasonable directions of Arkose Labs in relation to the use of the Services. Client agrees to install, incorporate and maintain the technology and software codes provided by Arkose Labs, including any updates, fixes or patches provided by Arkose Labs from time to time, on the Client Websites as reasonably necessary for Arkose Labs to provide the Services.

4.2 End Users. Client represents and warrants that it shall comply with all applicable laws, rules and regulations, including without limitation all applicable privacy laws, in relation to any and all Personally Identifiable Information that it collects from its End Users or which it otherwise collects in connection with its use of the Services. Client shall be solely responsible for all notice to and consents by End Users with respect to any cookies or tracking technology used by Client in connection with the Services. Client acknowledges and agrees that as a result of Client and End Users accessing and using the

Services, Arkose Labs will receive End User Information via the Services on the Client Website. Client is responsible for informing End Users that Arkose Labs and its Third Party Providers will receive the Personally Identifiable Information for use as contemplated hereunder.

4.3 Restrictions. Client shall not, and shall not permit any third party to, directly or indirectly (a) use any of Arkose Labs' Confidential Information (defined below) to create any service, software, documentation or data that is similar to or competes with any aspect of the Services, (b) disassemble, decompile, reverse engineer or use any other means to attempt to discover any source code or object code of the Services or any Arkose Labs Technology, or the underlying structure, ideas, algorithms or trade secrets therein (provided that reverse engineering is prohibited only to the extent such prohibition is not expressly prohibited by applicable statutory law), (c) use the Documentation for any reason other than in connection with the Services, (d) encumber, sublicense, transfer, rent, lease, time-share or use the Services in any service bureau arrangement or otherwise for the benefit of any third party, (e) copy, modify, distribute, manufacture, adapt, create derivative works of, translate, localize, port or otherwise modify any aspect of the Services, (f) remove or modify any proprietary marking or restrictive legends placed on the Services (g) introduce into the Services any software, virus, worm, "back door", Trojan horse or similar harmful code, (h) merge or interface any third party software (including source code or open source software) with the Services, (i) communicate directly with any Third Party Provider regarding Client's use of the Services, or (j) proxy, modify, obscure, hire or circumvent the identity, location or other identifiable information about any End User.

4.4 Account Security. Client will be responsible for maintaining the security of Client's Dashboard Account, including related passwords or other credentials, and for all uses of its Dashboard Account with or without Client's knowledge or consent, including the use of the Dashboard Account by any Named Users, personnel or other third parties who have accessed the Dashboard Account. Client agrees to promptly notify Arkose Labs if any username or password needs to be changed or deactivated. Arkose Labs is not responsible and will not be liable for any losses, damages, liabilities or expenses caused by any unauthorized use of the Dashboard Account.

4.5 API Usage. It is Client's responsibility to ensure it does not exceed the API transaction limit set forth in Client's Order Form unless otherwise expressly agreed to by Arkose Labs in such Order Form. Exceeding the applicable API transaction limit may result in throttling or suspension of Services by Arkose Labs.

4.6 API Key Restrictions. Client will restrict usage of each API Key to one path, domain or sub-domain in the aggregate. If Client wishes to use the Services across more than one domain or sub-domain in the aggregate, Client is required to purchase further API Keys.

5. CONFIDENTIALITY

5.1 Confidentiality. Each party (the "**Receiving Party**") understands that the other party (the "**Disclosing Party**") has disclosed or may disclose information relating to the Disclosing Party's business (hereinafter referred to as "**Confidential Information**" of the Disclosing Party). The Receiving Party agrees: (a) to take reasonable precautions to protect such Confidential Information, (b) not to use such Confidential Information except as necessary to perform its obligations or exercise its rights hereunder, and (c) not to divulge to any third person any such Confidential Information except to its employees, contractors and professional advisors (collectively, "**Representatives**") who (i) need to know such information for the Disclosing Party to perform its obligations or exercise its rights hereunder and (ii) are informed of the confidential nature of the information and are bound by confidentiality obligations consistent with those contained herein. The Receiving Party shall be responsible for any breaches of confidentiality by its Representatives. The Disclosing Party agrees that the foregoing shall not apply with respect to any information that the Receiving Party can document (1) is or becomes generally available to the public without fault of the Receiving Party or its Representatives, (2) was rightfully in its possession or known by it without restriction on disclosure prior to receipt from the Disclosing Party, (3) was rightfully disclosed to it without restriction on disclosure by a third party who does not have any confidentiality obligations, or (4) was independently developed without use of or reference to any Confidential Information of the Disclosing Party. In any event, Arkose Labs may use any data and information it collects relating to the Services for development, diagnostic and corrective purposes related to the Services.

5.2 Permitted Disclosures. If required by applicable law, rule or regulation, the Receiving Party may disclose Confidential Information of the Disclosing Party; however, the Receiving Party will give adequate prior notice of such disclosure to the Disclosing Party (to the extent legally permitted). The Receiving Party will reasonably cooperate with the Disclosing Party to permit the Disclosing Party to intervene and to request protective orders or other confidential treatment therefor. Both parties will have the right to disclose a copy of this Agreement to its legal, professional and financial advisors and potential investors or acquirers, subject to confidentiality obligations consistent with those herein, in connection with a bona fide due diligence inquiry for a potential financing, acquisition or similar transaction.

6. PROPRIETARY RIGHTS.

6.1 Client. Except for the limited rights and licenses expressly granted to Arkose Labs hereunder, no other license is granted and no other use is permitted. Client (and its licensors, where applicable) will retain all intellectual property rights in and to the Client Data, Client Content and Client Websites.

6.2 Arkose Labs. Except for the limited rights and licenses expressly granted to Client hereunder, no other license is granted and no other use is permitted. Arkose Labs (and its licensors) shall retain all rights, title and interests (including all intellectual property and proprietary rights) in and to the Arkose Labs Technology. Client will not copy, distribute, reproduce or use any Arkose Labs Technology except as expressly permitted under this Agreement. This Agreement is not a sale and does not convey to Client any rights of ownership in or related to any Arkose Labs Technology. Client agrees that Arkose Labs has no obligation to provide to Client any Arkose Labs Technology that is not specifically set forth on an applicable Order Form. Arkose Labs may, from time to time, provide Client with updates and improvements of the Services provided hereunder that Arkose Labs makes generally available to Arkose Labs' similar customers, in which case such updates and improvements shall also be referred to as the "**Services**".

6.3 Reports. Subject to the terms and conditions of this Agreement, all reports based specifically on Client Data shall be owned by Client, provided that Client shall only use such reports for Client's internal business use and shall not share any such reports with any other party without Arkose Labs' prior written consent. Furthermore, to the extent the reports contain any third party log data, subject to the terms and conditions of this Agreement, Arkose Labs hereby grants to Client a non-exclusive, worldwide, nontransferable, nonsublicensable license, during the Term of this Agreement, to use the "**Third Party Log**" feature included in the Services to ingest and use such data for Client's internal business purposes in understanding nature and frequency of attacks. Such Third Party Log data shall be considered Arkose Labs Data as used herein.

6.4 Feedback. All Feedback shall be owned by Arkose Labs and Client hereby assigns all right, title and interest in and to such Feedback to Arkose Labs.

6.5 General Knowledge. Notwithstanding anything herein to the contrary, Client agrees that Arkose Labs may calculate anonymized and/or aggregate statistics about the Client Data and use Client Data and information and materials derived therefrom, in connection with Arkose Labs' business and the operation, improvement and maintenance of the Services, including without limitation for sales, marketing, business development, product enhancement, and the provision of Services to Client, provided that Arkose Labs will not use such Client Data in any manner that discloses the identity of Client or its End Users. Furthermore, Client agrees that Arkose Labs is free to use (including for research purposes) and disclose anonymized and/or aggregate measures of Client's interaction with Arkose Labs Data, the Services, and all Arkose Labs Technology, and all usage and performance thereof, and to reuse all generalized knowledge, experience, know-how, works, and technologies (including ideas, concepts, processes, and techniques) related to or acquired during provision of the Services under this Agreement (including without limitation, that which it could have acquired performing the same or similar services for another customer), provided that Arkose Labs may not use or disclose such data and information in a way that discloses the identity of Client or its End Users.

7. PAYMENT OF FEES.

7.1 Fees. Client will pay Arkose Labs the Fees for the Services as set forth in the applicable Order Form. All Fees are in US Dollars.

7.2 Payment Terms. Unless otherwise set forth in an applicable Order Form, (a) Client will pay all applicable Subscription Fees in advance, prior to the beginning of each Subscription Term; (b) any monthly fees for Technical Service will be invoiced by Arkose Labs in arrears; and (c) Arkose Labs will bill all other Fees through an invoice, and full payment for invoices must be received by Arkose Labs thirty (30) days after the date of the invoice. The Subscription Fees, Implementation Fees and all additional fees related to the Services shall be the "**Fees**". In the event Client fails to pay any Fees when due, Arkose Labs may do one or more of the following: (i) charge interest on the amount owing at a rate of 1.5% per month, or the maximum rate permitted by law, whichever is lower; (ii) restrict or suspend the Services in accordance with Section 8.4 below or (iii) terminate this Agreement, in accordance with its terms. All Fees stated in the Order Form are exclusive of any local, state or federal withholding taxes or duties of any kind. Client will be responsible for, and will promptly pay, all taxes and duties of any kind (including, but not limited to sales, use and withholding taxes) associated with this Agreement or Client's use of the Services (except for taxes based on Arkose Labs' net income) such that Client will deliver the full amount of the Fees listed on the Order Form to Arkose Labs without any deduction or offset.

7.3 No Refunds. Except as expressly set forth in Sections 8.2(b), 9.2 and 10.3, or a termination of this Agreement by Client for Arkose Labs' uncured material breach in accordance with Section 8.2(a)(ii) herein, there shall be no refunds of any Fees paid hereunder.

8. TERMINATION.

8.1 Term. Subject to earlier termination as provided below, this Agreement shall commence on the Start Date of the first Order Form issued hereunder and shall continue in effect until terminated in accordance with this Agreement (the "**Term**").

8.2 Termination. The parties agree that: (a) either party may terminate this Agreement (i) upon written notice to the other party if there are no more outstanding Order Forms, (ii) upon thirty (30) days' notice (or ten (10) days in the case of nonpayment), if the other party materially breaches any of the terms or conditions of this Agreement and fails to cure such breach during the applicable notice period, or (iii) immediately upon written notice upon the institution by or against the other party of insolvency, receivership or bankruptcy proceedings, the other party's making an assignment for the benefit of creditors, or the other party's dissolution or ceasing to do business; and (b) Arkose Labs may also terminate this Agreement immediately upon notice to Client if Arkose Labs reasonably believes doing so is necessary to comply with its legal obligations or otherwise protect Arkose Labs' customers, users, partners or business, provided that in the event of a termination under the terms of this subclause (b), Arkose Labs shall provide Client with a pro-rated refund of Fees for Services not yet provided by the termination effective date.

8.3 Effect of Termination. Effect of Termination. Upon any termination or expiration of this Agreement, (a) all Client's Rights to use the Services shall immediately terminate, (b) Arkose Labs may, but is not obligated to, delete archived data, and (c) each party will return to the other party, or if return is impracticable destroy, the other party's Confidential Information, and copies thereof, in the receiving party's possession or control. All sections of this Agreement which by their nature should survive termination or expiration will survive termination, including, without limitation, accrued rights to payment, confidentiality obligations, warranty disclaimers, and limitations of liability.

8.4 Suspension. Arkose Labs may temporarily suspend (in part or in whole) the provision of the Services to Client if (a) Arkose Labs is required by applicable law, rule or regulation to do so, (b) Client has failed to pay any Fees when due, (c) a force majeure or other event outside of Arkose Labs' reasonable control occurs which affects or may affect Arkose Labs' ability to provide the Services, or (d) Client is in material breach of the Agreement.

9. WARRANTY AND DISCLAIMER.

9.1 General. Each party represents and warrants that (a) it is a duly organized and validly existing under the laws of the jurisdiction in which it is organized, (b) it has full power and authority to enter into this Agreement and to perform its obligations hereunder, (c) this Agreement is legally binding upon it and enforceable in accordance with its terms, and (d) the execution, delivery and performance of this Agreement does not and will not conflict with any agreement, instrument, judgment or understanding, oral or written, to which it is a party or by which it may be bound.

9.2 Arkose Labs. Arkose Labs warrants to Client that the Services will be provided in a professional and workmanlike manner and in material conformance with the applicable Documentation. Arkose Labs' sole obligation and Client's exclusive remedy in respect of any breach of this warranty is to, at Arkose Labs' discretion, replace or repair the nonconforming portion of the Service to bring it into conformance, or, if in Arkose Labs' sole discretion it determines that repair or replacement is impracticable, terminate this Agreement or the applicable Order Form, and provide Client with a pro-rated refund of any Fees prepaid for use of the Services not completed by the termination effective date.

9.3 Client. Client represents and warrants that (a) it is the owner of each Client Website (or is legally authorized to act on behalf of the owner of each Client Website for the purposes of this Agreement) and that is has all rights necessary to grant the rights set forth in this Agreement, including without limitation to place the Services on each Client Website and to permit Arkose Labs and its Third Party Providers to collect and use End User Information, (b) it will comply with all applicable laws, rules and regulations, including without limitation by ensuring that any Personally Identifiable Information collected via the Services or otherwise provided to Arkose Labs hereunder is collected lawfully, (c) it is the owner of, or otherwise has sufficient rights to, the Client Content on each Client Website, and (d) the Client Websites, Client Data, Client Content and its use of the Services do not violate the privacy rights, publicity rights, copyright rights, contract rights, intellectual property rights, or any other rights of any person.

9.4 Disclaimers. THE SERVICES AND ALL ARKOSE LABS TECHNOLOGY ARE PROVIDED "**AS IS**". ARKOSE LABS DOES NOT WARRANT THAT THE SERVICES OR ARKOSE LABS TECHNOLOGY WILL MEET CLIENT'S REQUIREMENTS OR RESULT IN ANY OUTCOME, OR THAT THEIR OPERATION WILL BE UNINTERRUPTED OR ERROR-FREE. TO THE FULLEST EXTENT PERMITTED BY LAW, ARKOSE LABS HEREBY DISCLAIMS (FOR ITSELF AND ITS SUPPLIERS) ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, WITH RESPECT TO THE SERVICES OR THE ARKOSE LABS TECHNOLOGY INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, QUIET ENJOYMENT, INTEGRATION, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE AND ALL WARRANTIES ARISING FROM ANY COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE.

10. INDEMNIFICATION.

10.1 Arkose Labs. Subject to Section 10.4 and 10.5, Arkose Labs shall indemnify, defend and hold Client and its officers, directors, employees and agents harmless from all damages, losses, liabilities or expenses (including without limitation reasonable attorneys' fees) arising from a third party claim that the Services infringe any United States intellectual property right.

10.2 Client. Subject to Section 10.5, Client shall indemnify, defend, and hold Arkose Labs and its officers, directors, employees and agents harmless from any third party damages, losses, liabilities or expenses (including without limitation reasonable attorneys' fees) arising from a third party claim arising from (a) the gross negligence or willful misconduct of the Client or anyone who accesses the Client's Account, (b) the Client Data, End User Information or unauthorized End User Information, Client Content or Client Website, or (c) any breach of its representations, warranties or obligations set forth herein.

10.3 Infringement. If the Services or any Arkose Labs Technology becomes or, in Arkose Labs' opinion, is likely to become, the subject of any infringement claim or injunction preventing its use as contemplated herein, Arkose Labs may, at its option (a) obtain for Client the right to continue using the Services or (b) replace or modify the infringing portions of the Service so that it becomes non-infringing without substantially compromising its principal functions. If (a) and (b) are not reasonably available to Arkose Labs, then it may (c) terminate this Agreement upon written notice to Client and refund to Client any Fees for the Services that were prepaid for the then current term, pro-rated for the remainder thereof.

10.4 Exclusions. Arkose Labs shall have no liability or obligation hereunder with respect to any claim based upon (a) Client Content, Client Data, End User Information or unauthorized End User Information or Client Websites, (b) use of the Services in an application or environment, or with products, processes or materials, for which it they were not designed or contemplated, (c) modifications, alterations, combinations or enhancements not created by or for Arkose Labs, (d) any portion of the Services that implements Client's requirements, (e) Client's continuing allegedly infringing activity after being notified thereof or its continuing use of any version after being provided modifications that would have avoided the alleged infringement, (f) use of the Services not strictly in accordance with this Agreement, or (g) any intellectual property right in which Client or any of its affiliates has an interest.

10.5 Procedure. Any claim for indemnification hereunder requires that (a) the indemnified party provides prompt written notice of the claim and reasonable cooperation, information, and assistance in connection therewith (provided that a failure or delay in providing such notice shall not relieve the indemnifying party of its obligations hereunder except to the extent it is materially prejudiced thereby), and (b) the indemnifying party shall have sole control and authority to defend, settle or compromise such claim. The indemnifying party shall not make any settlement that requires a materially adverse act or admission by the indemnified party without the indemnified party's written consent (such consent not to be unreasonably delayed, conditioned or withheld).

10.6 Entire Liability. This Section 10 states the entire liability of Arkose Labs, and Client's exclusive remedy, with respect to any actual or alleged violation of intellectual property rights by the Services, any part thereof or its use or operation.

11. PUBLICITY. Client agrees that Arkose Labs may make reference to Client in marketing and public relations materials, including a press release announcing Client as a customer. Client hereby grants Arkose Labs a perpetual, nonexclusive, worldwide license to use and display Client's trademarks, trade names and logos in connection with the foregoing. This Section 11 will survive the termination or expiry of this Agreement.

12. **LIMITATION OF LIABILITY.** IN NO EVENT WILL ARKOSE LABS BE LIABLE FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR IN ANY WAY CONNECTED WITH THE USE OF THE SERVICES OR ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT, THE DELAY OR INABILITY TO USE THE SERVICES OR ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT OR OTHERWISE ARISING FROM THIS AGREEMENT, OR FOR ANY LOSS OF REVENUE OR ANTICIPATED PROFITS OR LOST BUSINESS OR LOST SALES, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR OTHERWISE, EVEN IF ARKOSE LABS HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. THE TOTAL LIABILITY OF ARKOSE LABS, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), OR OTHERWISE, WILL NOT EXCEED THE FEES PAID TO ARKOSE LABS HEREUNDER IN THE TWELVE (12) MONTH PERIOD ENDING ON THE DATE THAT A CLAIM OR DEMAND IS FIRST ASSERTED. THE FOREGOING LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

13. **COMPLIANCE WITH LAWS.** Client will use the Services in accordance with this Agreement and in compliance with all applicable laws and regulations (including but not limited to any European privacy laws, intellectual property, consumer and child protection, obscenity or defamation law). The Services are subject to the trade laws and regulations of the United States and other countries, including the Export Administration Regulations (EAR, 15 CFR Part 730 et seq.) and the sanctions programs administered by the Office of Foreign Assets Control (OFAC, 31 CFR Part 500). Client will not import, export, re-export, transfer or otherwise use the Services in violation of these laws and regulations. By using the Services, Client represents and warrants that Client is not located in any embargoed country or on any restricted list in violation of the aforementioned laws and regulations. Client will not engage in activity that would cause Arkose Labs to be violation of these laws and regulations, and will indemnify Arkose Labs for any fines, penalties or other liabilities incurred by Arkose Labs for Client's failure to comply with this provision.

14. **MISCELLANEOUS.**

This Agreement is the entire agreement between Arkose Labs and Client regarding Client's use of Services and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. The parties agree that any term or condition stated in Client's purchase order or in any other Client order documentation (excluding Order Forms) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the applicable Order Form, (2) this Agreement, and (3) the Documentation. If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable. This Agreement is not assignable, transferable or sublicensable by Client except with Arkose Labs' prior written consent. All waivers and modifications to this Agreement must be in a writing signed by both parties, except as otherwise provided herein. No agency, partnership, joint venture, or employment is created as a result of this Agreement and Client does not have any authority of any kind to bind Arkose Labs in any respect whatsoever. In any action or proceeding to enforce rights under this Agreement, the prevailing party will be entitled to recover costs and attorneys' fees. All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested. This Agreement shall be governed by the laws of the State of California without regard to its conflict of laws provisions. Exclusive jurisdiction and venue for any action arising under this Agreement shall be in the federal and state courts located in San Francisco, and both parties hereby consent to such jurisdiction and venue for this purpose. Arkose Labs may revise these Master Service Terms and Conditions at any time by posting such revised version at https://arkoselabs.com/legal/msa (https://arkoselabs.com/legal/msa), upon which such revised Master Service Terms and Conditions will supersede and replace any earlier version. Any provision of services to Client after such revision will be deemed to be an acceptance by Client of the revised version.

UNDERSTOOD AND AGREED:

ARKOSE LABS, INC.

Signature:____

Name:____

Title:____

CLIENT:

Signature: ____

Name:____

Title:____

Date:____ Date:____

ATTACHMENT 1
UPTIME SLA

1. DEFINITIONS

"Monthly Uptime Percentage" is calculated by subtracting from 100% the percentage of minutes during the month in which the Services were in a state of "Unavailable". Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any SLA Exclusion (defined below).

"Service Credit" means a dollar credit, calculated as set forth below, that Arkose Labs may credit back to an eligible account.

"Unavailable" means that while using the most up-to-date Arkose Labs API and a fully functioning Internet connection, an API response from the Arkose Labs service exceeds 5 seconds.

2. UPTIME SERVICE LEVEL AGREEMENT (SLA)

Arkose Labs will use commercially reasonable efforts to make Arkose Labs available with a Monthly Uptime Percentage of at least 99.9% during each month of usage (the "**Service Commitment**"). In the event Arkose Labs does not meet the Service Commitment, Client will be eligible to receive a Service Credit as further described below.

3. SERVICE COMMITMENT & SERVICE CREDITS

Service Credits are calculated as a percentage of the charges paid by Client for the month in which the unavailability occurred in accordance with the schedule below:

Monthly Uptime Percentage	Service Credit
Below 99.9% but at least 98.0%	Seven (7) days of Service credited to Client's account
Below 98.0% but at least 95.0%	Fourteen (14) days of Service credited to Client's account
Below 95.0%	Thirty (30) days of Service credited to Client's account

Arkose Labs will apply Service Credits against future payments otherwise due from Client. Service Credits will not entitle Client to any refund or other payment from Arkose Labs. Client's sole and exclusive remedy for any unavailability, non-performance, or other failure to provide Arkose Labs Service is the receipt of a Service Credit (if eligible) in accordance with the terms and conditions of this Uptime SLA.

4. CREDIT REQUEST AND PAYMENT PROCEDURES

To receive a Service Credit, please submit a claim by emailing support@arkoselabs.com (about:blank). To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

- the words "SLA Credit Request" in the subject line;
- the dates and times of the claimed outage;
- the affected Public Keys and sites; and
- Client request logs that document the errors and corroborate Client's claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage of such request is confirmed by us and is less than the Service Commitment, then Arkose Labs will issue the Service Credit to Client within one billing cycle following the month in which Client's request is submitted.

5. SLA EXCLUSIONS

The Service Commitment does not apply to any unavailability, suspension or termination of the Services: (i) that result from a termination of service as described in Agreement or any Order Form; (ii) caused by factors outside of Arkose Labs' reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Arkose Labs; (iii) that result from any actions or inactions of Client or any third party; (iv) that result from Client's equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within Arkose Labs' direct control); (v) that result from any maintenance as provided for pursuant to the Agreement; or (vii) arising from suspension or termination of Client's right to use Arkose Labs in accordance with the Agreement (collectively, the "**SLA Exclusions**"). If availability is impacted by factors other than those used in Arkose Labs' Monthly Uptime Percentage calculation, then Arkose Labs may issue a Service Credit considering such factors at its discretion.

ATTACHMENT 2
SUPPORT SERVICES TERMS & AUTOMATED ABUSE SLA

1. GENERAL DEFINITIONS

"Acid Test" means Arkose Labs' proprietary method of seeking to Remediate an instance of Automated Abuse, which may involve the use of one or more Enforcement Challenges or other enforcement mechanisms. For the avoidance of doubt, Arkose Labs shall solely determine the means, scope and manner in which the Acid Test is administered and managed within any Customer Page.

"API" means the Arkose Labs application programming interface and any related scripts, widgets, embeddable snippets, and other tools provided therewith.

"API Key" means a pathway through which Customer interacts with the API.

"API Request" means each time a Customer Page is loaded by an End User.

"API Usage" means Customer's consumption of API Requests over the Term.

"Attack Incident" means a suspected, unique, automated attack by a third party on a Customer Page.

"Automated Abuse" means a confirmed Attack Incident limited to Credential Stuffing coming from an unauthorized, non-human End User.

"Business Day" means any day except any Saturday, any Sunday, any day which is a federal legal holiday in the United States or any day on which banking institutions in the State of New York are authorized or required by law or other governmental action to close.

"Change" means a change to Customer's account configuration.

"Change Management Process" means the combination of (i) an associated approved Change ticket within the Arkose Labs ticketing system and (ii) approval of the Change from one of Customer's authorized contacts.

"Credential Stuffing" means the automated injection of breached username/password pairs by an unauthorized third party in order to gain unauthorized access to Customer's network.

"Custom Runbook" means a runbook customized to Customer's unique account environment, processes, and escalation rules, created and maintained by Arkose Labs, subject to Customer input and approval.

"Customer" means the named customer on the Order Form.

"Customer Account Report" means a Quarterly Business Review, Monthly Security Review, Monthly Threat Advisory Report or Weekly Operational Review, as applicable.

"Customer Page" means the user interface containing the Enforcement Challenge on any of Customer's web or native mobile applications.

"Customer Portal" means the online account dashboard made available to Customer at https://support.arkoselabs.com.

“Customer Pre-Production” means the point at which Arkose Labs has concluded the initial implementation of the Security Services on Contract with Customer.

“Customer Request” means a written request for support from Customer to Arkose Labs via an approved electronic communication channel within Customer’s Service Tier.

“Dedicated Security Expert” means a Security Expert who acts as a single point of contact to manage Customer’s business priorities and communications with respect to the Security Services on Contract. The Dedicated Security Expert coordinates Customer’s deliverables, works closely with Customer’s team to understand Customer’s security profile and business priorities, provides contextual recommendations and coordinates the implementation of changes to Customer’s security configurations, as needed.

“End User” means any individual or entity that accesses the Enforcement Challenge through a Customer Page.

“Enforcement Challenge” means the challenge component of the Security Services on Contract that is intended to prevent Automated Abuse.

“HealthChecks” means programmatic checks by Arkose Labs’ technical team on Customer’s account to compare account configurations against established best practices and remedy any material gaps that are discovered.

“Incident Analysis Report” means a written analysis of an Attack Incident after its occurrence, including any actions taken and any recommendations after the Attack Incident has been resolved.

“Initial Response Time” means the duration of time after which a Customer Request is received by Arkose Labs that Arkose Labs will respond to the Customer. Notwithstanding anything to the contrary herein, Customer acknowledges that all Customer Requests reported to Arkose Labs via email or Slack will be treated by Arkose Labs as P3 issues and be subject to corresponding Initial Response Times.

“Monthly Security Review” means a monthly summary of the security activity, overall security posture, professional services fulfillment, and project updates relating to Customer’s account.

“Monthly Threat Advisory Report” means a monthly summary of the latest threat advisories across the Arkose Labs platform with insights from our threat intelligence research experts.

“Order Form” means the purchase order and primary service agreement between Customer and Arkose Labs for security and support services.

“Primary Security Analyst” means a dedicated member of SOC as available during Standard Business Hours and backed up by pooled SOC resources when not available.

“Priority Level” means one of three defined priority levels, related impacts and classifications for Customer Requests that apply to each Service Tier and their underlying support service components, as solely determined in each case by Arkose Labs:

Priority Level	Impact	Classification	Arkose Staff Availability
P1	Critical	The Security Services on Contract is down and the customer’s users cannot be verified. *Example: The Enforcement Challenge fails to load, preventing users from logging into your website or application.*	The appropriate Arkose Labs staff will be alerted and respond day or night, within the applicable Initial Response Time.

P2	Major	Important functions of the Security Services on Contract are impaired or degraded. The issue is important to resolve but not so critical that it has to be resolved immediately. *Example: Your website or application is experiencing a wave of abuse from suspected automated traffic, but authentic users continue to be able to reach your service.*	The appropriate Arkose Labs staff will be alerted and respond day or night, within the applicable Initial Response Time.
P3	Low	Non-critical functions of the Security Services on Contract are behaving abnormally. Response time is less critical. *Example: Your users are receiving an unexpectedly large number of Enforcement Challenges.*	The appropriate Arkose Labs staff will be alerted and respond only during Standard Business Hours, within the applicable Initial Response Time.

“Quarterly Business Review” means an executive-level review that includes items such as industry trends and service roadmap insights. Among other things, the QBR seeks to highlight the value provided by Arkose Labs to Customer, and includes summary information relating to HealthChecks on Customer’s account.

“Remediate” or “Remediation” means the cessation or material reduction of traffic attributable to a single instance of Automated Abuse within the applicable SLA Period.

“Standard Business Hours” means 9:00 a.m. to 8:00 p.m. in the Eastern Time Zone of the United States on any Business Day.

“Security Expert” means a member of Arkose Labs’ staff having knowledge of the Security Services on Contract.

“Security Services on Contract” means the security services Arkose Labs provides Customer (excluding any support services described herein) pursuant to the then-current Order Form.

“SLA Period” means a duration of time starting when Arkose Labs begins running the Acid Test with respect to any specific instance of Automated Abuse.

“SOC” means Arkose Lab’s Security Operations Center.

“Technical Support Team” means Arkose Labs’ pooled team of technical support specialists.

“Term” means the stated term of the Security Services on Contract within the Order Form.

“Training Cycle” means a deep analysis of the End User and Enforcement Challenge activity on the Customer Pages of Customer and Arkose Labs’ subsequent tuning of the Security Services on Contract to better optimize performance on Customer’s account.

“Weekly Operational Review” means a summary of action plans for resolving any short-term problems and opportunities for continuous improvement on Customer’s account, delivered to Customer each week except the weeks that Customer receives a QBR or MSR.

2. **SUPPORT SERVICE TIERS:**

Arkose Labs provides three tiers of support services for its customers as follows (each, a “Service Tier”):

- Tier 1: Starter Services;
- Tier 2: Essential Services; and

- Tier 3: Managed Security Services.

Customer's selected Service Tier will be indicated on the order form for Security Services on Contract. If no Service Tier is indicated on the Customer's order form, Customer shall by default receive Starter Services. If at any time during the Term Customer desires to upgrade its Service Tier, an Order Form amendment will need to be executed by Customer and Arkose Labs.

Regardless of which Service Tier Customer elects, Arkose Labs will not make a Change unless the Change Management Process has been met (except for Tier 3 Customers electing to create Custom Runbooks, as described below). With respect to any Change, Customer acknowledges that Arkose Labs is not responsible for confirming Customer's internal approval of the Change all requested Changes that adhere to the Change Management Process will be deemed by Customer and Arkose Labs to have received such internal approval from Customer.

There is a one-time per API Key implementation fee that covers costs associated with configuring the default requirements specific to Customer's business, including security, user experience and branding. This fee is earned once Arkose Labs has completed Customer Pre-Production.

Moreover, upon Customer's request, Arkose Labs may (i) support a remote meeting with Customer to discuss the contents of any Customer Account Report available to Customer in Customer's Service Tier and (ii) amend the content included in any Customer Account Report available to Customer in Customer's Service Tier, in each case at Arkose Labs' sole discretion.

Any support service not explicitly described in the applicable Service Tier is subject to additional fee if provided to Customer.

Descriptions of the specific support services available in each of the three (3) Service Tiers follow:

Tier 1: Starter Services

Starter Services reflects the base level Service Tier, which Customers will receive by default.

Starter Services include Tier 1 access to **General Support** and **Security Advisory Support**, as described below.

Tier 1 General Support

The Technical Support Team will respond to Tier 1 Customer Requests related to the development and integration of Arkose Labs' solutions, non-critical bugs, or feature requests.

Each Tier 1 Customer Request will be classified, prioritized, and escalated as the Technical Support Team in its sole discretion deems appropriate in accordance with the applicable Priority Level as follows:

- Initial Response Times for Tier 1 Customer Requests:

- P1 Issues: Four (4) hours or less
- P2 Issues: Eight (8) hours or less
- P3 Issues: Three (3) Business Days or less

Tier 1 Customers may submit Customer Requests to Arkose Labs through either of two channels:

1. The Customer Portal, accessible at https://support.arkoselabs.com (https://support.arkoselabs.com/); or
2. Via e-mail*, to support@arkoselabs.com (mailto:support@arkoselabs.com).

*Any Tier 1 Customer Requests submitted via email shall be given a Priority Level of P3 regardless of subject matter.

Tier 1 Security Advisory Support

Tier 1 Customers will further receive access to:

- Quarterly Business Reviews.

Tier 2: Essential Services

Essential Services reflects the mid-level Service Tier and additionally provides a customer with prioritized access to Arkose Labs' Security Experts for advisory support as well as direct access to SOC for reactive support for Customer's Security Services on Contract.

Essential Services includes Tier 2 access to **General Support** and **Security Advisory Support**, as described below.

Tier 2 General Support

The Technical Support Team will respond to Tier 2 Customer Requests related to the development and integration of Arkose Labs' solutions, non-critical bugs, or feature requests.

Each Tier 2 Customer Request will be classified, prioritized, and escalated as the Technical Support Team in its sole discretion deems appropriate in accordance with the applicable Priority Level as follows:

- Initial Response Times for Tier 2 Customer Requests:

- P1 Issues: Two (2) hours or less
- P2 Issues: Four (4) hours or less
- P3 Issues: Two (2) Business Days or less

Tier 2 Customers may submit Customer Requests to Arkose Labs through any of three channels:

1. The Customer Portal, accessible at https://support.arkoselabs.com (https://support.arkoselabs.com/); or
2. Via e-mail*, to support@arkoselabs.com (mailto:support@arkoselabs.com); or
3. Via Slack*, on a dedicated channel between Arkose Labs and Customer.

*Any Tier 2 Customer Requests submitted via email or Slack shall be given a Priority Level of P3 regardless of subject matter.

Tier 2 Customers will receive an Incident Analysis Report in connection with any Attack Incident, as needed.

Tier 2 Security Advisory Support

Tier 2 Customers will further receive access to:

- A Dedicated Security Expert;

- Quarterly Business Reviews; and:

- Monthly Security Reviews.

Tier 3: Managed Security Services

Managed Security Services reflects the top-level Service Tier and is for Customers seeking around-the-clock monitoring, management and response to advanced threats.

Managed Security Services includes Tier 3 access to **General Support, Security Advisory Support**, **Customer Runbook**, **Proactive Risk Management**, and **Limited Warranty Eligibility**, as described below.

Tier 3 General Support

The Technical Support Team will respond to Tier 3 Customer Requests related to the development and integration of Arkose Labs' solutions, non-critical bugs, or feature requests.

Each Tier 3 Customer Request will be classified, prioritized, and escalated as the Technical Support Team in its sole discretion deems appropriate in accordance with the applicable Priority Level as follows:

- Initial Response Times for Tier 3 Customer Requests:

- P1 Issues: One (1) hour or less
- P2 Issues: Two (2) hours or less
- P3 Issues: One (1) Business Day or less

Tier 3 Customers may submit Customer Requests to Arkose Labs through either of three channels:

1. The Customer Portal, accessible at https://support.arkoselabs.com (https://support.arkoselabs.com/); or
2. Via e-mail*, to support@arkoselabs.com (mailto:support@arkoselabs.com); or
3. Via Slack*, on a dedicated channel between Arkose Labs and Customer.

*Any Tier 3 Customer Requests submitted via email or Slack shall be given a Priority Level of P3 regardless of subject matter.

Tier 3 Customers will receive an Incident Analysis Report in connection with any Attack Incident, as needed, and be assigned a Primary Security Analyst.

Tier 3 Security Advisory Support

Tier 3 Customers will further receive access to:

- A Dedicated Security Expert;
- Quarterly Business Reviews;
- Monthly Security Reviews;
- Monthly Threat Advisory Reports; and
- Weekly Operational Reviews.

Tier 3 Custom Runbook

Tier 3 Customers are eligible to receive a Custom Runbook as follows:

- If Customer elects to receive a Custom Runbook, Customer shall permit SOC to review monitoring alerts and, as deemed necessary by SOC pursuant to the agreed-to protocols set forth in the Custom Runbook, initiate and manage changes to Customer's configuration in order to mitigate attacks. Unless otherwise specified in the Custom Runbook, Arkose Labs will not seek Customer's consent or otherwise notify Customer before implementing changes deemed necessary to mitigate attacks.
- If Customer elects not to receive a Custom Runbook, Arkose Labs will not change Customer's configuration unless the change adheres to the Change Management Process.

Tier 3 Proactive Risk Management

Tier 3 Customers further receive Proactive Risk Management Support which includes:

- Proactive monitoring and alerting of designated Arkose Labs detection and enforcement signatures (e.g. a recognizable digital signature from potential bad actors).
- Proactive detection & notification of unusual traffic which, once classified by Arkose Labs, shall be assigned a ticket within the Arkose Labs ticketing system.
- Attack Incident monitoring which provides near real-time alerting originating from available SOC notifications.

Tier 3 Limited Warranty Eligibility

As part of the Managed Security Services subscription, Tier 3 Customers are also eligible to receive additional protection from Automated Abuse under Arkose Labs' Managed Security Services Limited Warranty. The Managed Security Services Limited Warranty is only available to Tier 3 Customers, comes at no additional cost to the Managed Security Services subscription, and is conditioned on such Tier 3 Customer's agreement to the comprehensive terms and conditions of the Managed Security Services Limited Warranty.

3. ADDITIONAL SUPPORT SERVICES

The following support services are available to Customers on an a la carte basis (i.e. individually for an additional fee as applicable) regardless of which Service Tier they select:

Custom Dashboard:

The default dashboard reports high level metrics such as the number of End Users who load, attempt and solve the applicable Enforcement Challenges. The dashboard within the Customer Portal may be customized so Customer can view any important details or metrics. This can also include End User information Customer provides to Arkose Labs, for example user IDs or other values to break out abuse and conversion metrics to align with your internal systems. The Custom Dashboard will be considered delivered, in full, when it is made available in the Customer Portal.

Custom Development:**

This is development by Arkose Labs specifically for Customer which adds a new feature or functionality to the Arkose Labs Platform as requested by Customer. An example of this might be development done to support the Enforcement Challenge within a video game console. A statement of work is created when Customer chooses to move forward with Custom Development to fully outline the scope of the development. A custom developed feature will remain in this category until it has been formally incorporated into Arkose Labs' product development roadmap for wider availability across the customer base.

Custom Security Branding:**

Arkose Labs can incorporate Customer's logo and/or branding within the Enforcement Challenge. To ensure security is maintained, Customer will work with Arkose Labs' in-house 3D modelling team to create a representation that meets minimum security standards. Under high abuse scenarios, Arkose Labs may dynamically shift to alternative images temporarily. Any Custom Security Branding associated with Customer's account will be delivered and maintained through the Term.

Custom User Interface:**

This includes Customer specific changes to the design and/or display of the Enforcement Challenge beyond the scope of what is customizable within the standard Enforcement Challenge template. Examples of these types of changes can include: sizing of the actual challenge, moving buttons / images to non-standard placements not driven by compatibility requirements, etc. A statement of work is created when a customer chooses to move forward with a custom UI to fully outline the scope of the customization.

Training Cycles:

Training Cycles can result in changes such as:

- Enhancing resistance to machine learning by changing image types or game formats;
- Enabling features and customize settings to hinder sweatshops (organized paying of humans to solve the Enforcement Challenge for abusive purposes), such as with timers, curses, and telemetry detection; and
- Improving legitimate user experience and conversion, such as letting users through without seeing any sign of the Enforcement Challenge, or users see versions of the Enforcement Challenge which are very easy to solve.

For example, after a 30-day cycle, we may report to you that automated attacks were detected by telemetry, so the system adapted to it and prevented it. In the following 30-day cycle, we may report that telemetry detected that the attackers switched to sweatshop tactics, so the system adapted to defend against that (while maintaining defence against prior machine attacks).

Even when things are in an ideal state on your own app/site, Arkose Labs telemetry is always plugged into activity across the whole Arkose Labs network, so continual adjustments are made to your service as a defensive measure from usage and trends from all of our other customers.

Training Cycles are done on a per API Key basis.

**Customer's purchase and/or use of these additional support services may impact its ability to receive (i) the benefit of Arkose Labs' SLA Guarantee (see below) and (ii) coverage under the Managed Security Services Limited Warranty, if available to Customer.

4. <u>AUTOMATED ABUSE SLA PERIODS</u>

Arkose Labs SLA Guarantee

Customers across all Service Tiers receive the benefit of Arkose Labs' SLA Guarantee on Automated Abuse, which means Arkose Labs guarantees that it will Remediate any unique instance of Automated Abuse within the SLA Period corresponding to Customer's applicable Service Tier, as further set forth in the table below and subject to the conditions that follow (the "SLA Guarantee"):

SLA Periods for Automated Abuse Remediation***

Tier 1 (Starter Services) Customers	96 hours or less
Tier 2 (Essential Services) Customers	72 hours or less
Tier 3 (Managed Security Services) Customers	48 hours or less

***Customer acknowledges that, regardless of Service Tier, (i) Remediation may be delayed where a code change and/or deployment is necessary and (ii) the SLA Guarantee only applies to Automated Abuse which can undergo the Acid Test process (e.g. this would exclude certain modes of the Enforcement Challenge, such as Audio accessibility).

Arkose Labs's obligations under the SLA Guarantee are subject to and conditioned upon (i) Customer maintaining the appropriate configuration settings on the applicable Customer Page, the appropriateness of which shall be solely determined by Arkose Labs, (ii) Customer cooperating fully with Arkose Labs' instructions in deploying and administering the applicable Acid Test to Remediate the Automated Abuse, and (iii) Customer having the latest version of Arkose Labs' API running, in order for the SLA Guarantee to apply.

If Arkose Labs does not meet the SLA Guarantee and Customer is otherwise up to date and in compliance with its obligations under the applicable Order Form, Customer's sole remedy under this SLA Guarantee will be to terminate the applicable Order Form with no further obligations to Arkose Labs.

* * *

ATTACHMENT 3
DATA PROCESSING ADDENDUM

THIS DATA PROCESSING ADDENDUM ("**ADDENDUM**") SHALL APPLY TO THE EXTENT THAT YOU OR THE ENTITY YOU REPRESENT ("**CLIENT**") PROVIDE ARKOSE LABS, INC. ("**ARKOSE LABS**" OR "**COMPANY**") WITH ANY PERSONAL DATA (DEFINED BELOW). CLIENT REPRESENTS AND AGREES THAT IT ACCEPTS THE TERMS IN THIS ADDENDUM, WHICH SUPPLEMENT ANY ORDER FORM BETWEEN CLIENT AND ARKOSE LABS' AS WELL AS THE AGREEMENT TO WHICH THIS ADDENDUM IS ATTACHED OR REFERENCED (COLLECTIVELY, THE "**AGREEMENT**"). IF YOU ARE ACCESSING THE SERVICES ON BEHALF OF YOUR EMPLOYER, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO AGREE TO THIS ADDENDUM ON YOUR EMPLOYER'S BEHALF AND THE RIGHT TO BIND YOUR EMPLOYER THERETO. IF CLIENT DOES NOT UNCONDITIONALLY AGREE TO ALL THE TERMS AND CONDITIONS OF THIS ADDENDUM, CLIENT SHALL HAVE NO RIGHT TO USE ARKOSE LABS' SERVICES. This Addendum incorporates the terms of the Agreement, and any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control.

1. Definations

1.1 "Affiliate" means (i) an entity of which a party directly or indirectly owns fifty percent (50%) or more of the stock or other equity interest, (ii) an entity that owns at least fifty percent (50%) or more of the stock or other equity interest of a party, or (iii) an entity which is under common control with a party by having at least fifty percent (50%) or more of the stock or other equity interest of such entity and a party owned by the same person, but such entity shall only be deemed to be an Affiliate so long as such ownership exists.

1.2 "Anonymous Data" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person.

1.3 "Authorized Employee" means an employee of Company who has a need to know or otherwise access Personal Data to enable Company to perform their obligations under this Addendum or the Agreement.

1.4 "Authorized Sub-Processor" means a third-party who has a need to know or otherwise access Personal Data to enable Company to perform its obligations under this Addendum or the Agreement, and who is either (1) listed at the sub-processor on Exhibit C hereto, or (2) authorized by Client to do so under Section 4.2 of this Addendum.

1.5 "Client Account Data" means personal data that relates to Client's relationship with Company, including the names or contact information of individuals authorized by Client to access Client's account and billing information of individuals that Client has associated with its account. Client Account Data also includes any data Company may need to collect for the purpose of managing its relationship with Client, identity verification, or as otherwise required by applicable laws and regulations.

1.6 "Client Usage Data" means Service usage data collected and processed by Company in connection with the provision of the Services, including without limitation data used to identify the source and destination of a communication, activity logs, and data used to optimize and maintain performance of the Services, and to investigate and prevent system abuse.

1.7 "Data Protection Laws" means all applicable data privacy, data protection, and cybersecurity laws, rules and regulations to which the Personal Data are subject. "Data Protection Laws" shall include, but not be limited to: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act ("**CCPA**"); (ii) and the Virginia Consumer Data Protection Act (Va. Code §§ 59.1-575 et seq.) ("**VCDPA**"); (iii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**"); (iv) the Swiss Federal Act on Data Protection; (v) the EU GDPR as it forms part of the law of England and Wales by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") (together with the EU GDPR, the "**GDPR**"); (vi) the Swiss Federal Act of Data Protection (vii) the UK Data Protection Act 2018; and (viii) the Privacy and Electronic Communications (EC Directive) Regulations 2003; in each case, as updated, amended or replaced from time to time.

1.8 "Data Subject" means an identified or identifiable person to whom Personal Data relates.

1.9 "EU SCCs" means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time), as modified by Section 6.2 of this Addendum.

1.10 "ex-EEA Transfer" means the transfer of Personal Data, which is processed in accordance with the GDPR, from the Data Exporter to the Data Importer (or its premises) outside the European Economic Area (the "**EEA**"), and such transfer is not governed by an adequacy decision made by the European Commission in accordance with the relevant provisions of the GDPR.

1.11 "ex-UK Transfer" means the transfer of Personal Data covered by Chapter V of the UK GDPR, which is processed in accordance with the UK GDPR and the Data Protection Act 2018, from the Data Exporter to the Data Importer (or its premises) outside the United Kingdom (the "**UK**"), and such transfer is not governed by an adequacy decision made by the Secretary of State in accordance with the relevant provisions of the UK GDPR and the Data Protection Act 2018.

1.12 "Instruction" means a direction, either in writing, in textual form (e.g., by e-mail) or by using a software or online tool, issued by Client to Company and directing Company to Process Personal Data.

1.13 "Personal Data" means any information relating to Data Subject which is subject to Data Protection Laws (defined below) and which Company Processes on behalf of Client other than Anonymous Data.

1.14 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

1.15 "Process" or "**Processing**" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.16 "Services" shall have the meaning set forth in the Agreement.

1.17 "Standard Contractual Clauses" means the EU SCCs and the UK SCCs.

1.18 "UK SCCs" means the EU SCCs, as amended by the UK Addendum.

1.19 "UK Addendum" means the addendum attached hereto as Exhibit D.

1.20 "Supervisory Authority" means an independent public authority which is established by a member state of the European Union, Iceland, Liechtenstein, or Norway, and the UK Information Commissioner's Office where UK GDPR is applicable.

2. Processing of DataDefinations

2.1 The rights and obligations of the Client with respect to this Processing are described herein. Client shall, in its use of the Services, at all times Process Personal Data, and provide instructions for the Processing of Personal Data, in compliance with Data Protection Laws. Client shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with Client's instructions will not cause Company to be in breach of the Data Protection Laws. Client is solely responsible for the accuracy, quality, and legality of (i) the Personal Data provided to Company by or on behalf of Client, (ii) the means by which Client acquired any such Personal Data, and (iii) the instructions it provides to Company regarding the Processing of such Personal Data. Client shall not provide or make available to Company any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Company from all claims and losses in connection therewith. This Addendum does not apply to Personal Data for which Company is a controller, except where otherwise noted.

2.2 Company shall not Process Personal Data (i) for purposes other than those set forth in the Agreement and/or Exhibit A, (ii) in a manner inconsistent with the terms and conditions set forth in this Addendum or any other documented instructions provided by Client, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Supervisory Authority to which the Company is subject; in such a case, the Company shall inform the Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest and (iii) in violation of the GDPR. Client hereby instructs Company to Process Personal Data in accordance with the foregoing and as part of any Processing initiated by Client in its use of the Services.

2.3 The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this Addendum.

2.4 Following completion of the Services, at Client's choice, Company shall return or delete the Personal Data, unless further storage of Personal Data is required or authorized by applicable law. If return or destruction is impracticable or prohibited by law, rule or regulation, Company shall take measures to block such Personal Data from any further Processing (except to the extent necessary for its continued hosting or Processing required by law, rule or regulation) and shall continue to appropriately protect the Personal Data remaining in its possession, custody, or control. If Client and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the certification of deletion of Personal Data that is described in Clause 8.1(d) and Clause 8.5 of the EU SCCs (as applicable) shall be provided by Company to Client only upon Client's request.

2.5 CCPA and VCDPA. Personal Data subject to the CCPA or VCDPA shall be processed in accordance with Exhibit E to this Addendum.

3. Authorized Employees

3.1 Company shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Employee.

3.2 Company shall ensure that all Authorized Employees are made aware of the confidential nature of Personal Data and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement with Company, any Personal Data except in accordance with their obligations in connection with the Services.

3.3 Company shall take commercially reasonable steps to limit access to Personal Data to only Authorized Employees.

4. Authorized Sub-Processors

4.1 Client acknowledges and agrees that Company may (1) engage its Affiliates and the Authorized Sub-Processors listed in the link provided in Exhibit B to this Addendum to access and Process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the Processing of Personal Data. By way of this Addendum, Client provides general written authorization to Company to engage sub-processors as necessary to perform the Services.

4.2 A list of Company's current Authorized Sub-Processors (the "**List**") will be made available to Client, either within Exhibit B attached hereto, at a link provided to Client, via email or through another means made available to Client. Such List which may be updated by Company from time to time. The List may provide a mechanism to subscribe to notifications of new Authorized Sub-Processors and Client agrees to subscribe to such notifications where available. At least ten (10) days before enabling any third party other than Authorized Sub-Processors to access or participate in the Processing of Personal Data, Company will add such third party to the List. Client may reasonably object to such an engagement on legitimate grounds by informing Company in writing within ten (10) days of receipt of the aforementioned notice by Client. Client acknowledges that certain sub-processors are essential to providing the Services and that objecting to the use of a sub-processor may prevent Company from offering the Services to Client.

4.3 If Client reasonably objects to an engagement in accordance with Section 4.2, and Company cannot provide a commercially reasonable alternative within a reasonable period of time, Company may terminate this Addendum. Termination shall not relieve Client of any fees owed to Company under the Agreement.

4.4 If Client does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Company, that third party will be deemed an Authorized Sub-Processor for the purposes of this Addendum.

4.5 Company will enter into a written agreement with the Authorized Sub-Processor imposing on the Authorized Sub-Processor data protection obligations comparable to those imposed on Company under this Addendum with respect to the protection of Personal Data. In case an Authorized Sub-Processors fails to fulfill its data protection obligations under such written agreement with Company, Company will remain liable to Client for the performance of the Authorized Sub-Processor's obligations under such agreement

4.6 If Client and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), (i) the above authorizations will constitute Client's prior written consent to the subcontracting by Company of the processing of Personal Data if such consent is required under the Standard Contractual Clauses, and (ii) the parties agree that the copies of the agreements with Authorized Sub-Processors that must be provided by Company to Client pursuant to Clause 9(c) of the EU SCCs may have commercial information, or information unrelated to the Standard Contractual Clauses or their equivalent, removed by the Company beforehand, and that such copies will be provided by the Company only upon request by Client.

5. Security of Personal Data.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Company shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data.

6. Transfers of Personal Data

6.1 The parties agree that Company may transfer Personal Data processed under this Addendum outside the European Economic Area ("**EEA**") or Switzerland as necessary to provide the Services. If Company transfers Personal Data protected under this Addendum to a jurisdiction for which the European Commission has not issued an adequacy decision, Company will ensure that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Data Protection Laws.

6.2 Ex-EEA Transfers. The parties agree that ex-EEA Transfers are made pursuant to the EU SCCs, which are deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

6.2.1 Module One (Controller to Controller) of the EU SCCs apply when Company is processing Personal Data as a controller pursuant to Section 9 of this Addendum.

6.2.2 Module Two (Controller to Processor) of the EU SCCs apply when Client is a controller and Company is processing Personal Data for Client as a processor pursuant to Section 2 of this Addendum.

6.2.3 Module Three (Processor to Sub-Processor) of the EU SCCs apply when Client is a processor and Company is processing Personal Data on behalf of Client as a sub-processor.

6.2.4 Module Four (Processor to Controller) of the EU SCCs apply when Client is a processor of Client Usage Data and Company processes Client Usage Data as a controller.

6.3 For each module, where applicable the following applies:

6.3.1 The optional docking clause in Clause 7 does not apply;

6.3.2 In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of sub-processor changes shall be as set forth in Section 4.2 of this Addendum;

6.3.3 In Clause 11, the optional language does not apply;

6.3.4 All square brackets in Clause 13 are hereby removed;

6.3.5 In Clause 17 (Option 1), the EU SCCs will be governed by the law of the EU member state where the data exporter is located.

6.3.6 In Clause 18(b), disputes will be resolved before the courts of the EU member state where the data exporter is located.

6.3.7 Exhibit B to this Addendum contains the information required in Annex I of the EU SCCs;

6.3.8 Exhibit C to this Addendum contains the information required in Annex II of the EU SCCs; and

6.3.9 By entering into this Addendum, the parties are deemed to have signed the EU SCCs incorporated herein, including their Annexes.

6.4 Ex-UK Transfers. The parties agree that ex-UK Transfers are made pursuant to the UK SCCs, which are deemed entered into and incorporated into this Addendum by reference.

6.5 Transfers from Switzerland. The parties agree that transfers from Switzerland are made pursuant to the EU SCCs with the following modifications:

6.5.1 The terms "General Data Protection Regulation" or "Regulation (EU) 2016/679" as utilized in the EU SCCs shall be interpreted to include the Federal Act on Data Protection of 19 June 1992 (the "FADP," and as revised as of 25 September 2020, the "**Revised FADP**") with respect to data transfers subject to the FADP.

6.5.2 The terms of the EU SCCs shall be interpreted to protect the data of legal entities until the effective date of the Revised FADP.

6.5.3 Clause 13 of the EU SCCs is modified to provide that the Federal Data Protection and Information Commissioner ("**FDPIC**") of Switzerland shall have authority over data transfers governed by the FADP and the appropriate EU supervisory authority shall have authority over data transfers governed by the GDPR. Subject to the foregoing, all other requirements of Section 13 shall be observed.

6.5.4 The term "EU Member State" as utilized in the EU SCCs shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from exercising their rights in their place of habitual residence in accordance with Clause 18(c) of the EU SCCs.

6.6 Supplementary Measures. In respect of any ex-EEA Transfer or ex-UK Transfer, the following supplementary measures shall apply:

6.6.1 As of the date of this Addendum, the Data Importer has not received any formal legal requests from any government intelligence or security service/agencies in the country to which the Personal Data is being exported, for access to (or for copies of) Client's Personal Data ("Government Agency Requests");

6.6.2 If, after the date of this Addendum, the Data Importer receives any Government Agency Requests, Company shall attempt to redirect the law enforcement or government agency to request that data directly from Client. As part of this effort, Company may provide Client's basic contact information to the government agency. If compelled to disclose Client's Personal Data to a law enforcement or government agency, Company shall give Client reasonable notice of the demand and cooperate to allow Client to seek a protective order or other appropriate remedy unless Company is legally prohibited from doing so. Company shall not voluntarily disclose Personal Data to any law enforcement or government agency. Data Exporter and Data Importer shall (as soon as reasonably practicable) discuss and determine whether all or any transfers of Personal Data pursuant to this Addendum should be suspended in the light of such Government Agency Requests; and

6.6.3 The Data Exporter and Data Importer will meet regularly to consider whether:

(i) the protection afforded by the laws of the country of the Data Importer to data subjects whose Personal Data is being transferred is sufficient to provide broadly equivalent protection to that afforded in the EEA or the UK, whichever the case may be;

(ii) additional measures are reasonably necessary to enable the transfer to be compliant with the Data Protection Laws; and

(iii) it is still appropriate for Personal Data to be transferred to the relevant Data Importer, taking into account all relevant information available to the parties, together with guidance provided by the supervisory authorities.

6.6.4 If Data Protection Laws require the Data Exporter to execute the Standard Contractual Clauses applicable to a particular transfer of Personal Data to a Data Importer as a separate agreement, the Data Importer shall, on request of the Data Exporter, promptly execute such Standard Contractual Clauses incorporating such amendments as may reasonably be required by the Data Exporter to reflect the applicable appendices and annexes, the details of the transfer and the requirements of the relevant Data Protection Laws.

6.6.5 If either (i) any of the means of legitimizing transfers of Personal Data outside of the EEA or UK set forth in this Addendum cease to be valid or (ii) any supervisory authority requires transfers of Personal Data pursuant to those means to be suspended, then Data Importer may by notice to the Data Exporter, with effect from the date set out in such notice, amend or put in place alternative arrangements in respect of such transfers, as required by Data Protection Laws.

7. Rights of Data Subjects

7.1 Company shall, to the extent permitted by law, notify Client upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, erasure, data portability, restriction or cessation of Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision-making (such requests individually and collectively "**Data Subject Request(s)**"). If Company receives a Data Subject Request in relation to Client's data, Company will advise the Data Subject to submit their request to Client and Client will be responsible for responding to such request, including, where necessary, by using the functionality of the Services. Client is solely responsible for ensuring that Data Subject Requests for erasure, restriction or cessation of Processing, or withdrawal of consent to Processing of any Personal Data are communicated to Company, and for ensuring that a record of consent to Processing is maintained with respect to each Data Subject.

7.2 Company shall, at the request of the Client, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Client in complying with Client's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that (i) Client is itself unable to respond without Company's assistance and (ii) Company is able to do so in accordance with all applicable laws, rules, and regulations. Client shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8. Actions and Access Requests

8.1 Company shall, taking into account the nature of the Processing and the information available to Company, provide Client with reasonable cooperation and assistance where necessary for Client to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Client does not otherwise have access to the relevant information. Client shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.2 Company shall, taking into account the nature of the Processing and the information available to Company, provide Client with reasonable cooperation and assistance with respect to Client's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Client shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Company.

8.3 Company shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum and retain such records for a period of three (3) years after the termination of the Agreement. Client shall, with reasonable notice to Company, have the right to review, audit and copy such records at Company's offices during regular business hours.

8.4 Upon Client's request, Company shall, no more than once per calendar year, either (i) make available for Client's review copies of certifications or reports demonstrating Company's compliance with prevailing data security standards applicable to the Processing of Client's Personal Data, or (ii) if the provision of reports or certifications pursuant to (i) is not reasonably sufficient under Data Protection Laws, allow Client or its authorized representative, upon reasonable notice and at a mutually agreeable date and time, to conduct an audit or inspection of Company's data security infrastructure and procedures that is sufficient to demonstrate Company's compliance with its obligations under this Addendum, provided that Client shall provide reasonable prior notice of any such request for an audit and such inspection shall not be unreasonably disruptive to Company's business. Client shall be responsible for the costs of any such audits or inspections, including without limitation a reimbursement to Company for any time expended for on-site audits. If Client and Company have entered into Standard Contractual Clauses as described in Section 6 (Transfers of Personal Data), the parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with this Section 8.4.

8.5 Company shall immediately notify Client if an instruction, in the Company's opinion, infringes the Data Protection Laws or Supervisory Authority.

8.6 In the event of a Personal Data Breach, Company shall, without undue delay, inform Client of the Personal Data Breach and take such steps as Company in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Company's reasonable control).

8.7 In the event of a Personal Data Breach, Company shall, taking into account the nature of the Processing and the information available to Company, provide Client with reasonable cooperation and assistance necessary for Client to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.8 The obligations described in Sections 8.6 and 8.7 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Client. Company's obligation to report or respond to a Personal Data Breach under Sections 8.6 and 8.7 will not be construed as an acknowledgement by Company of any fault or liability with respect to the Personal Data Breach.

9. Company's Role as a Data Controller.

The parties acknowledge and agree that with respect to Client Account Data and Client Usage data, Company is an independent controller, not a joint controller with Client. Company will process Client Account Data and Client Usage Data as a controller (i) to manage the relationship with Client; (ii) to carry out Company's core business operations, such as accounting, audits, tax preparation and filing and compliance purposes; (iii) to monitor, investigate, prevent and detect fraud, security incidents and other misuse of the Services, and to prevent harm to Client; (iv) for identity verification purposes; (v) to comply with legal or regulatory obligations applicable to the processing and retention of Personal Data to which Company is subject; and (vi) as otherwise permitted under Data Protection Laws and in accordance with this Addendum and the Agreement. Company may also process Client Usage Data as a controller to provide, optimize, and maintain the Services, to the extent permitted by Data Protection Laws. Any processing by Company as a controller shall be in accordance with Company's privacy policy set forth at: https://www.arkoselabs.com/legal/privacy-policy/.

EXHIBIT A TO THE ADDENDUM

Details of Processing

Nature and Purpose of Processing:

Company will process Client's Personal Data as necessary to provide the Services under the Agreement, for the purposes specified in the Agreement and this Addendum, and in accordance with Client's instructions as set forth in this Addendum. The nature of processing includes, without limitation:

- Receiving data, including collection, accessing, retrieval, recording, and data entry;
- Holding data, including storage, organization and structuring;
- Using data, including analysis, consultation, testing, automated decision making and profiling;
- Updating data, including correcting, adaptation, alteration, alignment and combination;
- Protecting data, including restricting, encrypting, and security testing;
- Sharing data, including disclosure, dissemination, allowing access or otherwise making available;
- Returning data to the data exporter or data subject; and
- Erasing data, including destruction and deletion.

Duration of Processing:

Company will process Client's Personal Data as long as required (i) to provide the Services to Client under the Agreement; (ii) for Company's legitimate business needs; or (iii) by applicable law or regulation. Client Account Data and Client Usage Data will be processed and stored as set forth in Company's privacy policy.

Categories of Data Subjects:

Client may provide Personal Data to Company, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and users of Client's services (who are natural persons)
- Employees or contact persons of Client's prospects, customers, and business partners
- Employees, consultants, agents, advisors, freelancers of Client (who are natural persons)
- Visitors to websites owned, operated or linked to by Client (who are natural persons)

Type of Personal Data:

Client may provide Personal Data to Company, the extent of which is determined and controlled by Client in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- User IP Address
- User Email Address
- User ID and/or Username

Sensitive Data or Special Categories of Data: None.

EXHIBIT B TO THE ADDENDUM

The following includes the information required by Annex I and Annex III of the EU SCCs, and Appendix 1 of the UK SCCs.

1. The Parties

CLIENT (referred to herein as the "Data Exporter")
Address: As provided in the Agreement
Contact person's name, position and details: As provided in the Agreement

And

ARKOSE LABS, INC. (referred to herein as the "Data Importer")
Address: As provided in the Agreement
Contact person's name, position and details: As provided in the Agreement

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified herein.

The Clauses become effective at the same time as the Addendum. You represent and warrant that you have the authority to agree to these terms on its behalf and the right to bind your employer thereto. If either you or your employer do not unconditionally agree to the Clauses, you have no right to use Arkose Labs' Services.

2. Description of the Transfer

Data Subjects	As described in Exhibit A
Categories of Personal Data	As described in Exhibit A
Special Category Personal Data (if applicable)	None
Nature of the Processing	As described in Exhibit A
Purposes of Processing	As described in Exhibit A
Duration of Processing and Retention (or the criteria to determine such period)	As described in the Addendum.
Frequency of the transfer	Continuously, as the Services are provided pursuant to the Agreement.
Recipients of Personal Data Transferred to the Data Importer	Affiliates and authorized sub-processors of the data importer.

3. Competent Supervisory Authority

The supervisory authority shall be the supervisory authority of the Data Exporter, as determined in accordance with Clause 13.

4. List of Authorized Sub-Processors

Please visit www.arkoselabs.com/sub-processors/ (https://www.arkoselabs.com/sub-processors/) to view the list of Authorized Sub-processors and to sign up for notifications.

EXHIBIT C TO THE ADDENDUM

Description of the Technical and Organisational Security Measures implemented by the Data Importer

The following includes the information required by Annex II of the EU SCCs and Appendix 2 of the UK SCCs.

Policies and Procedures. Company will maintain policies and procedures designed to secure Personal Data processed on behalf of Client against accidental or unlawful access or disclosure, and identify and minimize reasonably foreseeable internal security risks, including the following:

Access Control

1. Physical access to Company's facilities is limited to authorized employees and contractors.
2. Customer access to user data is limited to information supplied by the customer or user.
3. Administrator-level access privileges are restricted to authorized administrators.
4. Company has developed a process to register and authorize new users. New users must be authorized prior to being issued system credentials to access production.
5. Multifactor authentication is required for access to the production environment via VPN. Remote access to the production environment is limited and encrypted.

6. Company monitors, documents, and approves all access requests and changes. Access to modify security rules is restricted to authorized individuals.
7. Company maintains separate development, testing, and production environments. Access to release code into the production environment is restricted to only authorized personnel.

Operations and System Integrity

1. Policy and procedures for processes, such as reporting failures, incidents, system problems, concerns, and complaints, are made available to users.
2. Antivirus software is installed on workstations and laptops for personnel with access to the services systems environment.
3. Company has security policies that are approved by management.
4. Data transmission over customer portal is encrypted via Transport Layer Security ("TLS"). Access to the internal administrator tool is controlled via VPN.
5. Company performs and/or contracts with third-party vendors to perform SOC 2 Security audits, external vulnerability scans, comprehensive internal vulnerability scans, and penetration testing.
6. Vendor systems are subject to review at least annually as part of the vendor risk management process, including reviewing independent third-party reports.
7. Company has documented incident response and business continuity plans, including disaster recovery and backup restoration, which is reviewed at least annually.
8. Company schedules regular system backups to protect data loss in the event of a system failure. Restoration from backups is performed on an as-needed basis, or at least annually, to verify adequate recovery.

Organization of Information and Personnel Security

1. Company has formal organizational structures and defined roles, which includes departmental reporting lines with defined structures and responsibilities.
2. Employees are presented with an employee handbook which includes a code of conduct and statement of integrity.
3. Company has defined job descriptions for personnel responsible for designing, developing, implementing, operating, monitoring, and maintaining the information security.
4. Verification checks are performed on full-time employees when appropriate and permitted by local laws.
5. The technical competence of any personnel in a technical position is evaluated during the screening process.
6. Personnel are required to review information security policies during the onboarding process, and sign an acknowledgement affirming to abide by such policies.
7. Security trainings are conducted annually for all personnel.

EXHIBIT D TO THE ADDENDUM

UK Addendum

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

Part 1: Tables

Table 1: Parties

Start Date	This UK Addendum shall have the same effective date as the Addendum	
The Parties	Exporter	Importer
Parties' Details	Customer	Company
Key Contact	*See* Exhibit B of the Addendum	*See* Exhibit B of the Addendum

Table 2: Selected SCCs, Modules and Selected Clauses

EU SCCs	The Version of the Approved EU SCCs which this UK Addendum is appended to as defined in the Addendum and completed by Section 6.2 and 6.3 of the Addendum.

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 UK Addendum is set out in:

Annex 1A: List of Parties	As per Table 1 above
Annex 2B: Description of Transfer	See Exhibit B of the Addendum
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	*See* Exhibit C of the Addendum
Annex III: List of Sub processors (Modules 2 and 3 only):	*See* Exhibit B of the Addendum

Table 4: Ending this UK Addendum when the Approved UK Addendum Changes

Ending this UK Addendum when the Approved UK Addendum changes	☒ Importer ☐ Exporter ☐ Neither Party

Entering into this UK Addendum:

1. Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making ex-UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this UK Addendum

3. Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

UK Addendum	means this International Data Transfer Addendum incorporating the EU SCCs, attached to the Addendum as Exhibit D.
EU SCCs	means the version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information
Appendix Information	shall be as set out in Table 3

Appropriate Safeguards	means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making an ex-UK Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved UK Addendum	means the template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under Section 18 of the UK Addendum.
Approved EU SCCs	means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time).
ICO	means the Information Commissioner of the United Kingdom.
ex-UK Transfer	shall have the same definition as set forth in the Addendum.
UK	means the United Kingdom of Great Britain and Northern Ireland
UK Data Protection Laws	means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	shall have the definition set forth in the Addendum.

4. The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws applies.
7. If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for ex-UK Transfers, the hierarchy in Section 10 below will prevail.
10. Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.
11. Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.

Incorporation and Changes to the EU SCCs:

12. This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:
    A. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

B. Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and

C. the UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales

13. Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.
15. The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made:

A. References to the "Clauses" means this UK Addendum, incorporating the EU SCCs;

B. In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679",

C. Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

D. Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

E. Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

F. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

G. References to Regulation (EU) 2018/1725 are removed;

H. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

I. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

J. Clause 13(a) and Part C of Annex I are not used;

K. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

L. In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

M. Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales"

N. Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales." A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts."; and

O. The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to the UK Addendum

16. The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved UK Addendum which:

A. makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

B. reflects changes to UK Data Protection Laws;

The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

19. If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:

A. its direct costs of performing its obligations under the UK Addendum; and/or

B. its risk under the UK Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.

20. The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.

EXHIBIT E

United States Privacy Law Exhibit

This United States Privacy Law Exhibit ("Exhibit") supplements the DPA and includes additional information required by the CCPA and the VCDPA, in each case, as updated, amended or replaced from time to time. Any terms not defined in this Exhibit shall have the meanings set forth in the DPA and/or the Agreement.

A. CALIFORNIA

1. Definitions
   A. For purposes of this Section A, the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" shall have the meanings set forth in the CCPA.
   B. All references to "Personal Data," "Controller," "Processor," and "Data Subject" in the DPA shall be deemed to be references to "Personal Information," "Business," "Service Provider," and "Consumer" as defined in the CCPA.
2. Obligations
   A. Except with respect to Account Data and Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Business and Company is a Service Provider for the purposes of the CCPA (to the extent it applies) and Company is receiving Personal Information from Customer in order to provide the Services pursuant to the Agreement, which constitutes a Business Purpose.
   B. Customer shall disclose Personal Information to Company only for the limited and specified purposes described in Exhibit A to this DPA.
   C. Company shall not Sell or Share Personal Information provided by Customer under the Agreement.
   D. Company shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of performing the Services for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the CCPA.
   E. Company shall not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement outside of the direct business relationship between Company and Customer, except where and to the extent permitted by the CCPA.
   F. Company shall notify Customer if it makes a determination that it can no longer meet its obligations under the CCPA.
   G. Except and to the extent permitted by the CCPA, Company will not combine Personal Information received from, or on behalf of, Company with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.
   H. Company shall comply with all obligations applicable to Service Providers under the CCPA, including by providing Personal Information provided by Customer under the Agreement the level of privacy protection required by CCPA.
   I. In the event that Company engages a new sub-processor to assist Company in providing the Services to Customer under the Agreement, Company shall: (i) notify Customer of such engagement via the notification mechanism described in section 4.2 of the DPA at least ten (10) days before enabling a new Sub-Processor; and (ii) enter into a written contract with the Sub-processor requiring Sub-processor to observe all of the applicable requirements set forth in the CCPA.
3. Consumer Rights
   A. Company shall assist Customer in responding to Verifiable Consumer Requests to exercise the Consumer's rights under the CCPA as set forth in Section 7 of the DPA.
4. Audit Rights
   A. To the extent required by CCPA, Company shall allow Customer to conduct inspections or audits in accordance with Sections 8.3 and 8.4 of the DPA.

B. VIRGINIA

1. Definitions
   A. For purposes of this Section B, the terms "Consumer," "Controller," "Personal data," "Processing," and "Processor" shall have the meanings set forth in the VCDPA.
   B. All references to "Data Subject" in this DPA shall be deemed to be references to "Consumer" as defined in the VCDPA.

2. Obligations
   A. Except with respect to Account Data and Usage Data (as defined in the DPA), the parties acknowledge and agree that Customer is a Controller and Company is a Processor for the purposes of the VCDPA (to extent it applies).
   B. The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Exhibit A to this DPA.
   C. Company shall adhere to Customer's instructions with respect to the Processing of Customer Personal Data and shall assist Customer in meeting its obligations under the VCDPA by:
      i. Assisting Customer in responding to Consumer rights requests under the VCDPA as set forth in Section 7 of the DPA;
      ii. Complying with Section 5 (*Security of Personal Data*) of the DPA with respect to Personal Data provided by Customer;
      iii. In the event of a Personal Data Breach, providing information sufficient to enable Customer to meet its obligations pursuant to Va. Code § 18.2-186.6; and
      iv. Providing information sufficient to enable Customer to conduct and document data protection assessments to the extent required by VCDPA.
   D. Company shall maintain the confidentiality of Personal Data provided by Customer and require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;
   E. Upon Customer's written request, Company shall delete or return all Personal Data provided by Customer in accordance with Section 2.4 of the DPA, unless retention of such Personal Data is required or authorized by law or the DPA and/or Agreement.
   F. In the event that Company engages any other person a new Sub-processor to assist Company in providing the Services to Customer under the Agreement, Company shall enter into a written contract with the Sub-processor requiring Sub-processor to observe all of the applicable requirements of a Processor set forth in the VCDPA.
3. Audit Rights
   A. Upon Customer's written request at reasonable intervals, Company shall, as set forth in Sections 8.3-8.4 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate Company's compliance with its obligations under the VCDPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the VCDPA.

SOLUTIONS

Account Takeover (https://www.arkoselabs.com/solutions/account-takeover/)

Spam & Abuse (https://www.arkoselabs.com/solutions/spam-abuse/)

Payment Fraud (https://www.arkoselabs.com/solutions/payment-fraud/)

New Account Fraud (https://www.arkoselabs.com/solutions/new-account-fraud/)

Scraping (https://www.arkoselabs.com/solutions/scraping/)

API Security (https://www.arkoselabs.com/solutions/api-abuse/)

Micro-Deposit Fraud (https://www.arkoselabs.com/solutions/micro-deposit-fraud/)

IRSF (https://www.arkoselabs.com/solutions/international-revenue-share-fraud/)

Recaptcha Alternative (https://www.arkoselabs.com/recaptcha-alternative/)

PRODUCTS

Arkose Detect (https://www.arkoselabs.com/arkose-detect)

Arkose Protect (https://www.arkoselabs.com/arkose-protect)

Why Arkose? (https://www.arkoselabs.com/why-arkose)

Arkose Enforce (https://www.arkoselabs.com/arkose-enforce/)

SLA Guarantee (https://www.arkoselabs.com/sla-guarantee/)

Credential Stuffing Warranty (https://www.arkoselabs.com/credential-stuffing-warranty/)

Customers (https://www.arkoselabs.com/customers/)

INDUSTRIES

Finance & Fintech (https://www.arkoselabs.com/industries/finan fintech/)

Online Gaming (https://www.arkoselabs.com/industries/gami

Retail (https://www.arkoselabs.com/industries/retail

Sharing Economy (https://www.arkoselabs.com/industries/shari economy/)

Media & Streaming (https://www.arkoselabs.com/industries/medi streaming/)

Technology Platforms (https://www.arkoselabs.com/industries/techn platforms/)

Travel (https://www.arkoselabs.com/industries/trave

Online Gambling and iGaming (https://www.arkoselabs.com/industries/onlin gambling-igaming/)

Professional services (https://www.arkoselabs.com/services)

Integrations (https://www.arkoselabs.com/integrations/)

Global Infrastructure (https://www.arkoselabs.com/global-infrastructure/)

RESOURCES

All Resources (https://www.arkoselabs.com/resources/)

Whitepapers (https://www.arkoselabs.com/resources/?category=whitepaper)

Solution Briefs (https://www.arkoselabs.com/resources/?category=solution-brief)

eBooks (https://www.arkoselabs.com/resources/?category=ebook)

Reports (https://www.arkoselabs.com/resources/?category=report)

Case Studies (https://www.arkoselabs.com/resources/?category=case-study)

Videos (https://www.arkoselabs.com/resources/?category=video)

Infographics (https://www.arkoselabs.com/resources/?category=infographic)

Account Security Glossary (https://www.arkoselabs.com/explained/)

Blog (https://www.arkoselabs.com/blog/)

'A Founder and a Felon' series (https://www.arkoselabs.com/founder-and-felon-talk-about-future-cybercrime/)

BrightTalk Channel (https://www.arkoselabs.com/brighttalk-channel/)

G2 Leadership (https://www.arkoselabs.com/g2-leadership/)

EXPLORE

About Us (https://www.arkoselabs.com/about-us/)

Leadership (https://www.arkoselabs.com/leadership/)

Careers (https://www.arkoselabs.com/careers/)

News (https://www.arkoselabs.com/news/)

Events (https://www.arkoselabs.com/events/)

Customers (https://www.arkoselabs.com/customers/)

Compliance (https://www.arkoselabs.com/compliance/)

USEFUL LINKS

Sign In (https://dashboard.arkoselabs.com/login)

Brand Resources (https://www.arkoselabs.com/brand-resources/)

Developers (https://developer.arkoselabs.com/)

Support (https://support.arkoselabs.com/)

Sitemap (https://www.arkoselabs.com/sitemap/)

Arkose Labs (https://www.arkoselabs.com)

Contact Us (https://www.arkoselabs.com/contact-sales/)

(https://twitter.com/arkoselabs) (https://www.facebook.com/ArkoseLabs/) (https://www.linkedin.com/company/arkoselab

Terms of Use (/legal/terms-of-use/) | Privacy Policy (/legal/privacy-policy/) | Cookies