ENTRUST IDENTITY AS A SERVICE

TERMS OF SERVICE

These ENTRUST IDENTITY AS A SERVICE TERMS OF SERVICE ("Terms of Service") contain the terms and conditions that govern access to and use of the Service (as defined herein) by a Customer (as defined herein), MSP (as defined herein), and/or a Tenant (as such herein). These Terms of Service may be supplemented or modified by Special Terms and Conditions (as defined herein).

Our Agreement (as defined herein) with you takes effect when an "I Accept", "Start Trial" or similar button, and/or a check box presented with these Terms of Service is clicked and/or checked by you (the "**Effective Date**").

You, as the individual clicking and/or checking the aforementioned buttons and/or boxes, represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for (e.g. Customer, MSP, or Tenant), or, if you are an MSP administrator agreeing on behalf of one of your Tenants, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS, USE, DOWNLOAD, AND/OR INSTALL THE SERVICE. CONTINUED RIGHT TO ACCESS AND USE THE SERVICE IS CONTINGENT ON YOUR (OR THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE) CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT.

What is the Agreement?

For a Customer or MSP, the "**Agreement**" consists of:

- **For any Trial Period** (as defined herein), these Terms of Service and any additional agreements, policies, or terms and conditions referenced therein – e.g. acceptable use policy, service level agreement, data processing agreement, etc.); or
- **For any period of commercial or production use**, the Order (as defined herein) or Order Form (as defined herein), these Terms of Service, any applicable Special Terms and Conditions (must be referenced in an Order), and any additional agreements, policies, or terms and conditions referenced therein – e.g. acceptable use policy, service level agreement, data processing agreement, etc.).

For a Tenant, the "**Agreement**" consists of:

- These Terms of Service, and any additional agreements, policies, or terms and conditions referenced therein – e.g. acceptable use policy, service level agreement, data processing agreement, etc.).

The Agreement is between: (a) Customer; or (b) if applicable, Tenant, and (i) Entrust (Europe) Limited, if Customer is located in Europe; (ii) Entrust, Inc., if Customer is located in the United States; or (iii) Entrust Limited, if Customer is located in any other jurisdiction (as applicable, "**Entrust**").

1. DEFINITIONS. The following capitalized terms have the meanings set forth below whenever used in the Agreement.

1.1. "Affiliates" means, with respect to Entrust, any subsidiary of Entrust Corporation, and, with respect to Customer, any corporation or other entity that is directly or indirectly controlled by Customer either

through ownership of fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control.

1.2. "Application Program Interface" or "API" means proprietary interface software developed by Entrust to facilitate the connection and communication (*i.e.* the transmission of data, between an application and the Service, via the interface which consists of a series of commands), and provided to Customer by Entrust.

1.3. "Authentication Client" means one of the following software components responsible for authentication for a specific type of client (as further described in the Documentation): Citrix Web Interface Protection, RADIUS Protection, AD FS Protection, IIS Website Protection, Windows Logon Protection, or Secure Device Provisioning.

1.4. "Authentication Record" means a record setting out the details of each authentication attempt made by a User. Authentication Records may include Personal Data.

1.5. "Authorized Reseller" means (i) if Customer is an MSP, a distributor authorized by Entrust to market, sell and distribute the Service to MSPs, or (ii) if Customer is not an MSP, a distributor or reseller, as applicable, authorized by Entrust to market, sell and distribute the Service to Customers.

1.6. "AUP" means Entrust's acceptable use policy, as may be modified from time to time, available on the Service portal or on Entrust's website at https://www.entrustdatacard.com/resource-center/-/media/documentation/productsupport/intellitrust-aup.pdf.

1.7. "Claim" means, for the purposes of Article 11 (*Indemnification*), a third-party claim, demand, suit, or proceedings.

1.8. "Cloud Components" means elements of the Service which Entrust hosts on its (or its hosting providers') computers.

1.9. "Confidential Information" means any non-public information disclosed by one party ("Disclosing Party") to the other party ("Receiving Party") in any form (written, oral, etc.) that is designated as confidential when it is disclosed or that reasonably should be understood to be confidential given the nature of the information and/or the circumstances of the disclosure, including but not limited to intellectual property, know-how, trade secrets, product designs, product specifications, formulas, compositions, software, drawings, processes, technical, sales, marketing, financial and other strategic or sensitive business information or data, including any copies or tangible embodiments containing such information. Without limiting the generality of the foregoing, all Entrust financial information (including pricing) and Documentation is Entrust Confidential Information whether or not so designated.

1.10. "Customer" means the legal entity referenced in the web-based intake form completed by Customer (or otherwise provided to Entrust in writing) and validated by Entrust prior to Customer accepting the terms and conditions of the Agreement. Use of the term "Customer" shall include MSPs, unless otherwise specified.

1.11. "Customer Account" means the account Customer sets up through the Service once Customer has agreed to the terms and conditions of the Agreement. Any reference to information (including, without limitation, data) being supplied through Customer Account shall include any such information provided or supplied by Tenants and/or Users through their own respective Tenant and/or User accounts that are set up subordinate to the main Customer Account.

1.12. “Customer Data” means any Customer, Tenant, or User data or information (including, third-party data or information) that is supplied to Entrust (or its sub-processors) by or on behalf of Customer, Tenants, and/or Users, through the Customer Account or otherwise in connection with the Service (including without limitation, device and computer information). Irrespective of any actual database encryption, or logical or physical segregation, any data or information uploaded to the Service by a Tenant or a User is considered to have been uploaded to the Service by Customer. Customer Data may include Personal Data.

1.13. “Documentation” means written materials prepared by Entrust (or its licensors or service providers) relating to the Service, including, without limitation, guides, manuals, instructions, policies, reference materials, release notes, online help or tutorial files, support communications (including any disputes between the parties) or any other materials provided in connection with modifications, corrections, or enhancements to the Service, all as may be modified from time to time.

1.14. “DPA” means the latest version of Entrust’s standard data processing agreement, as may be modified from time to time, available on the Service portal or on Entrust’s website at https://www.entrustdatacard.com/resource-center/-//-/media/documentation/licensingandagreements/data-processing-agreement.pdf.

1.15. “Extension” means any separately licensed and downloaded (by Customer or Tenants) Entrust suite, configuration file, add-on, software integration, technical add-on, example module, command, function or application that extends the features or functionality of third-party software or third-party services (including cloud services) separately licensed or lawfully accessed by Customer (or Tenants). For clarity, an Extension shall not form part of the Service.

1.16. “Indemnified Associates” means, in relation to a party being indemnified pursuant to Article 11 (*Indemnification*), its officers, directors, shareholders, parents, Affiliates, agents, successors, and assigns.

1.17. “Licensed Software” means either (i) Entrust Identity as a Service Gateway software application, or (ii) Authentication Clients (licensed by Entrust hereunder or pursuant to separate terms and conditions made available at the point of download), in either case including updates and new versions Entrust provides to Customer and/or Tenants, as applicable, or any similar replacement software designated by Entrust. Licensed Software shall not include Ancillary Software (as defined in Section 14.4 (*Third Party Software*)).

1.18. “MSP” means a Customer that (i) is a managed security service provider that offers hosting infrastructure and/or business applications to Tenants, and (ii) meets the MSP requirements set out in the Documentation.

1.19. “Order” means a Customer-issued purchase order (excluding any terms and conditions thereon) that is accepted by Entrust and refers to a valid Entrust quote for the Service and incorporates these Terms of Service and any applicable Special Terms and Conditions.

1.20. “Order Form” means an order form signed by MSP and Entrust, in the format set out in the Documentation, for the Service (applicable to MSP-model only).

1.21. “Personal Data” has the meaning set out in the DPA.

1.22. "Profile" means User and device profiles constructed from authentication patterns and device-identifying technical data. Profiles may include data from third party service providers, and may also include Personal Data.

1.23. "Service" means the Identity as a Service platform which consists of Cloud Components, as well as Licensed Software and Documentation.

1.24. "Service Data" means any information and data relating to the access, use, and/or performance of the Service, including data generated in connection with Customer's, Tenants', and/or Users' use of the Service (e.g., analytics data, statistics data and performance data). Service Data does not include Authentication Records, Customer Data, Profiles, or Personal Data.

1.25. "SLA" means Entrust's standard Identity as a Service service level agreement, as may be modified from time to time, available on the Service portal or on Entrust's website at https://www.entrustdatacard.com/resource-center/-/media/documentation/productsupport/intellitrust-sla.pdf.

1.26. "Special Terms and Conditions" means any terms and conditions: (i) that are specific to a particular Service functionality; and (ii) that are attached as a schedule to these Terms of Service.

1.27. "Tenant" means any MSP client that has entered into a Tenant Agreement and has accepted the terms and conditions of the Agreement. Reference to "Tenant(s)" in the Agreement shall only be applicable if the Customer is an MSP.

1.28. "Tenant Agreement" has the meaning set forth in Section 7.6 (*Tenant Agreements*).

1.29. "Term" has the meaning set out in Section 13.1 (*Term*).

1.30. "Tokens" means the Entrust tokens (if any) specified in an Order.

1.31. "Third-Party Integrations" has the meaning set out in Section 6.8 (*Third-Party Integrations*).

1.32. "User" means any individual end user who accesses or uses the Service through the Customer Account, via the Service portal or otherwise (e.g. API-based access).

2. CLOUD COMPONENTS & USE OF THE SERVICE.

2.1. Grant of Right to Use the Cloud Components. Subject to Customer's (and Tenant's) compliance with the Agreement, Entrust grants to Customer (or Tenant), during the Term of the Agreement, a worldwide, non-exclusive, non-transferable, non-sub-licensable right to, all in accordance with the Documentation and for the sole purpose of authenticating the identity of a User, and not for resale or any other commercial purpose:

(a) access and use the Cloud Components via the Service portal or otherwise for the purpose of managing its Users' access to and use of the Cloud Components, and grant its Users access to and use of the Cloud Components; and

(b) if Customer is an MSP, grant its Tenant(s) access to and use of the Cloud Components via the Service portal or otherwise for the purpose of managing their Users' access to and use of the Cloud Components, and the right to grant such Tenants' Users access to and use of the Cloud Components.

Notwithstanding the foregoing grant of rights, any access to and use of the Cloud Components by Customer, Tenants, and/or Users during any Trial Period (as defined herein) shall be solely for evaluation purposes and not for resale or any other commercial purpose.

2.2. Licenses from Customer (or Tenant). Subject to the terms and conditions of the Agreement, Customer (or Tenant) grants to Entrust the non-exclusive, nontransferable worldwide right to copy, store, record, transmit, display, view, print or otherwise use (a) Customer Data solely to the extent necessary to provide the Service to Customer (or Tenant), and (b) any trademarks that Customer (or Tenant) provides Entrust for the purpose of including them in Customer's user interface of the Service ("**Customer Trademarks**"). Customer shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness and copyright of all Customer Data.

2.3. Service Levels. The sole remedies for any failure of the Cloud Components are listed in the SLA. Service credits issued pursuant to the SLA, if any, will only be applied against the costs associated with Customer's (or Authorized Reseller's, if applicable) subsequent subscription renewal. Entrust is not required to issue refunds for or to make payments against such service credits under any circumstances.

2.4. Documentation. Customer may reproduce and use the Documentation solely as necessary to support Customer's, Tenants', and Users' access to and use of the Service. Each permitted copy of all or part of the Documentation must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust or downloaded or otherwise accessed by Customer.

2.5. Service Revisions. Entrust may add, reduce, eliminate or revise Service features and functionality at any time. Additionally, Entrust may add, reduce, eliminate or revise services levels at any time where a third-party service level agreement applicable to the Service has been changed. Where any such change will cause a material detrimental impact on Customer, Entrust will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice (email or posting notice at the Service portal constitutes written notice). If Customer is an MSP, it will be Customer's responsibility to notify its Tenants of any such changes.

2.6. Tenants; Users. Customer will make no representations or warranties regarding the Service or any other matter, to Tenants, Users, and/or any other third party, for or on behalf of Entrust, and Customer will not create or purport to create any obligations or liabilities on or for Entrust regarding the Service or any other matter. Customer will be liable to Entrust for any and all Tenants' (notwithstanding that any such Tenant accepts the Agreement by clicking an "I Accept", "Start Trial" or similar button, and/or check a box signifying acceptance of the Agreement) and/or Users' acts and/or omissions in relation to or breach of the Agreement or otherwise in relation to their access to and/or use of the Service. Customer acknowledges and agrees that it shall be responsible for coordinating all communication with Entrust under the Agreement, and that Entrust shall direct any requests or other communications by Tenants or Users to Customer.

2.7. Support (Non-MSP Customer). If an Order calls for support, any such support be will provided pursuant to the terms and conditions set out at http://www.Entrust Datacard.com/legal/agreements/esupport.pdf. Notwithstanding the foregoing, where support is purchased through an Authorized Reseller and the Order indicates that the Authorized Reseller will provide support, then such support will be provided by the Authorized Reseller (and not Entrust). Entrust will have no obligation to provide support or other services directly to Users. Entrust will have no obligation to provide support or other services in relation to Ancillary Software.

2.8. Support (MSP). If Customer is an MSP, Entrust and MSP will provide support to the MSP pursuant to the terms and conditions set out at http://www.EntrustDatacard.com/legal/agreements/IntelliTrustMSPsupport.pdf. MSP will be solely responsible to provide First Line Support (as defined in the MSP Support Terms and Conditions (Identity as a Service) referenced at the aforementioned link) to its Tenants. MSP will enter into a support agreement with each of its Tenants (which will not contain any reference to Entrust, create any obligations or liabilities on Entrust, and will not make any representations, warranties or conditions on behalf of Entrust). Tenants and Users shall not directly contact Entrust, and Entrust shall have no obligation to provide support or other services directly to Tenants and/or Users. Entrust will have no obligation to provide support or other services in relation to Ancillary Software.

3. LICENSED SOFTWARE.

3.1. License. Subject to Customer's (or Tenant's) compliance with the Agreement, Entrust hereby grants Customer (or Tenant):

(a) a personal, non-exclusive, non-transferable, non-sub-licensable license to install and use the Licensed Software in accordance with the Agreement, in object code form only, all in accordance with the Documentation and for the sole purpose of conducting Customer's (or Tenant's) internal business operations, and not for resale or any other commercial purpose; or

(b) if Customer is an MSP, a right to grant a personal, non-exclusive, non-transferable, non-sub-licensable license to each of its Tenants to install and use the Licensed Software, in object code form only, all in accordance with the Documentation and for the sole purpose of conducting such Tenants' internal business operations, and not for resale or any other commercial purpose.

Notwithstanding the foregoing, any installation and use of the Licensed Software by Customer and/or Tenants during any Trial Period (as defined in Section 4.3 (*Trial Period; Termination or Suspension*)) shall be solely for evaluation purposes and not for resale or any other commercial purpose.

3.2. Restrictions on Software Rights. Copies of the Licensed Software provided to Customer (or Tenant) pursuant to the Agreement are licensed, not sold, and Customer (or Tenant) receives no title to or ownership of any copy of the Licensed Software itself. Furthermore, Customer (or Tenant) receives no rights to the Licensed Software other than those specifically granted in Section 3.1 (*License*) above. Without limiting the generality of the foregoing, Customer (and Tenant) will not: (a) modify, translate, create derivative works from, distribute, publicly display, publicly perform, or sublicense (or further sublicense beyond the right to sub-license granted Section 3.1(b), if Customer is an MSP) the Licensed Software; (b) use the Licensed Software in any way prohibited by Section 7.1 (*Acceptable Use and Restrictions)* below; (c) reverse engineer the Licensed Software or Tokens, or decompile, disassemble, or otherwise attempt to derive any of the Licensed Software's source code (except to the extent such prohibition is contrary to applicable law that cannot be excluded by the agreement of the parties); or (d) attempt to circumvent or disable any restriction or entitlement mechanism that is present or embedded in the Licensed Software.

3.3. Hosting and Management. Customer (or Tenant) agrees that it will be responsible for installing and managing the Licensed Software on its own premises (or, in the case Customer is an MSP, causing each of its Tenants to take responsibility for installing and managing the Licensed Software on such Tenant's premises) in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Service resulting from Customer's (or Tenants') improper installation and/or management of the Licensed Software.

3.4. Authentication Clients. The Authentication Clients may be made available under separate license terms and conditions ("Separate EULA") than those of the Agreement. To the extent Customer's (or Tenants') obtained a license to use the Authentication Clients pursuant to Separate EULA, then their use of the Authentication Clients shall be subject to the Separate EULA. In the event the Separate EULA expires or is terminated (other than for breach by the Customer or Tenants, as applicable), then Customer and/or Tenants may continue to use the Authentication Clients pursuant to the Agreement.

4. EVALUATION.

4.1. Evaluation Purposes. Evaluation purposes do not include (i) any purpose from which Customer (or Tenants, if applicable) generate revenue, and (ii) use within a production environment. For clarity, only fictitious non-production data can be used in an evaluation environment.

4.2. Inapplicable Sections. Sections 2.3 (*Service Levels*), 11.2 (*Indemnification by Entrust*) and 11.4 (*Mitigation by Entrust*) do not apply to Customer, or any Tenant and/or Users access to or use of the Service for evaluation purposes.

4.3. Trial Period; Termination or Suspension. Customer's (or Tenants') evaluation of the Service pursuant to this Section 4 (*Evaluation*) shall commence on the Effective Date and continue for a period of thirty (30) days ("Trial Period"), or as otherwise agreed to by Entrust in writing with Customer (or Tenant or Authorized Reseller). Notwithstanding the foregoing, Entrust may in its sole discretion suspend or terminate Customer's, Tenants', or any of their respective Users' evaluation access to and use of the Service at any time, for any or no reason, without advanced notice.

5. FEES.

5.1. Customer shall pay Entrust (or an Authorized Reseller, as applicable) the fees (including where overages are applicable, any overage fees) for the Service as set out in an Order or Order Form (or equivalent Authorized Reseller document, if applicable). Unless otherwise stated in the Order or Order Form (or equivalent Authorized Reseller document, if applicable), Customer will pay all amounts payable under the Agreement within thirty (30) days of the date of the invoice. All amounts payable by Customer under the Agreement are non-refundable and will be paid without setoff or counterclaim and without any deduction or withholding. There may be changes to fees and charges for the Service (including, without limitation, for any new feature or functionality of a Service) which, if applicable, will be effective following notice (email or posting notice at the Service portal to suffice as adequate notice) to Customer of any such change. Customer will be responsible for all taxes (other than taxes based on Entrust's net income), fees, duties, or other similar governmental charges. Entrust may elect to charge Customer interest for late fees at the lesser of 1.5% per month or the maximum rate permitted by law. In addition, if Entrust does not receive payment from Customer (or from an Authorized Reseller, as applicable) within five (5) business days of Entrust providing written notice to Customer that a payment is delinquent pursuant to the payment terms of the Agreement (or those between Entrust and the Authorized Reseller, if applicable), Entrust may suspend or terminate Customer's, Tenant's, and/or Users' access to and use of all or part of the Service, and may refuse any additional Orders or Order Forms.

6. CUSTOMER DATA, AUTHENTICATION RECORDS & PRIVACY.

6.1. Customer Data; Profiles; Authentication Records; Personal Data. Customer (or Tenant) acknowledges and agrees that the Service requires certain Customer Data, Profiles, and Personal Data, in order to operate. Use of the Service by Customer, Tenants, and Users will also generate

Authentication Records. Customer (or Tenant) grants to Entrust, its Affiliates, and any of their respective applicable subcontractors and hosting providers), a world-wide, limited right, during the Term, to host, copy, transmit and display Customer Data and Personal Data as reasonably necessary for Entrust (or its Affiliates, and any of their respective applicable subcontractors and hosting providers) to provide the Service in accordance with the Agreement.

6.2. Service Regions. Customer will select the geographic region(s) (each a "**Service Region**") where Authentication Records, Customer Data, Profiles and Service Data will be stored (subject to any limitations of Entrust's hosting provider). With respect to the Authentication Records, Customer Data, Profiles and Service Data, and any Personal Data contained therein, that Entrust may collect hereunder, Customer consents to the storage in and/or the transfer into, the Service Region(s) which the Customer has selected. Notwithstanding the foregoing, Customer (and Tenant) acknowledges and agrees: (i) that Entrust may send short message service (SMS) messages through the United States and/or Canada as part of the Service; and (ii) Customer's billing information may be stored in the United States and/or Canada.

6.3. Data Processing. To the extent Entrust processes any Personal Data on Customer's behalf in performance of the Agreement, the terms of the DPA, which are incorporated herein by reference, shall apply and Entrust, Customer (and Tenant) agree to comply with such terms. Customer's (and Tenant's) acceptance of the Agreement shall be treated as acceptance and signing of the DPA (including the Standard Contractual Clauses attached to the DPA). Entrust reserves the right to update the DPA from time to time to comply with legal and regulatory requirements, and to keep current with upgrades and enhancements to its products and services. The latest version of the DPA posted on Entrust's website shall always apply.

6.4. Excluded Data. Customer represents and warrants that Customer Data, Personal Data, and Profiles do not and will not include any Excluded Data. "Excluded Data" refers to: (i) social security numbers or their equivalent (e.g., social insurance numbers), driver license numbers, biometric data, health card numbers and other health-related information; (ii) other Personal Data that would be considered sensitive in nature including without limitation of a "special category of data" under EU Directive 95/46; and (iii) data regulated under the Health Insurance Portability and Accountability Act or the Gramm-Leach-Bliley Act, or the Payment Card Industry Data Security Standards or similar laws or regulations in place now or in the future in the applicable jurisdiction (collectively, the "Excluded Data Laws"). CUSTOMER (AND TENANTS) RECOGNIZE(S) AND AGREE(S) THAT: (i) ENTRUST HAS NO LIABILITY FOR ANY FAILURE TO PROVIDE PROTECTIONS SET FORTH IN THE EXCLUDED DATA LAWS OR OTHERWISE TO PROTECT EXCLUDED DATA; AND (ii) THE SERVICE IS NOT INTENDED FOR MANAGEMENT OR PROTECTION OF EXCLUDED DATA AND MAY NOT PROVIDE ADEQUATE OR LEGALLY REQUIRED SECURITY FOR EXCLUDED DATA.

6.5. Profiles; Service Data; Use of Data. Entrust owns all right, title and interest in and to Service Data and Profiles (excluding any Personal Data contained in the Profiles) and, without limiting the generality of the foregoing, may use, reproduce, sell, publicize, or otherwise exploit such Profiles and Service Data in any way, in its sole discretion.

6.6. Consents. Customer (or Tenant) represents and warrants that, before authorizing a User to use the Service and before providing Customer Data or Personal Data to Entrust, Customer (or Tenant) will have provided and/or obtained the requisite consents (if any) and made all requisite disclosures (if any) to Users, in accordance with all applicable laws, rules or regulations for the collection, use, and disclosure of the Customer Data or Personal Data, by Entrust (including by any of its applicable subcontractors or hosting service providers) in accordance with the Agreement. Customer (or Tenant) shall be responsible for the accuracy, quality and legality of Customer Data or Personal Data

and the means by which Customer (or Tenant) acquired them.

6.7. Consents relating to Extensions. Customer (or Tenant) acknowledges and agrees that certain Extensions may enable third-party software or third-party services (including cloud services) to download certain Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data from the Service, and, by enabling such third-party software or third-party services (including cloud services) Customer (or Tenant) agrees to such downloads. Customer (or Tenant) represents and warrants that, before using any Extension, Customer (or Tenant) will have obtained the requisite consents (if any) from and made all requisite disclosures (if any) to Users, in accordance with all applicable laws, rules or regulations in order to allow for the downloading and/or transfer of such Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data, from Entrust (including any applicable subcontractors and hosting providers) to the Customer-licensed (or Tenant-licensed) third-party software or third-party services (including cloud services) enabled by the Extension.

6.8. Third-Party Integrations. Customer (or Tenant) may enable integrations between the Service and certain third-party services contracted by Customer or, if applicable, Tenants (each, a "Third-Party Integration"). By enabling a Third-Party Integration between the Service and any such third-party services, Customer (or Tenant) is expressly instructing Entrust to share all Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data, necessary to facilitate the Third-Party Integration. Customer (or Tenant) is responsible for providing any and all instructions to such third part services provider about the use and protection of such Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data. Customer (or Tenant) acknowledges and agrees that Entrust is not a sub-processor for any such third-party services providers in relation to any Personal Data contained in the aforementioned data or information, nor are any such third-party services providers sub-processors of Entrust in relation to any Personal Data contained in the aforementioned data or information.

7. CUSTOMER'S RESPONSIBILITIES, RESTRICTIONS & ACKNOWLEDGEMENTS.

7.1. Acceptable Use and Restrictions. Customer (or Tenant) will comply with the AUP. In addition to the restrictions in Section 3.2 (*Restrictions on Software Rights),* unless otherwise expressly authorized elsewhere in the Agreement, Customer (or Tenant) shall not: (a) license, use, rent, sell, resell, lease, distribute, pledge, assign, transfer, display, host, outsource, disclose or otherwise commercially exploit the Service; (b) use the Service for service bureau or time-sharing purposes; (c) modify, make derivative works of, disassemble, reverse compile, or reverse engineer any part of the Service; (d) provide Service passwords or other log-in information to any third party; I permit any unauthorized third parties from accessing the Service; (f) copy, reproduce, distribute, republish, download, display, post or transmit in any form or by any means, including but not limited to electronic, mechanical, photocopying, recording, or other means, any part of the Service; (g) share non-public Service features or content with any third party; (h) access the Service in order to build a competitive product or service, to build a product using similar ideas, features, functions or graphics of the Service, or to copy any ideas, features, functions or graphics of the Service; (i) send or store infringing or unlawful material or viruses, worms, time bombs, Trojan horses and other harmful or malicious codes, files, scripts, agents or programs; (j) attempt to gain unauthorized access to, or disrupt the integrity or performance of, the Service or the data contained therein; or (k) use the Service other than in accordance with the Agreement and in compliance with all applicable laws, rules or regulations. In the event that Entrust suspects any breach of the requirements of this Section 7.1 *(Acceptable Use and Restrictions)*, including, without limitation, by Customer, Tenants, and/or Users, Entrust may suspend Customer's, Tenants' and/or Users' access to and use of the Service without advanced

notice, in addition to such other remedies as Entrust may have pursuant to the Agreement. Neither the Agreement nor the AUP requires that Entrust take any action against any Customer, Tenant, and/or User or other third party for violating the AUP, this Section 7.1 *(Acceptable Use and Restrictions)*, or the Agreement, but Entrust is free to take any such action at its sole discretion.

7.2. Unauthorized Access. Customer (or Tenant) will take reasonable steps to prevent unauthorized access to the Service, including, without limitation, by protecting its passwords and other log-in information. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Service or breach of its security and will use best efforts to stop such breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Tenants and/or Users.

7.3. Compliance with Laws. In its access to and use of the Service, the Tokens, any Extensions, and any Third-Party Integrations, Customer (or Tenant) will comply with, and cause all its Tenants and/or Users to comply with, all applicable laws, rules or regulations, including, without limitation, (i) all privacy and data protection laws, rules or regulations governing the protection of Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data; and all trade control laws, rules or regulations, including the Export Administration Regulations (EAR) administered by the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") and U.S. sanctions regulations administered by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"); and (iii) any import or export licenses required pursuant to Section 14.18 (*Technology Export*).

7.4. Tenants; Users; Service Access. Customer is responsible and liable for: (a) the configuration of the Service to meet its own (and its Tenants' and/or Users') requirements; (b) Customer Data, Profiles, Personal Data, and any other data uploaded to the Service through the Customer Account or otherwise by Customer, its Tenants, and/or Users; (c) Customer's, its Tenants', and/or Users' access to and use of the Service, including, without limitation, any Tenant or User conduct that would violate the AUP or any other the requirements of the Agreement (including, without limitation, those applicable to Customer); and (d) any access to and use of the Service through the Customer Account. Entrust will have no responsibility or liability for the accuracy of data uploaded to the Service by Customer, its Tenants, and/or Users, including, without limitation, Customer Data, Profiles, and Personal Data. Customer (or Tenant) will comply with all applicable laws, rules and regulations, and obtain all permits, licenses and authorizations or certificates that may be required, in connection with its activities pursuant to the Agreement.

7.5. End User Licenses. Where Customer (or Tenant) grants Users access to and use of the Service, Customer (or Tenant) will do so pursuant to an agreement with each User (each an "**End User License**") which contains terms and conditions that: (i) only permit access to and use of the Service in combination with Customer's (or Tenant's) products or systems; (ii) prohibit decompiling, reverse engineering or modification of the Service (except as and only to the extent any foregoing restriction is prohibited by applicable laws, rules, or regulations); (iii) are at least as protective of the Service including, without limitation, the intellectual property rights and Confidential Information of Entrust (and its Affiliates, licensors, suppliers and hosting providers), as the terms and conditions of the Agreement; (iv) flow through the acknowledgements and obligations pursuant to Section 7.7 (*No Hazardous Environments*); and (v) disclaim, to the extent permitted by applicable laws, rules or regulations, any liability or responsibility of Entrust (including its Affiliates, licensors, suppliers and hosting providers) to Tenants and/or Users. Customer (or Tenant) will not make any representations and/or warranties on behalf of Entrust, whether express, implied, statutory, or otherwise, including, without limitation, warranties of merchantability, fitness for a particular purpose, satisfactory quality, title, or non-infringement. Customer (or Tenant) agrees to enforce Entrust's rights under the End User Licenses, in the same manner and to the same extent as Customer (or Tenant) enforces its own rights

thereunder or to allow Entrust to do so by naming it as a third-party beneficiary in the End User License that applies to Customer's (or Tenant's) products or systems. Customer (or Tenant) agrees to cooperate with Entrust to maintain Entrust's ownership of the Service, and to the extent that Customer (or Tenant) becomes aware of any claims relating to the Service, Customer agrees to use reasonable efforts to promptly provide notice of any such claims to Entrust (and Tenant agrees to notify it's MSP to assist in this regard).

7.6. Tenant Agreements. Notwithstanding that each Tenant shall accept the Agreement, MSP will enter into a Tenant Agreement with each of its Tenants which will be at least as protective of Entrust (and its Affiliates, licensors, suppliers and hosting providers) and the Service as the terms and conditions of the Agreement. Tenant Agreement will: (i) not make any representation or warranty on behalf of Entrust (and its Affiliates, licensors, suppliers and hosting providers) or create or purport to create any obligation or liability on Entrust (and its Affiliates, licensors, suppliers and hosting providers); (ii) disclaim any and all liability on behalf of Entrust (and its Affiliates, licensors and suppliers); (iii) name Entrust (and its Affiliates, licensors, suppliers and hosting providers) and their respective officers, directors, employees, and contract workers as indemnified parties in any indemnification obligation benefiting MSP; (iv) make Entrust (and its Affiliates, licensors, suppliers and hosting providers) third-party beneficiaries to the clauses implementing (ii) and (iii) above; and (v) cause Tenant to provide all appropriate notices to Users and obtain from the Users all necessary consents required for MSP to meet its obligations to Entrust under the Agreement. MSP will comply with all requirements relating to onboarding of Tenants as set out in the Documentation. If MSP agrees to the terms and conditions of the Agreement on behalf of a Tenant (e.g. an MSP administrator clicks the "I Accept", "Start Trial" or similar button, and/or checks the box presented with these Terms of Service), MSP represents and warrants that it has legal authority to bind such Tenant, and shall ensure that Tenant is made aware of and complies with all the applicable terms and conditions in the Agreement.

7.7. No Hazardous Environments. Customer (or Tenant) acknowledges and agrees that neither the Service nor the Tokens are sufficiently fault-tolerant for life-safety operations, and neither is designed, manufactured, or intended for use in or in conjunction with control equipment in hazardous environments, including without limitation the operation of nuclear facilities, aircraft navigation or critical communications systems, air traffic control, transportation control, or life support devices. Customer (or Tenant) will not use the Service or Tokens for any purpose listed in this Section 7.7 *(No Hazardous Environments)* and any attempt to do so will be at Customer's (or Tenant's) own risk.

8. IP & FEEDBACK.

8.1. IP Rights in the Service. Except for the limited licenses and rights granted pursuant to the Agreement, Entrust retains all right, title, and interest in and to the Service, including, without limitation, in and to the Licensed Software used to provide the Service, and all graphics, user interfaces, logos, and trademarks reproduced through the Service.

8.2. Feedback. "Feedback" refers to Customer's, Tenants', and/or Users' suggestions, comments, or other feedback about the Service or other Entrust products and services. Even if designated as confidential, Feedback will not be subject to any confidentiality obligations binding Entrust. Customer (or Tenant) hereby agrees that Entrust will own all Feedback and all associated intellectual property rights in or to Feedback, and Customer (or Tenant) hereby assigns (and will cause all Tenants and/or Users to assign) to Entrust all of Customer's, Tenants', and Users' right, title, and interest thereto, including without limitation intellectual property rights.

9. CONFIDENTIAL INFORMATION.

9.1. Nondisclosure. During the Term and for a period of three (3) years thereafter, Receiving Party will not use Confidential Information (both as defined in Section 1.9) for any purpose other than as reasonably required in connection with the Service and/or the Agreement (the "Purpose"). Receiving Party: (a) will not disclose Confidential Information to any employee or contractor of Receiving Party unless such person needs access in order to facilitate the Purpose and is bound by confidentiality obligations with Receiving Party that are no less restrictive than those of this Article 9 *(Confidential Information)* and Receiving Party remains responsible for its employees' or contractors' compliance with the confidentiality obligations set forth in this Section 9.1 *(Nondisclosure)*; and (b) will not disclose Confidential Information to any other third party without the prior written consent of Disclosing Party (as defined in Section 1.9). Without limiting the generality of the foregoing, Receiving Party will protect Confidential Information with the same degree of care it uses to protect its own confidential information of similar nature and importance, but with no less than reasonable care. Receiving Party will promptly notify Disclosing Party of any misuse or misappropriation of Confidential Information that comes to Receiving Party's attention. Notwithstanding the foregoing, Receiving Party may disclose Confidential Information as required by applicable law or by proper legal or governmental authority. Receiving Party will give Disclosing Party prompt notice of any such legal or governmental demand and reasonably cooperate with Disclosing Party in any effort to seek a protective order or otherwise contest such required disclosure, at Disclosing Party's expense. For purposes of this Article 9 *(Confidential Information)*, receipt and/or disclosure by a party's Affiliate (or in the case of an MSP, by one of its Tenants) shall be deemed receipt and/or disclosure by such party.

9.2. Exclusions. Confidential Information does not include information that: (a) entered the public domain other than as a result of the act or omission of Receiving Party or a breach of the Agreement; (b) was in the public domain at the time of disclosure; (c) was received from a third party without a duty of confidentiality to the Disclosing Party; or (d) by written evidence, was known to or developed by the Receiving Party independent of and without access to, or reliance on the Disclosing Party's Confidential Information.

9.3. Injunction. Receiving Party agrees that breach of this Article 9 *(Confidential Information)* may cause Disclosing Party irreparable injury, for which monetary damages would not provide adequate compensation, and that in addition to any other remedy, Disclosing Party may be entitled to injunctive relief against such breach or threatened breach, without proving actual damage or posting a bond or other security.

9.4. Return. Upon termination or expiry of the Agreement, Receiving Party will return all copies of Confidential Information to Disclosing Party or certify, in writing, the destruction thereof.

10. REPRESENTATIONS & WARRANTIES.

10.1. Warranty Disclaimers. EXCEPT TO THE EXTENT SET FORTH IN THE SLA AND SECTION 14.9 (*HARDWARE*), CUSTOMER (OR TENANT) ACCEPTS THE SERVICE, THE TOKENS (IF ANY), AND ANYTHING ELSE PROVIDED IN CONNECTION WITH THE AGREEMENT "AS IS" AND AS AVAILABLE. ENTRUST AND ITS AFFILIATES, LICENSORS, SUPPLIERS, AND HOSTING PROVIDERS DISCLAIM ANY AND ALL REPRESENTATIONS, CONDITIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF NON-INFRINGEMENT, TITLE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR SATISFACTORY QUALITY, OR ANY IMPLIED

REPRESENTATIONS, CONDITIONS OR WARRANTIES ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. ENTRUST AND ITS AFFILIATES, LICENSORS, SUPPLIERS, AND HOSTING PROVIDERS MAKE NO REPRESENTATIONS, CONDITIONS OR WARRANTIES REGARDING ANY THIRD-PARTY SOFTWARE OR THIRD-PARTY SERVICE (INCLUDING ANY THIRD-PARTY CLOUD SERVICE) WITH WHICH THE SERVICE MAY INTEROPERATE (INCLUDING, WITHOUT LIMITATION, BY WAY OF AN EXTENSION OR A THIRD-PARTY INTEGRATION). WITHOUT LIMITING THE GENERALITY OF THE FOREGOING: (A) ENTRUST AND ITS AFFILIATES, LICENSORS, SUPPLIERS, AND HOSTING PROVIDERS DO NOT REPRESENT OR WARRANT THAT THE SERVICE WILL PERFORM WITHOUT INTERRUPTION OR ERROR; AND (B) ENTRUST AND ITS AFFILIATES, LICENSORS, SUPPLIERS, AND HOSTING PROVIDERS DO NOT REPRESENT OR WARRANT THAT THE SERVICE IS SECURE FROM HACKING OR OTHER UNAUTHORIZED INTRUSION OR THAT, WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, AUTHENTICATION RECORDS, CUSTOMER DATA, PROFILES, PERSONAL DATA, WILL REMAIN PRIVATE OR SECURE.

11. INDEMNIFICATION.

11.1. Indemnification by Customer. Customer will indemnify, defend and hold harmless Entrust and its Indemnified Associates (as defined below in Section 11.3 (*Litigation & Additional Terms*)) from and against any and all Claims, arising out of or related to: (i) Customer's (or Tenants') breach of the Agreement; (ii) Authentication Records, Customer Data, Profiles, Personal Data; or (iii) Customer's (or Tenants') alleged or actual use of, misuse of, or failure to use the Service, including, without limitation: (a) Claims by Tenants, Users, or by Customer's or Tenants' employees, subcontractors, agents, or customers; (b) Claims related to unauthorized disclosure or exposure of Authentication Records, Customer Data, Profiles, or Personal Data; (c) Claims related to infringement, misappropriation or violation of a copyright, trademark, trade secret, or privacy or confidentiality right by written material, images, logos or other content uploaded to the Service through the Customer Account, including, without limitation, in Customer Data, Profiles, or in any Customer or Tenant branding; and (d) Claims related to the injury to or death of any individual, or any loss of or damage to real or tangible personal property, caused by the act or omission of Customer, Tenants, Users, and/or any Customer's or its Tenants' employees, subcontractors or agents. Notwithstanding the foregoing, Customer will have no obligation to indemnify, defend and hold harmless Entrust and its Indemnified Associates from any Claim covered by Section 11.2 (*Indemnification by Entrust*) below.

11.2. Indemnification by Entrust. Entrust will defend Customer and Customer's Indemnified Associates against any and all Claims (excluding any Claims by Customer Affiliates, Tenants, Tenant Affiliates, and/or any Users) brought against Customer or Customer's Indemnified Associates alleging that the Service infringes any third-party intellectual property rights. Entrust will pay any damages finally awarded by a court of competent jurisdiction against Customer and Customer's Indemnified Associates or settled by agreement which are attributable to such Claim. Entrust obligations set for in this Section 11.2 (*Indemnification by Entrust*) do not apply to the extent that the Claim arises from: (i) Customer's (including Customer's Indemnified Associates) or a Tenant's breach of the Agreement, (ii) the Service being used in an manner not authorized pursuant to the Agreement, or being used in a manner or for a purpose other than that for which it was supplied, as contemplated by the Documentation; (iii) the Service having been modified without the written consent of Entrust; (iv) the combination of the Service with hardware or software not provided by Entrust (to the extent the Claim was related to such combination); (v) the use of any version of the Service other than the current, unaltered release, if such Claim would have been avoided by the use of a current unaltered release of the Service; (vi) any third-party software, third-party service or other third-party product on which

the Service relies (e.g. hosting provider). The foregoing states Entrust's entire liability and Customer's sole and exclusive remedy with respect to any infringement or misappropriation of any intellectual property rights of any kind. This Section 11.2 (*Indemnification by Entrust*) and Section 11.4 (*Mitigation by Entrust*) will not apply to any Service provided (or licensed) for no fee including, without limitation, any free trial or evaluation of the Service pursuant to Article 4 (*Evaluation*).

11.3. Litigation & Additional Terms. The obligations of the indemnifying party pursuant to this Article 11 (*Indemnification*) include retention and payment of attorneys and payment of costs and expenses, as well as settlement at the indemnifying party's expense. The indemnified party or Indemnified Associate(s) must provide the indemnifying party prompt notice of the Claim and agree to reasonably to cooperate and provide assistance (at indemnifying party's sole expense) in the defense; provided that failure by the indemnified party to provide prompt notice will relieve the indemnifying party of its obligations only to the extent that the indemnifying party was actually and materially prejudiced by such failure. The indemnifying party will control the defense of any Claim, including appeals, negotiations, and any settlement or compromise thereof; provided that the indemnified party and Indemnified Associates will have the right to reject any settlement or compromise that requires that it or they admit wrongdoing or liability or that subjects it or them to any ongoing affirmative obligations. Entrust, Customer, and/or their respective Indemnified Associates may participate in the defense of any Claim for which they are indemnified under this Article 11 (*Indemnification*) at their sole expense.

11.4. Mitigation by Entrust. If (i) Entrust is subject to (or is believes it may become subject to) an actual or potential Claim, or (ii) Customer (or Tenant) provides Entrust with notice of an actual or potential Claim, Entrust may, at its sole option: (i) procure for Customer the right to continue to use the affected portion of the Service; (ii) modify or replace the affected portion of the Service with functionally equivalent or superior software so that Customer's use is non-infringing; or (iii) if (i) or (ii) are not commercially reasonable, terminate the Customer's license or access to the affected Service and refund to Customer any associated pre-paid subscription fees for the affected portion of the Service on a pro-rata basis.

12. LIMITATION OF LIABILITY.

12.1. Exclusion. IN NO EVENT WILL ENTRUST BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR EXEMPLARY DAMAGES (INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA OR COSTS OF REPROCUREMENT) ARISING OUT OF OR IN CONNECTION WITH THE AGREEMENT AND THE SERVICE AND/OR TOKENS PROVIDED THEREUNDER.

12.2. Dollar Cap. ENTRUST'S TOTAL CUMULATIVE LIABILITY TO CUSTOMER (OR TENANT), ARISING OUT OF OR IN CONNECTION WITH THE AGREEMENT, AND THE SERVICE AND/OR TOKENS PROVIDED THEREUNDER WILL NOT EXCEED THE FEES PAID TO ENTRUST BY CUSTOMER (OR BY AN AUTHORIZED RESELLER, AS APPLICABLE) FOR THE SERVICE AND/OR TOKENS FROM WHICH THE LIABILITY AROSE IN THE TWELVE MONTHS PRIOR TO THE MONTH IN WHICH THE LIABILITY AROSE.

12.3. Clarifications & Disclaimers. THE LIABILITIES LIMITED BY ARTICLE 12 *(LIMITATION OF LIABILITY)* APPLY: (a) TO LIABILITY FOR NEGLIGENCE; (b) REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, STRICT PRODUCT LIABILITY, OR OTHERWISE; (c) EVEN IF ENTRUST IS ADVISED IN ADVANCE OF THE POSSIBILITY OF THE DAMAGES IN QUESTION AND EVEN IF SUCH DAMAGES WERE FORESEEABLE; AND (d) EVEN IF CUSTOMER'S REMEDIES (OR TENANT'S REMEDIES, IF ANY) FAIL OF THEIR ESSENTIAL PURPOSE. If applicable laws, rules or regulations limit the application of the provisions of Article 12

(Limitation of Liability), Entrust's liability will be limited to the maximum extent permissible. For the avoidance of doubt, Entrust's liability limits and other rights set forth in this Article 12 *(Limitation of Liability)* apply likewise to Entrust's Affiliates, and their respective licensors, suppliers, hosting providers, agents, directors, officers, employees, consultants, and any other representatives.

13. TERM, TERMINATION & SUSPENSION.

13.1. Term. The Agreement will commence on the Effective Date and, unless otherwise terminated pursuant to the Agreement, will expire on either the date the Trial Period ends, or, the date the applicable subscription term referenced in the Order or Order Form for the Service expires, whichever is later (the "**Term**").

13.2. Termination or Suspension for Cause. Entrust may, at its sole discretion, suspend or terminate Customer's, Tenants', and/or Users' access to the Service at any time, without advanced notice, if: (a) Entrust reasonably concludes that Customer, Tenants, and/or Users have conducted themselves in a way (i) that is not consistent with or violates the requirements of the AUP, the Documentation, or is otherwise in breach of the Agreement; or (ii) in a way that subjects Entrust to potential liability or interferes with the use of the Service by other Entrust customers, tenants, and/or users; (b) Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including, without limitation, the security of other Entrust customers', tenants', and/or users' information or data processed by the Service; or (c) Entrust reasonably concludes that Customer, Tenants, and/or Users are violating applicable laws, rules or regulations. Entrust may also, without notice, suspend Customer's, Tenants', and/or User's access to the Service for scheduled or emergency maintenance. Termination of the Agreement will result in termination of all Orders and Order Forms. Termination of the Agreement in relation to a particular MSP shall also result in the immediate termination of the Agreement in relation to all of their respective Tenants.

13.3. Effects of Termination. Upon termination or expiration of the Agreement, all applicable licenses and access rights will immediately terminate, and where no other Orders or Order Forms are in place, Customer (or Tenant) will cease all use of the Service, and delete, destroy, or return all copies of Entrust's Confidential Information, the Documentation, and Licensed Software in its possession or control. The following provisions in these Terms of Service will survive termination or expiration of the Agreement: Articles and Sections 3.2 (*Restrictions on Software Rights*), 8 (*IP & Feedback*), 9 (*Confidential Information*), 10 (*Representations & Warranties*), 11 (*Indemnification*), 12 (*Limitation of Liability*) and 14 (*Miscellaneous*); and any other provision in these Terms of Service that must survive to fulfill its essential purpose. Termination is without prejudice to any right or remedy that may have accrued or be accruing to either party prior to termination. Termination will not relieve Customer (directly or through an Authorized Reseller) from any obligation to pay Entrust any and all fees or other amounts due under the Agreement.

14. MISCELLANEOUS.

14.1. Conflicts. In the event of a conflict or differences between the Terms of Service, Special Terms and Conditions, an Order or Order Form, and any additional agreements, policies, or terms and conditions referenced therein ("Additional Documents"), the order of precedence shall be as follows:

(a) Special Terms and Conditions (including any Additional Documents incorporated by reference);
(b) Terms of Service (including any Additional Documents incorporated by reference); and
(c) Order or Order Form, as applicable.

Where any conflict occurs between the provisions contained in two or more of the above classes of document the document lower in the order of precedence shall where possible be read in such a way as to resolve such conflict. An omission, whether deliberate or inadvertent, is not by itself to be

construed as giving rise to a conflict.

14.2. Independent Contractors. The parties are independent contractors and will so represent themselves in all regards. Neither party is the agent of the other, and neither party may make commitments on the other party's behalf. The parties agree that no Entrust employee or contractor is or will be considered an employee of Customer (or Tenant).

14.3. Publicity. Customer (or Tenant) agrees to participate in Entrust's press announcements, case studies, trade shows, or other marketing reasonably requested by Entrust. During the Term and for thirty (30) days thereafter, Customer (or Tenant) grants Entrust the right, free of charge, to use Customer's (or Tenant's) name and/or logo, worldwide, to identify Customer (or Tenant) as such on Entrust's website or other marketing or advertising materials.

14.4. Third Party Software. Versions of certain open source third-party software may be embedded in the Licensed Software or Tokens ("Ancillary Software"). If Ancillary Software is included with the Licensed Software or Tokens, then a separate agreement will apply to Customer's (or Tenant's) use of the Ancillary Software. Upon request Entrust will provide Customer a list of Ancillary Software included with the Licensed Software or Tokens and corresponding open source licenses.

14.5. Extensions and Third-Party Integrations. Customer's (or Tenant's) use of any Extension shall be subject to a separate end user license agreement (or other applicable agreement) between Customer (or Tenant) and Entrust (or one of its Affiliates). Customer's (or Tenant's) use of any Third-Party Integration shall be subject to the separate end user license agreement (or other applicable agreement) between Customer (or Tenant) with the relevant third party (e.g. service provider that provides the service which is the subject of the Third-Party Integration).

14.6. Inclusion of Entrust Affiliates. Entrust may use one or more Affiliate(s) to perform its obligations under the Agreement, provided that such use will not affect Entrust's obligations hereunder.

14.7. Customer Using Service Provider Functionality for its Affiliates. Where Entrust enables and Customer chooses to utilize the "service provider" functionality in respect of Customer Affiliates, (i) Customer will be permitted to allocate the aggregate number of User entitlements set out on the Order or Order Form between Customer and its Affiliates, and (ii) each of Customer's Affiliates to which subscriptions are allocated will be deemed to be the Customer for purposes of the Agreement and bound by the terms and conditions of the Agreement as if such Affiliate was Customer itself. Customer agrees to be jointly and severely liable for the performance (or lack thereof) of the Agreement by each such Affiliate including, without limitation, any breach of the Agreement, any and all indemnification obligations contained within the Agreement, and any and all acts or omissions of each such Affiliate as if such actions or omission has been performed by Customer itself. Customer will provide Entrust with prior written notice before adding any Affiliate. Such notice will include each Affiliate's full corporate name and address as well a point of contact within the Affiliate. To the extent Entrust requires additional information about an Affiliate or their usage of the Service including, without limitation, as part of a lawful access request or subpoena, Customer will make best efforts in co-operating with Entrust. Customer will remain responsible for payment for all fees set out on its Order or Order Form. Tenants are not permitted to utilize the "service provider" functionality without express written consent from Entrust, which may be withheld in Entrust's sole discretion.

14.8. Third-Party Service Providers. Customer (or Tenant) consents to, and will obtain all Tenants' and/or Users' consents necessary for, Entrust's use of third-party service providers, including, without limitation, hosting providers (who may further utilize subcontractors) in the provision of the Service. Customer (or Tenant) acknowledges and agrees that Authentication Records, Customer Data,

Profiles, Personal Data, and Service Data, may be transmitted to, processed by and/or reside on computers operated by the Entrust authorized third parties (e.g. Entrust's hosting providers) who perform services for Entrust. These third parties may use or disclose such Authentication Records, Customer Data, Profiles, Personal Data, and Service Data to perform the Service on Entrust's behalf or comply with legal obligations. Unless otherwise required by applicable laws, rules or regulations, and without limiting the generality of Article 12 (*Limitations of Liability*), Entrust shall have no responsibility or liability for Customer's (or Tenant's) failure to obtain any of the consents or disclosures described in this Section 14.8 *(Third Party Service Providers)*.

14.9. Hardware. If an Order calls for Tokens (or if Customer purchases Tokens through an Authorized Reseller), A) Customer will be the importer of record and responsible for all freight, packing, insurance and other shipping-related expenses, B) risk of loss and title to the Tokens will pass to Customer upon delivery of the Tokens by Entrust (or an Authorized Reseller) or one of their respective agents to the carrier, C) the Tokens will be free from material defects in materials and workmanship and will conform to the published specifications for such Tokens in effect as of the date of manufacture for a period of one (1) year from the date on which such Tokens are first delivered to Customer, D) Customer will use Entrust as Customer's point of contact for Token warranty inquiries, and E) as an express condition of the sale, Customer (or Tenant) acknowledges that Customer (or Tenant) is only permitted to use Tokens with the Service, and Customer (or Tenant) is expressly prohibited from using and agrees not to use Tokens with any other third-party provider's verification or identification software even if the Tokens may interoperate with such other provider's verification or identification software. The aforementioned Token warranty will not apply where the issue is caused by accident, misuse, abuse, improper operation, misapplication, or any other cause external to the Token. Any Token that is replaced becomes the property of Entrust. Entrust's exclusive liability and Customer's (or Tenant's) exclusive remedy for breach of this Section 14.9 is for Entrust at its option to repair or replace the Token, or take return of the Token and refund the price paid for the Token. If, in conjunction with the Service, any Entrust or third-party hardware (other than a Token) is sold and distributed by Entrust (including through an Authorized Reseller), such hardware will be sold and distributed pursuant to the applicable Entrust or third-party shrink-wrap/clickwrap agreement which accompanies or is embedded in such Entrust or third-party hardware product.

14.10. Notices. All notices to Entrust under the Agreement will be in writing and will be personally delivered or sent by certified or registered mail (return receipt requested) and will be deemed to have been duly given when received at 1000 Innovation Drive, Kanata, Ontario, K2K 3E7 (or such alternate address as may be provided to Customer in writing). All notices to Customer under the Agreement will be provided electronically or by certified or registered mail (return receipt requested) to Customer at the addresses which Customer has provided to Entrust and will be deemed to have been duly given when sent. For Entrust, all notices must be sent Attention: Legal Department. Any notices to Tenants under the Agreement shall be deemed duly given by Entrust providing MSP such notice.

14.11. Force Majeure. No delay, failure, or default, other than a failure to pay fees when due, will constitute a breach of the Agreement to the extent caused by acts of war, terrorism, hurricanes, earthquakes, other acts of God or of nature, strikes or other labor disputes, riots or other acts of civil disorder, embargoes, or other causes beyond the performing party's reasonable control.

14.12. Assignment & Successors. Customer (or Tenant) may not assign, transfer or sublicense the Agreement or any of its rights or obligations thereunder without Entrust's express written consent. An assignment will be deemed to include any merger of Customer (or Tenant) with another party, whether or not Customer (or Tenant) is the surviving entity, the acquisition of more than 50% of any class of Customer's (or Tenant) voting stock by another party, or the sale of more than 50% of Customer's (or

Tenant's) assets. Except to the extent forbidden in this Section 14.12 *(Assignment & Successors)*, the Agreement will be binding upon and inure to the benefit of the parties' respective successors and assigns.

14.13. Severability. To the extent permitted by applicable law, the parties hereby waive any provision of law that would render any clause of the Agreement invalid or otherwise unenforceable in any respect. In the event that a provision of the Agreement is held to be invalid or otherwise unenforceable, such provision will be interpreted to fulfill its intended purpose to the maximum extent permitted by applicable law, and the remaining provisions of the Agreement will continue in full force and effect.

14.14. No Waiver. Neither party will be deemed to have waived any of its rights under the Agreement by lapse of time or by any statement or representation other than by an authorized representative in an explicit written waiver. No waiver of a breach of the Agreement will constitute a waiver of any other breach of the Agreement.

14.15. Choice of Law & Jurisdiction: If Customer is located in the United States, the Agreement will be governed solely by the internal laws of the State of Minnesota, United States, otherwise the Agreement will be governed solely by the internal laws of the Province of Ontario, Canada, in either case including, without limitation, applicable federal law, without reference to or application of: (a) any conflicts of law principle that would apply the substantive laws of another jurisdiction to the parties' rights or duties; (b) the United Nations Convention on Contracts for the International Sale of Goods; (c) the Uniform Computer Information Act, or (c) other international laws. If Customer is located in the United States, the parties consent to the personal and exclusive jurisdiction of the federal courts and Minnesota state courts located in Hennepin County, Minnesota, United States. Otherwise, the parties consent to the personal and exclusive jurisdiction of the federal courts and Ontario provincial courts located in Ottawa, Ontario, Canada. This Section 14.15 (*Choice of Law & Jurisdiction*) governs all claims arising out of or related to the Agreement, including without limitation tort claims. Tenants shall be subject to the same choice of law and jurisdiction as their MSP.

14.16. Construction. The parties agree that the terms and conditions of the Agreement result from negotiations between them, and shall not be construed in favor of or against either party by reason of authorship.

14.17. U.S. Government End-Users. The Licensed Software and Documentation are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If the Licensed Software and Documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 227.7202-4 (for Department of Defense licenses only) and 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to the Licensed Software and Documentation are limited to the commercial rights and restrictions specifically granted in the Agreement. The rights limited by the preceding sentence include, without limitation, any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the Licensed Software and Documentation. This Section 14.17 (*U.S. Government End-Users*) does not grant Customer (or Tenant) any rights not specifically set forth in the Agreement. Customer (or Tenant) shall not remove or deface any legal notice appearing in the Licensed Software or Documentation or on any packaging or other media associated with the Licensed Software or Documentation.

14.18. Technology Export. Customer (or Tenant) will comply in all respects with any and all applicable laws, rules and regulations and obtain all permits, licenses and authorizations or certificates that may be required in connection Customer's (or Tenant's) use of the Service. In addition,

(a) Customer (or Tenant) represents and warrants that:

(i) they are not located in, under the control of, or a national or resident of any country to which the export of the Licensed Software or Documentation would be prohibited by the applicable laws, rules or regulations of the United States or Canada or other applicable jurisdiction;

(ii) they are not an individual to whom the export of the Licensed Software or Documentation would be prohibited by the laws of the United States or Canada or other applicable jurisdiction;

(iii) they have and will continue to comply with applicable laws, rules and regulations of the United States and Canada or other applicable jurisdiction and of any state, province, or locality or applicable jurisdiction governing exports of any product or service provided by or through Entrust.

(iv) they will not use the Service or the Tokens for any purposes prohibited by applicable laws, rules or regulations on exports, including, without limitation related to nuclear, chemical, or biological weapons proliferation;

(v) they are legally distinct from, not acting on behalf of, and not associated with any individuals or entities appearing on US or Canadian sanctions lists ("Blocked Persons"). "Associated" for purposes of the Agreement means the Customer (or Tenant) and/or their respective affiliates and subsidiaries are owned in the aggregate, directly or indirectly, fifty (50%) percent or more by one or more Blocked Persons, or the Blocked Person is an employee, executive, director, or other individual or entity exercising control, directly or indirectly, over the Customer and/or its Tenants. The US Treasury Department, Office of Foreign Assets Control ("OFAC") sanctions lists can be found at https://sanctionssearch.ofac.treas.gov/. The Canadian listed persons and sanctions lists can be found at https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/listed_persons-personnes_inscrites.aspx?lang=eng;

(vi) they are legally distinct from, and not an agent of any individuals or entities appearing on the US Department of Commerce, Bureau of Industry and Security ("BIS") Denied Persons List, Unverified List, and Entity List. BIS Denied Persons List can be found at https://www.bis.doc.gov/index.php/the-denied-persons-list, Unverified List can be found at https://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=15:2.1.3.4.28#ap15.2.744_122.6 and, the BIS's Entity List can be found at https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file; and

(vii) in the event any of the above statements and representations in (a) to (f) are incorrect or the Customer (or Tenant) engages in any conduct that is contrary to sanctions or export controls, any agreements, purchases order, performance of services, or other contractual obligations of Entrust are immediately terminated.

(b) If Customer is an MSP, it shall comply with all applicable export laws, rules and regulations relating to its assignment of Tenants and Users under its Customer Account. MSP shall not enter into support agreements with Blocked Persons or entities or persons prohibited under US or Canadian export control laws or regulations, including the Export Administration Regulations. Entrust products and services may never be provided to an entity or individual located or residing in Cuba, Iran, North Korea, Syria or the Crimea region of Ukraine. MSP shall notify Entrust

without undue delay if it becomes aware that it has entered into a support agreement in violation of any applicable sanctions or export control laws, rules and regulations. MSP shall also without undue delay take all steps necessary in order to mitigate any such violation.

14.19. Entire Agreement. The Agreement sets forth the entire agreement of the parties and supersedes all prior or contemporaneous writings, negotiations, and discussions with respect to its subject matter. Neither party has relied upon any such prior or contemporaneous communications. The parties acknowledge and agree that the terms and conditions of any Customer document (e.g. a purchase order), in either electronic or written form, issued by Customer to confirm Customer's purchase of the Service, shall not be binding upon the parties or in any way modify, amend, or supersede the terms and conditions of the Agreement and any such Customer document shall be deemed to incorporate the terms of the Agreement by reference.

14.20. Amendment. The Agreement may be amended by Entrust from time to time by posting a new version on its website, and such new version will become effective on the date it is posted except that if Entrust modifies the Agreement in a manner which materially reduces Customer's (or Tenant's) rights or increases Customer's (or Tenant's) obligations and such changes are not required for Entrust to comply with applicable laws, the changes will become effective sixty (60) days after Entrust provides Customer written notice of changes (email or posting notice at the Service portal to suffice as adequate notice). If Customer objects in writing during that sixty (60) day period, the changes to the Agreement will become effective at the end of Customer's current subscription term. Notwithstanding the foregoing, provisions of this Section 14.20 (*Amendment*), amendment of the AUP is governed by the AUP.

14.21. Insurance. MSP shall have and maintain in force appropriate insurance with reputable authorized insurers of good financial standing which shall cover the liability of MSP for the performance of its obligations under the Agreement. MSP shall provide to Entrust, upon written request from Entrust but not more than once in any twelve (12) month period, written confirmation from the arranging insurance brokers that such insurances are in effect. The provisions of any insurance or the amount of coverage shall not relieve MSP of any liability under the Agreement. It shall be the responsibility of MSP to determine the amount of insurance coverage that will be adequate to enable MSP to satisfy any liability in relation to the performance of its obligations under the Agreement.

SCHEDULE TO ENTRUST IDENTITY AS A SERVICE TERMS OF SERVICE

IDENTITY PROOFING

SPECIAL TERMS AND CONDITIONS

This Identity Proofing schedule ("Schedule") is attached to the Entrust Identity as a Service Terms of Service ("Terms of Service"). Capitalized terms not defined in Section 1 herein or elsewhere in this Schedule shall have the meaning set out in the Terms of Service. References to articles or sections herein shall be to articles or sections in this Schedule unless otherwise expressly stated. Provisions in this Schedule will prevail with respect to Identity Proofing (as defined herein) over any conflicting provision in the Terms of Service.

1. **DEFINITIONS.**

1.1. "Customer Application" means the application developed by Customer pursuant to the SDK License (as defined herein) to be used to access and use Identity Proofing.

1.2. "Customer Data", in addition to its meaning in the Terms of Service, with respect to Identity Proofing means Device Information, Risk Information, Identity Proofing Results, as well as data or information collected using the Customer Application.

1.3. "Database" means the centralized Global Intelligence Platform owned, operated and maintained by Entrust (or its service providers) which contains Device Information and associated information including Risk information.

1.4. "Device" means a particular computer, mobile phone, desktop, tablet or other computing device.

1.5. "Device Information" means a set of Device attributes and characteristics that are designed to identify a particular Device.

1.6. "Identity Proofing" means the identity proofing functionality which forms part of the Service (if selected by Customer and approved by Entrust in an Order).

1.7. "Identity Proofing SLA" means the Entrust's service level agreement specific to Identity Proofing, as set out in **Attachment A** to this Schedule.

1.8. "Response" means the recommendation, including Risk Information, returned by Identity Proofing about a Device which has been evaluated by Identity Proofing.

1.9. "Risk" means risk including, without limitation, transaction, abuse, reputation and fraud risk.

1.10. "Risk Information" means information relating to specific Risk(s).

1.11. "SDK License" means the Entrust Mobile ID Proofing SDK License through which Customer may obtain a license to use the Mobile ID Proofing software development toolkit. The SDK License is not a part of the Agreement.

1.12. "User" means any individual end user who accesses and/or uses Identity Proofing through the

Customer Account, via the Customer Application.

2. **USE OF IDENTITY PROOFING.**

2.1. Grant of License. Subject to Customer's compliance with the Agreement, Entrust grants to Customer, during the Schedule Term (as defined herein), a worldwide, non-exclusive, nontransferable, non-sub-licensable right to, all in accordance with the Documentation, provide its User(s) with access to and/or use of Identity Proofing, through the Customer Account, via the Customer Application:

2.1.1. for the purpose of authenticating the identity of a User, extracting identity information or data from the User's identity document(s), and sending authentication results (resulting from (i) through (iv) above) to Customer ("**Identity Proofing Results**"), and not for resale or any other commercial purpose;

2.1.2. for the purpose of collecting and processing Device Information and providing Responses to Customer.

2.2. Restrictions. Identity Proofing provided to Customer pursuant to the Agreement is licensed, not sold, and Customer receives no title to or ownership of Identity Proofing or any portion thereof. In addition to Customer's obligations set out in Section 7.1 (*Acceptable Use and Restrictions*) in the Terms of Service, unless otherwise expressly authorized elsewhere in this Schedule, Customer will not: (a) modify, translate, create derivative works from, distribute, publicly display, publicly perform, or sublicense Identity Proofing; (b) use Identity Proofing in any way forbidden by Section 7.1 (*Responsibilities and Restrictions)* below; (c) reverse engineer Identity Proofing, or decompile, disassemble, or otherwise attempt to derive any of Identity Proofing's source code (except to the extent such prohibition is contrary to applicable law that cannot be excluded by the agreement of the parties); or (d) attempt to circumvent or disable any restriction or entitlement mechanism that is present or embedded in Identity Proofing. Identity Proofing shall not be available: (i) to MSPs or Tenants; and/or (ii) for evaluation purposes.

2.3. Service Levels. The sole remedies for any failure of Identity Proofing are listed in the Identity Proofing SLA. Service credits issued pursuant to the Identity Proofing SLA, if any, will only be applied against the costs associated with Customer's (or Authorized Reseller's, if applicable) subsequent subscription renewal. Entrust is not required to issue refunds for or to make payments against such service credits under any circumstances.

3. **CUSTOMER DATA & PRIVACY.**

3.1. Service Regions. The Service Regions available for selection by Customer may be different for Identity Proofing than for the main components of the Service, depending on the nature of the Customer Data, Personal Data, or Service Data (and the related Entrust hosting provider). With respect to the Customer Data and Personal Data that Entrust may collect pursuant to Identity Proofing, Customer consents to the storage in and/or the transfer into, the Service Region(s) which the Customer has selected. Customer further grants to Entrust (or its Affiliates, and any of their respective applicable subcontractors and hosting providers), a world-wide, limited right, during the Schedule Term, to host, copy, transmit and display Customer Data and Personal Data as reasonably necessary for Entrust (or its Affiliates, and any of their respective applicable subcontractors and hosting providers) to provide Identity Proofing in accordance with the Agreement.

3.2. Excluded Data (Exception). Notwithstanding the provisions set out in Section 6.4 (*Excluded Data*) of the Terms of Service, Identity Proofing may involve the processing of Excluded Data. As such, Section 6.4 (*Excluded Data*) of the Terms of Service shall not apply with respect to any Excluded Data that is necessary or required in order for Entrust to provide Identity Proofing to Customer and its Users pursuant to the Agreement, but only to the extent necessary or required. Customer acknowledges and agrees that the provisions of Section 6.4 (*Excluded Data*) of the Terms of Service shall continue to apply in all other cases, and ALL other disclaimers, limitations and exclusions contained in the Terms of Service, including, without limitation, those set out in Articles and Sections 10.1 (*Warranty Disclaimers*), 11.1 (*Indemnification by Customer*), and 12 (*Limitation of Liability*) of the Terms of Service.

3.3. Consents; Accuracy; Rights. Customer represents and warrants that, before authorizing a User to use Identity Proofing and before providing Customer Data or Personal Data to Entrust, Customer will have provided and/or obtained the requisite rights, consents or permissions, and made all requisite disclosures (if any), to Users in accordance with all applicable laws, rules or regulations for the collection, use, and disclosure of the Customer Data or Personal Data contained therein, by Entrust (including any of its Affiliates, and any of their respective applicable subcontractors and hosting providers) in accordance with the Agreement. Customer further represents and warrants to Entrust that such Customer Data or Personal Data is accurate and up-to-date (and that Customer shall correct or update it as required), and that no Customer Data or Personal Data will violate or infringe (i) any third-party intellectual property, publicity, privacy or other rights; (ii) any applicable laws, rules or regulations or the AUP; or (iii) any third-party products or services terms and conditions. Customer will be fully responsible for any Customer Data or Personal Data submitted, uploaded, or otherwise provided to Identity Proofing by any User as if it was submitted, uploaded, or otherwise provided by Customer. Customer is solely responsible for the accuracy, content and legality of all Customer Data and Personal Data.

3.4. Rights in Customer Data and Personal Data. As between the parties, Customer will retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data and Personal Data provided to Entrust. Subject to the terms of the Agreement, Customer hereby grants to Entrust a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of and display the Customer Data and Personal Data contained therein solely to the extent necessary to provide Identity Proofing to Customer, and to sub-license such rights to any of Entrust's applicable subcontractors.

3.5. Rights in Certain Data (Device Reputation). As between the parties, Entrust owns and will retain all right, title and interest (including but not limited to any copyright, patent, trade secret, trademark or other proprietary and/or intellectual property rights) in and to Identity Proofing, and the Device Information, Database, and any Response. For clarity, the foregoing does not mean that Entrust owns or retains any right, title or interest in or to the data elements comprising the Device Information, the Database, or any Response. The foregoing is an acknowledgement that, as between the parties, Entrust will retain any right, title and interest it may have in the Device Information, Database, and any Response, as collective works. Customer acknowledges that the Device Information and the Database, as collective works, may be Confidential Information of Entrust.

4. CUSTOMER'S RESPONSIBILITIES, RESTRICTIONS & ACKNOWLEDGEMENTS.

4.1. Compliance with Laws. In addition to Section 7.3 (*Compliance with Laws*) of the Terms of Service, Customer represents, warrants and covenants that is shall (i) use commercially reasonable efforts to prevent unauthorized access to, or use of, Identity Proofing and shall notify Entrust as soon as possible if it becomes aware of any unauthorized access or use of Identity Proofing; (ii) use Identity

Proofing only for lawful purposes; (iii) not knowingly violate any law of any country with its use of Identity Proofing; and (iv) not knowingly violate the intellectual property rights of any third party with its use of Identity Proofing.

4.2. Users; Identity Proofing Access. . In addition to Section 7.4 (*Tenants; Users; Service Access*) of the Terms of Service, Customer is responsible and liable for: (a) handling, use, and/or consequences or impact of Results or Responses resulting from use of Identity Proofing (e.g. impact on User's credit rating or ability to open accounts or any other unfavorable impact).

5. TERM, TERMINATION & SUSPENSION.

5.1. Term. Unless otherwise specified in the Order that includes the subscription for Identity Proofing, this Schedule will commence on the date the Order is accepted by Entrust, and will remain effective for the subscription period specified for Identity Proofing in the Order, unless terminated earlier in accordance with the Agreement ("**Schedule Term**"). Upon expiration of the Schedule Term, Customer may elect to renew its subscription pursuant to this Schedule for an additional length of time, as set forth in an Order for renewal, in which case the Schedule Term for Identity Proofing will be extended to include such additional length of time upon payment of the applicable fees for the additional length of time, all as set out in the Order for renewal.

5.2. Termination or Suspension for Cause. Entrust may, at its sole discretion, suspend or terminate Customer's and/or Users' access to Identity Proofing at any time, without advanced notice, if: (a) Entrust reasonably concludes that Customer and/or Users have conducted themselves in a way (i) that is not consistent with or violates the requirements of the AUP, the Documentation, or is otherwise in breach of the Agreement; or (ii) in a way that subjects Entrust to potential liability or interferes with the use of Identity Proofing by other Entrust customers and/or users; (b) Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including, without limitation, the security of other Entrust customers' and/or users' information or data processed by Identity Proofing; or (c) Entrust reasonably concludes that Customer and/or Users are violating applicable laws, rules or regulations. Entrust may also, without notice, suspend Customer's and/or User's access to Identity Proofing for scheduled or emergency maintenance. Termination of this Schedule will not necessarily result in termination of the entire Agreement (e.g. if Customer has an Identity as a Service subscription then the Terms of Service and the applicable Order may still be active).

5.3. Effects of Termination. Upon termination or expiration of this Schedule, all applicable licenses and access rights granted hereunder will immediately terminate, and Customer (and its Users) will cease all use of Identity Proofing, and delete, destroy, or return all copies of Entrust's Confidential Information and Documentation in its possession or control (unless continued rights to use exist pursuant to the Agreement (e.g. if Customer continues to have an Identity as a Service subscription despite the termination or expiry to this Schedule). Entrust will delete, destroy, or return (at its option) all copies of Customer Data and Personal Data contained therein. The following provisions will survive termination or expiration of this Schedule: Sections 2.2 (*Restrictions*), 3.3. (*Consents; Accuracy; Rights*), 3.5 (*Rights in Certain Data (Device Reputation)*), 4.1 (*Compliance with Laws*), 4.2 (*Users; Identity Proofing Access*), 5.3 (*Effects of Termination*); and any other provision of this Schedule that must survive to fulfill its essential purpose. Termination is without prejudice to any right or remedy that may have accrued or be accruing to either party prior to termination. Termination will not relieve Customer (directly or through an Authorized Reseller) from any obligation to pay Entrust any and all fees or other amounts due under the Agreement.

ATTACHMENT A

TO SCHEDULE TO ENTRUST IDENTITY AS A SERVICE TERMS OF SERVICE
IDENTITY PROOFING
SPECIAL TERMS AND CONDITIONS

IDENTITY PROOFING SLA

Service Commitment
Entrust will use commercially reasonable efforts to make Identity Proofing available 99.8% of the time during any monthly billing cycle. In the event Identity Proofing does not meet the 99.8% target, Customer will be eligible to receive a Service Credit as described below.

Definitions. Capitalized terms not defined in Section 1 herein or elsewhere in this Attachment A shall have the meaning set out in the Schedule (or Terms of Service).

- "**Monthly Uptime Percentage**" is calculated by subtracting from 100% the percentage of minutes during the month in which Identity Proofing was unavailable. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Exclusion (as defined below).

- "**Service Credit**" is, for the purposes of this Attachment A, a dollar credit, calculated as set forth below, that will be credited by Entrust to Customer's future invoices.

Service Credits
Service Credits are calculated based on the number of transactions that could have been processed during the downtime x the transaction fee that would have been paid by Customer if those transactions had been processed.

If the downtime is less than a full hour:
Step 1 – Calculate the Number of Transactions Processed During the Previous Calendar Quarter. The number of transactions that could have been processed is calculated based on the total number of transactions actually processed by Entrust on Customer's behalf during the calendar quarter immediately preceding the date on which the downtime occurred.

Step 2 – Calculate the Total Number of Hours in the Calendar Quarter. Calculate the number of days in the calendar quarter and multiply by 24 hours per day.

Step 3 – Divide Step 1 by Step 2 to arrive at the average number of transactions processed per hour during the previous calendar quarter:

$$\frac{\text{Step 1}}{\text{Step 2}} = \text{Average Number of Transactions Processed Per Hour}$$

Step 4 – Divide the amount of actual downtime by 60 minutes to arrive at the pro rata amount of an hour that the downtime represents:

$$\frac{\text{Minutes of Downtime}}{60} = \text{Pro Rata Portion of 1 Hour Represented by the Downtime}$$

Step 5 – Multiply the result of Step 4 (the pro rata portion of 1 hour represented by the downtime) by the result of Step 3 (the average number of transactions processed per hour) to arrive at the number of transactions that could have been processed during the downtime:

Step 4 x Step 3 = the Number of Transactions that Could Have Been Processed During the Downtime

Step 6 – Multiply Step 5 by the appropriate fee set forth in the applicable Order.

Step 5 x Transaction Fee = Service Credit

A Service Credit will be issued for the amount arrived at in Step 6.

If the downtime is a full hour:
For any full hour of unavailability, the Customer will receive a Service Credit for the number of transactions that could have been processed in the hour (Step 3) multiplied by the Transaction Fee set forth in the applicable Order.

Example:

- **Step 1** = 5,000 transactions during the previous calendar quarter
- **Step 2** = 91 days in the calendar quarter x 24 hour/day = 2,184 hours during the quarter
- **Step 3** = 5,000 (Step 1) divided by 2,184 (Step 2) = 2.5 transactions processed per hour
- **Step 4** = Assume downtime = 65 minutes so 60 minutes is one full hour leaving 5 minutes for the balance of the calculation. Divide 5 minutes by 60 minutes = 8.3% of an hour is represented by the downtime
- **Step 5** = 8.3% (Step 4) x 2.5 transactions processed during an hour (Step 3) = 1 transaction when rounded up to a whole transaction
- **Step 6** = 1 (Step 5) x $1.00 (transaction fee per transaction) = Service Credit of $1.00
- **Step 7** = Service Credit for less than a full hour (Step 6) + average number of transactions processed per hour (Step 3) multiplied by the transaction fee per transaction or $1 transaction fee + (2.5 average hourly transactions x $1 transaction fee) = $3.5 Service Credit for 65 minutes of downtime

Credit Request and Payment Procedures
Within thirty (30) days of the end of the relevant calendar month, Customer must submit a written request to Entrust for a Service Credit, along with sufficient information for Entrust to verify the time(s) and date(s) of the event for which Customer is claiming a Service Credit. If the Monthly Uptime Percentage when

calculated by Entrust falls below the Uptime Guarantee, then Entrust will notify Customer that a Service Credit will be issued to Customer within one billing cycle following the month in which such request was confirmed by Entrust and the amount of the Service Credit. Customer's failure to request a Service Credit in a timely manner or provide sufficient information to Entrust that Entrust may reasonably request in order to verify the Monthly Uptime Percentage will disqualify Customer from receiving a Service Credit.

Exclusions

Exclusions shall not be included in the calculation of the time the Product was available in any given calendar month. As used herein, "**Exclusion**" shall mean any unavailability: (i) due to Entrust's planned maintenance or downtime the occurrence of which Customer received at least 24-hour advance written notice; (ii) caused by factors outside of Entrust's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Entrust's Product; (iii) that result from the Customer Application, or failure of equipment, software, technology or facilities provided by Customer, including but not limited to, network unavailability or bandwidth limitations outside of Entrust's network; (iv) that results from a failure of the device reputation functionality made available as part of Identity Proofing; or (v) arising from Entrust's suspension and termination of Customer's right to use Identity Proofing in accordance with the Agreement.