GDPR COMPLIANCE ADDENDUM

1. Relation to Agreement. Except as modified and supplemented herein, all other terms of the Agreement shall remain the same and in full force and effect. In the event of a conflict between the terms of this Addendum and the terms of the Agreement, the terms of this Addendum shall prevail and control.

2. Definitions.

(a) "**Applicable Laws**" means any statute, law, treaty, rule, code, ordinance, regulation, permit, certificate, or any other final and non-appealable action of a governmental authority having subject-matter jurisdiction. Applicable Laws, includes, without limitation: (i) Directive EC 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as amended, updated, or repealed from time to time ("Directive"), and any implementing, derivative, or related national legislation, rule, or regulation enacted thereunder by an European Union Member State subject to its jurisdiction, as well as the European General Data Protection Regulation (Regulation (EU) 2016/679), when it becomes applicable, and all related and derivative data protection laws (collectively "EU Data Protection Laws"), (ii) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and (iii) the Health Information Technology for Economic and Clinical Health ("HITECH") Act, and the Privacy and Security Rule regulations of HIPAA and the Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act and the Genetic Information Nondiscrimination Act ("Omnibus Final Rule") and all amendments to and further regulations of the HIPAA and HITECH Acts (collectively, "HIPAA").

(b) "**Personal Data**" means any information disclosed to, or otherwise received by, TokenEx in connection with the Agreement, that (alone or when used in combination with other information within TokenEx's direct control) can be used to identify, locate or contact an individual.

(c) **"Privacy Shield"** means the European Union-United States framework of privacy principles agreed to by the United States Department of Commerce and the European Union Commission on February 2, 2016 and formally adopted by the European Union Commission implementing decision C(2016) 4176 final on July 12, 2016.

(d) "**Security Incident**" means any unauthorized, accidental, or unlawful loss, acquisition, modification, use, destruction, alteration, disclosure, transfer, transport or access of Personal Data.

(e) "**Information System**" means the computing and/or network equipment, software and systems used by TokenEX in connection with the Agreement.

(f) "**Processing**" or "**Process**" means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, transfer, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking or dispersed erasure or destruction.

3. Ownership of Personal Data. During the term of the Agreement, TokenEx shall have a limited, non-transferable license to use Personal Data solely for performance under the Agreement for the benefit

Initial_____

of CLIENT. There are no implied licenses under this Addendum, and any rights to the Personal Data not expressly granted to TokenEx hereunder are reserved by CLIENT. Without limiting the foregoing, none of CLIENT's right, title and interest in Personal Data shall be diminished as a result of TokenEx's access to, or use of, such Personal Data.

4. Information Security and Privacy Compliance. With respect to Personal Data, TokenEx agrees to the following:

(a) TokenEx represents and warrants that it has developed and implemented, and that it maintains, monitors and uses appropriate administrative, technical, and physical security measures, safeguards, procedures and practices to protect the confidentiality, integrity and availability of all Personal Data against a Security Incident.

(b) TokenEx represents and warrants that it shall Process all Personal Data in accordance with all Applicable Laws and reasonable security requirements, policies, procedures and standards designated by CLIENT from time to time, including Processing of all Personal Data it receives from CLIENT's United States operations ("Privacy Shield Data") in accordance with CLIENT's Privacy Shield certification and Swiss-US Privacy Shield certification (collectively "Data Transfer Certifications") and that at all times TokenEx's protection of such Personal Data will meet or exceed the obligations for protection of such Personal Data set forth in the Privacy Shield principles. In the event new laws or regulations are implemented that require modifications to this Addendum, the parties mutually agree, in good faith, to modify this Addendum, within thirty (30) days of such law(s) or regulation(s) becoming effective. The parties further acknowledge that each is responsible to comply with any new law(s) or regulation(s) and to ensure that its handling of Personal Data is consistent therewith.

(c) TokenEx shall not transfer, disclose, use, transport, store, or in any manner Process, internally or via third parties, the Personal Data across any national borders or permit remote access to the Personal Data by any employee, affiliate, contractor, or other third party, unless such transfer or remote access is specifically permitted in the Processing instructions provided to it by CLIENT, or it has the prior written consent of CLIENT for such transfer or access. In order to receive Personal Data in the US from countries in the European Union or European Economic Area or Switzerland, TokenEx has been Privacy Shield certified, and if the data is from Switzerland, Swiss-U.S. Privacy Shield certified (collectively, the "Data Transfer Programs"). If TokenEx has not certified to the Data Transfer Programs, or if at any time during the course of this Agreement, if a particular Personal Data transfer does not qualify for the Data Transfer Programs, or if for some other reason the Data Transfer Programs are deemed invalid for purposes of a specific Personal Data transfer or for all Personal Data transfers, then the parties agree that for the duration of any such invalidity, the Model Contract Clause Provisions as approved by the EU Commission for Controller to Processor Personal Data transfers ("Controller to Processor Model Clauses") will be incorporated into this Addendum and this Agreement with respect to all Personal Data transfers from the EU and/or Switzerland, as the case may be, and TokenEx and CLIENT hereby agree to immediately complete, sign, and execute the Controller to Processor Model Clauses. In addition, TokenEx agrees to reasonably execute and undertake such other compliance mechanisms as may be required by Applicable Laws in other countries with similar data transfer restrictions. If, in addition to the Data Transfer Programs, the Controller to Processor Model Clauses are deemed invalid for the purpose of a specific Personal Data transfer or for all Personal Data transfers, the parties agree to

Initial_____

work together, and execute necessary documents, in order to determine an appropriate and legal mechanism for the transfer of such Personal Data.

(d) TokenEx shall Process Personal Data solely for the purpose of performing, and only to the extent needed to perform, TokenEx's obligations under the Agreement or as otherwise authorized in writing by CLIENT. If for any reason, TokenEx cannot comply with the obligations of this Addendum, with respect to the Processing of Personal Data, and with the obligations of the Privacy Shield principles, TokenEx shall immediately notify CLIENT in writing of such inability to comply.

(e) TokenEx shall not disclose, transfer, transport, or provide access to Personal Data to any third party unless such disclosure is necessary for performance under the Agreement, and provided that such third party is fully bound in a written agreement by obligations at least as restrictive as those contained herein, including those in the Privacy Shield principles. TokenEx shall remain responsible to CLIENT for all Processing of Personal Data undertaken by such third party and TokenEx shall remain responsible for any harm caused by such third party to the same extent as if TokenEx caused such harm itself, except to the extent TokenEx's disclosure of Personal Data to such third party is required or otherwise requested by CLIENT.

(f) Within thirty (30) days of (i) CLIENT's request, (ii) the date that Personal Data is no longer reasonably necessary for TokenEx's performance under the Agreement or (iii) termination or expiration of the Agreement, whichever occurs first, TokenEx shall return all Personal Data, including all copies and excerpts thereof, in TokenEx's possession and/or control (including any Personal Data in the possession of TokenEx's subcontractors or agents) to CLIENT in the original format in which the Personal Data was received (if alternative format is requested by CLIENT, it will be at CLIENT'S expense), or as requested by CLIENT, permanently and securely destroy such Personal Data using industry standard data wiping tools acceptable to CLIENT. TokenEx shall certify to CLIENT in writing that TokenEx has fully complied with the foregoing obligations.

5. TokenEx's Responsibilities for Required Disclosure, Security Incident Handling.

(a) Notwithstanding anything herein to the contrary, if TokenEx is required to disclose Personal Data pursuant to an order by a court or administrative body of competent jurisdiction or governmental agency TokenEx shall, if permitted by law, (i) immediately notify CLIENT prior to such disclosure; (ii) cooperate with CLIENT (at CLIENT's cost and expense) in the event that CLIENT elects to legally contest, request confidential treatment for, or otherwise attempt to avoid or limit, such disclosure; and (iii) limit such disclosure to the minimum extent required by law.

(b) TokenEx shall notify CLIENT of any suspected Security Incident immediately upon discovery of the Security Incident, but in no event more than forty-eight (48) hours after TokenEx reasonably believes a Security Incident has occurred. As part of such notification, TokenEx shall, to the extent known or can be reasonably determined, identify: (i) the specific Personal Data subject to the Security Incident; (ii) the nature of the unauthorized access, loss, use and/or disclosure; (iii) the person(s) involved in the Security Incident; (iv) the actions taken (or to be taken) by TokenEx to mitigate any deleterious effect of the Security Incident; and (v) the corrective actions taken (or to be taken) by TokenEx to prevent any future Security Incident. In addition, TokenEx shall provide to CLIENT such

Initial_____

other information as reasonably requested by CLIENT with respect to the Security Incident and whether such individual should be provided credit monitoring.

(c) In connection with any suspected Security Incident, TokenEx shall, at its sole cost and expense, be responsible for: (i) investigating the Security Incident; (ii) promptly taking all actions necessary or reasonably requested by CLIENT to mitigate the resulting damages; and (iii) providing all consumer notices and/or credit monitoring required by law or appropriate under the circumstances, provided that CLIENT will determine, in its sole discretion and pursuant to law, if any individual(s) should be notified of the Security Incident.

(d) At no cost to CLIENT, TokenEx will cure any Security Incident to any Information System which TokenEx develops and/or hosts for CLIENT, consistent with legal requirements and any forensic services that may require ensuring that evidence is properly preserved.

(e) In addition to any indemnification obligations of TokenEx under the Agreement, TokenEx shall indemnify, defend and hold harmless CLIENT, its affiliated companies, and each of their respective officers, directors, employees and agents, from and against any and all claims, actions, liabilities, losses, damages, judgments, awards, fines, penalties, costs and expenses (including reasonable attorneys' fees and defense costs and amounts paid in investigation, defense or settlement of the foregoing) which may be sustained or suffered by any of them arising out of or based upon a Security Incident or TokenEx's (including TokenEx's employees', agents' and subcontractors') breach of this Addendum. NO LIMITATION OF LIABILITY SET FORTH ELSEWHERE IN THE AGREEMENT IS APPLICABLE TO THE FOREGOING INDEMNITY OBLIGATIONS OR TOKENEX'S BREACH OF THIS ADDENDUM.

6. Assurance of Compliance.

(a) Upon CLIENT's written request, but not more frequently than annually, TokenEx shall certify in writing its compliance with this Addendum. Without limiting the foregoing, upon CLIENT's written request but not more frequently than annually, TokenEx shall provide documentary verification of its compliance with this Addendum and shall allow reasonable inspections and audits by CLIENT or its third-party designee(s) to verify such compliance. In connection therewith, CLIENT may require formal penetration testing, security logs or other information security tests. TokenEx shall timely comply with all reasonable recommendations that result from such inspections, audits and tests. Any such audit will be conducted at CLIENT's sole expense, except where the audit reveals TokenEx's material noncompliance with this Addendum, in which case the reasonable cost of the audit will be borne by TokenEx.

(b) In the event any CLIENT inspection or audit reveals TokenEx's noncompliance with this Addendum, or in the event CLIENT reasonably suspects any such noncompliance, TokenEx shall perform, upon CLIENT's request and at TokenEx's expense, a security audit by an independent third party approved by CLIENT in writing, to confirm TokenEx's compliance hereunder. The audit results, along with TokenEx's written plan for addressing or resolving any noncompliance or deficiencies identified by such audit, shall be provided to CLIENT within thirty (30) days of TokenEx's receipt of such audit results, subject to

Initial_____

reasonable confidentiality protections. If the audit finds TokenEx to be in compliance, then the cost associated with the requested audit will be borne by CLIENT.

(c) TokenEx shall maintain written policies and procedures regarding its disaster recovery and avoidance procedures, damage assessment and incident handling, and shall, upon CLIENT's reasonable request, provide CLIENT with access to such policies and procedures in a manner that allows CLIENT to assess TokenEx's effectiveness in maintaining the protection of Personal Data, including, without limitation, the operation, maintenance and technical controls of TokenEx's Information System.

(d) TokenEx acknowledges and understands that CLIENT has the right to provide a copy of this Agreement and this Addendum, or a summary hereof, to the United States Department of Commerce, or any other regulatory authority, at any time.

7. Termination.

(a) CLIENT may terminate the Agreement upon written notice in the event TokenEx is in material breach of any obligation under this Addendum, which default is incapable of cure or which, being capable of cure, has not been cured within thirty (30) days after receipt of notice of such default.

(b) Each provision of this Addendum that by its terms would survive expiration or termination of the Agreement shall so survive.

Initial_____