Additional Obligations regarding U.S. Users

This Schedule (Additional Obligations regarding U.S. Users) applies to the extent Customer makes available to a User who is located in, or resident of, the United States ("**U.S. User**") any of the Entrust Identity Verification services listed in the section of the Entrust Identity Verification Service Product Privacy Notice headed *"Additional Obligations regarding U.S. Users*" (each a "**Relevant Service**"), available here: https://www.entrust.com/sites/default/files/documentation/licensingandagreements/product-privacy-notice-identity-verification-services.pdf.

1. Definitions. Unless otherwise defined elsewhere in the Agreement, the terms below shall have the following meanings:

   1.1. "**Biometric Data**" means data generated by automatic measurements of an individual's biological characteristics, including: (i) biometric identifiers such as a fingerprint, voiceprint, retina or iris scan, scan of a hand or face geometry, or other unique biological patterns or characteristics that is used to identify a specific individual; and (ii) any information based on an individual's biometric identifier used to identify an individual.

   1.2. **"Facial Scan and Voice Recording Policy"** means the Identity Verification Services Facial Scan and Voice Recording Policy available at https://www.entrust.com/legal-compliance/data-privacy, as may be amended and updated from time to time.

   1.3. "**Sub-processor**" means any third-party engaged by Entrust to process Customer Personal Data for the purpose of providing the Services to Customer.

   1.4. "**U.S. Biometric Data Protection Laws**" means all applicable U.S. state, federal, or local laws and regulations with respect to the Processing, including collection, of Biometric Data, including but not limited to the Illinois Biometric Information Privacy Act (BIPA), Texas Capture or Use of Biometric Identifier Act (CUBI), and Washington Biometric Law.

2. Customer shall at all times during the Term comply with U.S. Biometric Data Protection Laws and take all necessary steps to ensure that Entrust and its Sub-processors may lawfully Process Biometric Data for the purpose of providing each Relevant Service and improving and developing the Entrust Identity Verification services, in accordance with U.S. Biometric Data Protection Laws.

3. Before any Biometric Data relating to a U.S. User is captured by, or uploaded or made available to, a Relevant Service, Customer shall provide notice to, and obtain consent from, the U.S. User which satisfies the notice and consent requirements set forth in this Schedule. Customer shall provide confirmation of this consent to Entrust before any Biometric Data relating to a U.S. User is captured by, or uploaded or made available to, a Relevant Service (see here for details of how to provide confirmation of consent), and shall retain a record of this consent for at least seven (7) years.

4. The notice and consent required by this Section must meet the requirements of U.S. Biometric Data Protection Laws and must not conflict with the Facial Scan and Voice Recording Policy. Without limiting the foregoing, this notice and consent must inform the U.S. User that if they consent, a third-party identity verification service provider (named Entrust) will:

   4.1. Process, including collect, their Biometric Data for the purpose of providing each Relevant Service and for the purpose of improving and developing the Entrust Identity Verification services;

   4.2. disclose their Biometric Data to Sub-processors who will Process it for those same purposes; and

4.3. retain their Biometric Data for the period set forth in the Facial Scan and Voice Recording Policy.

5. To the extent that U.S. Biometric Data Protection Laws require Customer to post a publicly available written policy that includes a retention schedule and guidelines for permanently destroying biometric data ("**Customer Biometric Data Retention Policy**"), such Customer Biometric Data Retention Policy shall not conflict with the Facial Scan and Voice Recording Policy.

6. Upon Entrust's request, Customer shall promptly provide information and documentation sufficient to substantiate Customer's compliance with this Schedule.

7. Customer shall enter into a valid and binding contractual agreement with each U.S. User ("**User Agreement**") prior to allowing the U.S. User to use a Relevant Service. The User Agreement shall include a mandatory arbitration provision that contains a non-severable class-action waiver (the "**Arbitration Agreement**") and shall expressly name Entrust Corporation and its Affiliates as intended third-party beneficiaries thereof, and state that Entrust Corporation and its Affiliates shall be entitled to enforce the Arbitration Agreement as if they were direct parties to it. For greater clarity, the class-action waiver contained in the Arbitration Agreement shall require that U.S. Users bring claims against Entrust Corporation or its Affiliates in the U.S. User's individual capacity, and not as a plaintiff or class member in any purported class or representative proceeding.