ENTRUST DATACARD INTELLITRUST TERMS OF SERVICE

This ENTRUST DATACARD INTELLITRUST TERMS OF SERVICE (this "Agreement") contains the terms and conditions that govern access to and use of the Service (as defined below) and is an agreement between Entrust, Inc. and you or the entity you represent ("Customer") if you or the entity you represent are located in the United States. Otherwise this is an agreement between Entrust Datacard Limited and Customer (Entrust, Inc or Entrust Datacard Limited, as applicable, to be referred to as "Entrust Datacard"). This Agreement takes effect when an "I Accept" button or check box presented with these terms is clicked (the "Effective Date"). The Agreement includes, the AUP, Privacy Statement, SLA, (all as defined below in Article 1 (*Definitions*)), and all such documents are incorporated by reference. You represent to us that you are lawfully able to enter into contracts (e.g., you are not a minor). If you are entering into the Agreement for an entity, such as the company you work for, you represent to us that you have legal authority to bind that entity.

Entrust Datacard has developed the IntelliTrust™ cloud-based authentication platform (the "Service") which consists of technology hosted on Entrust Datacard's (or its hosting provider's) computers and accessed remotely, via the cloud, as well as Licensed Software hosted on Customer's computers. Entrust Datacard desires to make the Service available to Customer for Customer's Internal Business Purposes (as defined in Section 2.1 (*Use of Service*)). Therefore, in consideration for the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

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

1.1. "Affiliates" means any corporation or other entity that a party directly or indirectly controls. A party "controls" a corporation or other entity if it owns fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control for the corporation or other entity.

1.2. "Authentication Record" means a record setting out the details of each authentication attempt made by a User.

1.3. "AUP" means Entrust Datacard's acceptable use policy, as may be modified from time to time, available on the Service portal.

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

1.5. "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. All Entrust Datacard financial information is Confidential Information whether or not it is so designated. Confidential Information does not include Customer Data.

1.6. "Customer's Clients" means any third party whom Customer allows to use the Service or to whom Customer gives access to the Service, including without limitation third party agents and employees.

1.7. "Customer Data" means any information (including without limitation data) about Users that is supplied to Entrust Datacard by or on behalf of Customer or any other User in connection with the Service (including without limitation, device and computer information). Customer Data may include Personal Information and does not include Service Data.

1.8. "Documentation" means Entrust Datacard's guides, manuals, instructions, policies and reference materials related to the Service, as may be modified from time to time.

1.9. "Internal Business Purpose" has the meaning set forth in Section 2.1 (*Use of Service*).

1.10. "Licensed Software" means Entrust Datacard's Enterprise Service Gateway software application (including updates and new versions Entrust Datacard provides to Customer).

1.11. "Order" means an order for the Service accepted by Entrust Datacard.

1.12. "Personal Information" means information about an identified or identifiable individual protected under the privacy and/or data protection legislation applicable in the individual's jurisdiction.

1.13. "Privacy Statement" means Entrust Datacard's Privacy Statement, as may be modified from time to time, available at www.entrust.com/privacy or by request at privacy@entrustdatacard.com.

1.14. "Profile" means User and device profiles constructed from authentication patterns and device-identifying technical data. Profiles may include data from third party service providers.

1.15. "Service Data" has the meaning set forth in Section 6.5 (*Profiles and Service Data*).

1.16. "SLA" means Entrust Datacard's standard Intellitrust service level agreement, as may be modified from time to time, available on the Service portal.

1.17. "Term" is defined in Section 13.1 (*Term*) below.

1.18. "Tokens" means the Entrust Datacard Identity Guard tokens (if any) specified in the Order.

1.19. "User" means any entity or individual who directly or indirectly uses (or otherwise accesses) the Service on Customer's behalf or through Customer's account, whether authorized or not including without limitation Customer and Customer's Clients and their respective employees and agents.

2. CLOUD COMPONENTS & USE OF THE SYSTEM IN GENERAL.

2.1. Use of the Service. Subject to Customer's compliance with its payment obligations and Customer's and User's compliance with Section 7.1 (*Acceptable Use and Restrictions*), during the Term, Customer may grant authorized Users access to and use of the Cloud Components in accordance with the Agreement in such quantities and for such duration(s) as are set forth on Customer Order(s). Access and use are for the sole purpose of conducting Customer's business operations, and not for resale or any other commercial purpose ("Internal Business Purposes").

2.2. Service Levels. The sole remedies for any failure of the Cloud Components are listed in the SLA. Credits issued pursuant to the SLA will only be applied against the costs associated with Customer's subsequent subscription renewal. Entrust Datacard is not required to issue refunds for or to make payments against such credits under any circumstances.

2.3. Documentation. Customer may reproduce and use the Documentation solely as necessary to support Users' access to and use of the Service.

2.4. Cloud Component Revisions. Entrust Datacard may add, reduce, eliminate or revise Service features and functionality at any time. Additionally, Entrust Datacard 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 Datacard will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice (email or posting notice at the Service portal to suffice as adequate notice).

2.5. Customer's Clients. Customer will make no representations or warranties regarding the Service or any other matter, to Users or any other third party, from or on behalf of Entrust Datacard, and Customer will not create or purport to create any obligations or liabilities for Entrust Datacard. Customer will be jointly and severally liable to Entrust Datacard for Users acts and omissions. Entrust Datacard will have no obligation to provide support or other services to Users.

3. LICENSED SOFTWARE.

3.1. License. Subject to Customer's compliance with its payment obligations for the Service and the restrictions set forth below in Section 3.2 (*Restrictions on Software Rights*), Entrust Datacard hereby grants Customer a personal, non-exclusive, non-transferable, non-sub-licensable license to during the Term install and use the Licensed Software in accordance with the Agreement, in object code form only, in such quantities and for such durations as set forth on Customer Order(s), as necessary for Customer's Internal Business Purposes and solely as a component of the Service.

3.2. Restrictions on Software Rights. Copies of the Licensed Software created or transferred pursuant to this Agreement are licensed, not sold, and Customer receives no title to or ownership of any copy or of the Licensed Software itself. Furthermore, Customer 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 will not: (a) modify, translate, create derivative works from, distribute, publicly display, publicly perform, or sublicense the Licensed Software; (b) use the Licensed Software in any way forbidden 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 Service.

3.3. Hosting and Management. Customer agrees to host and manage the Licensed Software in accordance with the Documentation. Entrust Datacard will have no responsibility or liability for any failure of the Service resulting from Customer's hosting and management of the Licensed Software.

4. EVALUATION.

4.1. Evaluation Access. In the event that Customer is only permitted to use the Service for evaluation purposes this Section 4.1(*Evaluation Access*), and not Sections 2.1(*Use of Service*) and 3.1 (*License*) will apply. Subject to Customer's compliance with Sections 3.2 (*Restrictions on Software Rights*) and, 7.1 (*Acceptable Use and Restrictions*), for thirty (30) days Customer may: (i) grant authorized Users

access to and use of the Cloud Components in such quantities as are set forth on the applicable Order for evaluation purposes only, (ii) use the Licensed Software in object code form only in such quantities as are set forth on the applicable Order, as necessary for Customer's evaluation of the Service.

4.2. Inapplicable Sections. Sections 2.2 (*Service Levels*), 11.2 (*Indemnification by Entrust Datacard*) and 11.4 (*Mitigation by Entrust Datacard*) do not apply to any Customer evaluation of the Service.

4.3. Termination or Suspension. Entrust Datacard may in its sole discretion suspend or terminate Customer's (or any of its User's) evaluation access to the Service at any time, for any or no reason, without advanced notice.

5. FEES.

5.1. Customer shall pay Entrust Datacard (or an authorized reseller as applicable) the fees (including where overages are permitted, any overage fees) for the Service pursuant Entrust Datacard's pricing schedule. Unless otherwise stated in the pricing schedule, Customer will pay all amounts payable under this Agreement within thirty (30) days of the date of the invoice. All amounts payable by Customer under this 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 Datacard's net income), fees, duties, or other similar governmental charges. Entrust Datacard may elect to charge Customer interest for late fees at the lesser of 1.5 percent (1.5%) per month or the maximum rate permitted by law.

6. CUSTOMER DATA & PRIVACY.

6.1. Use of Customer Data. The Service requires certain Customer Data in order to operate (e.g. user names, IP addresses, passwords and other login information). Customer instructs Entrust Datacard to process Customer Data in accordance with the terms and conditions of this Agreement and the Privacy Statement. Entrust Datacard will not access, collect, process, store, log or otherwise use Customer Data except as set out in its Privacy Statement or as necessary to: (a) provide, optimize, troubleshoot and maintain the Service, including to generate Authentication Records; or (b) generate Profiles and Service Data; or (c) comply with applicable laws, rules or regulations or a binding order of a governmental body. Entrust Datacard will process and store Customer Data and Authentication Records in accordance with Entrust Datacard's Information Security Policy, as may be modified from time to time, and is made available on the Service portal. Customer acknowledges that it has read such policy and agrees that the policy is adequate to protect Customer Data and store Authentication Records.

6.2. Service Regions. Notwithstanding anything that may be stated to the contrary in Entrust Datacard's Privacy Statement, Customer will select the geographic region(s) (each a "**Service Region**") where Customer Data and Authentication Records will be stored. Customer acknowledges and consents to the storage of Customer Data and Authentication Records in, and the transfer of Customer Data and Authentication Records into, the Service Region(s) which the Customer selects.

Notwithstanding the foregoing, Customer acknowledges: i) that Entrust Datacard 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. Authorized Disclosure or Movement of Customer Data. Notwithstanding anything that may be stated to the contrary in Entrust Datacard's Privacy Statement, unless Entrust Datacard is prohibited from doing so, Entrust Datacard will give Customer reasonable notice of any legal or governmental demand for disclosure or movement of Customer Data or Authentication Records, or redirect any such demand to Customer to allow Customer to seek a protective order or otherwise to contest such required disclosure at Customer's expense, prior to making any disclosure or movement.

6.4. Excluded Data. Customer represents and warrants that Customer Data does 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 Information 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 RECOGNIZES AND AGREES THAT: (i) ENTRUST DATACARD HAS NO LIABILITY FOR ANY FAILURE TO PROVIDE PROTECTIONS SET FORTH IN THE EXCLUDED DATA LAWS OR OTHERWISE TO PROTECT EXCLUDED DATA; AND (ii) ENTRUST DATACARD'S 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 and Service Data. Entrust Datacard owns all right, title and interest in and to Profiles and Service Data and for greater certainty may use, reproduce, sell, publicize, or otherwise exploit Profiles and Service Data in any way, in its sole discretion. "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 and other User's use of the Service (e.g., analytics data, statistics data and performance data). For the avoidance of doubt, nothing in the Privacy Statement shall be construed or interpreted as limiting Entrust Datacard's ability to exploit Service Data and/or Profiles in any manner or requiring any further consent or authorization by Customer or any User for Entrust Datacard's use, reproduction, etc. of Service Data and/or Profiles.

6.6. Consents. Customer represents and warrants that, before authorizing a User to use the Service and before providing Customer Data to Entrust Datacard, Customer will have obtained the requisite consents and made all requisite disclosures to Users, in accordance with all applicable laws, for the use of the Customer Data (in particular Personal Information), by Entrust Datacard, its subcontractors and its hosting providers in accordance with this Agreement and Entrust Datacard's Privacy Statement.

7. CUSTOMER'S RESPONSIBILITIES, RESTRICTIONS & ACKNOWLEDGEMENTS.

7.1. Acceptable Use and Restrictions. Customer will comply with the AUP. In addition to the restrictions in Section 3.2 (*Restrictions on Software Rights),* Customer will not: (a) rent, sell, lease, distribute, pledge, assign or otherwise transfer, or encumber rights to the Service, or any part thereof, or use the Service for service bureau or time-sharing purposes or in any other way allow third parties to

exploit the Service, except Customer's Clients as specifically authorized by this Agreement; (b) provide Service passwords or other log-in information to any third party, except Customer's Clients as specifically authorized by this Agreement; (c) share non-public Service features or content with any third party; (d) 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; (e) 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; (f) attempt to gain unauthorized access to, or disrupt the integrity or performance of, the Service or the data contained therein; or; (g) use the Service other than in accordance with this Agreement and in compliance with all applicable laws and regulations. In the event that Entrust Datacard suspects any breach of the requirements of this Section 7.1 *(Acceptable Use and Restrictions)*, including without limitation by Users, Entrust Datacard may suspend Customer's access to the Service without advanced notice, in addition to such other remedies as Entrust Datacard may have. Neither this Agreement nor the AUP requires that Entrust Datacard take any action against Customer or any User or other third party for violating the AUP, this Section 7.1 *(Acceptable Use and Restrictions)*, or this Agreement, but Entrust Datacard is free to take any such action it sees fit.

7.2. Unauthorized Access. Customer 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 Datacard 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.

7.3. Compliance with Laws. In its use of the Service and the Tokens, Customer will comply with all applicable laws, including without limitation laws governing the protection of Personal Information and other laws applicable to the protection of Customer Data.

7.4. Customer's Clients & Other Users; Service Access. Customer is responsible and liable for: (a) the configuration of the Service to meet its own (and its Users') requirements; (b) Customer Data and any other data uploaded to the Service by Customer and other Users; (c) Customer's and other Users' use of the Service, including without limitation unauthorized User conduct and any User conduct that would violate the AUP or the requirements of this Agreement applicable to Customer; and (d) any use of the Service through Customer's account, whether authorized or unauthorized. Entrust Datacard will have no responsibility or liability for the accuracy of data uploaded to the Service by Customer, including without limitation Customer Data and any other data uploaded by Users. Customer 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 this Agreement, including without limitation any import or export licenses required pursuant to Section 14.15 (*Technology Export*).

7.5. Customer Product EULA. Where Customers grant authorized Users access to and use of the Cloud Components, Customer will do so pursuant to a written agreement ("**End User License**") which contains terms and conditions that (i) only permit the use of the Cloud Components in combination with Customer products or systems, (ii) prohibit decompiling, reverse engineering or modification of the Cloud Components (except as and only to the extent any foregoing restriction is prohibited by applicable law), (iii) are at least as protective of the Service including without limitation the

intellectual property rights and Confidential Information of Entrust Datacard and its licensors as the terms and conditions of this Agreement, (iv) flow through the acknowledgements and obligations pursuant to Section 10.2 (*No Hazardous Environments*) and (v) disclaim, to the extent permitted by law, any liability or damages of Entrust Datacard (including its Affiliates, licensors and suppliers) to Users. Customer will not make any representations and/or warranties on behalf of Entrust Datacard, whether express, implied, statutory, or otherwise, including, without limitation, warranties of merchantability, fitness for a particular purpose, satisfactory quality, title, or non-infringement. Customer agrees to enforce Entrust Datacard' rights under Customers agreements with Users, in the same manner and to the same extent as Customer enforces its own rights thereunder or to allow Entrust Datacard to do so by naming it as a third party beneficiary in the end user license language that applies to Customer products or systems. Customer agrees to cooperate with Entrust Datacard to maintain Entrust Datacard's ownership of the Cloud Components, and to the extent that Customer becomes aware of any claims relating to the Cloud Components, Customer agrees to use reasonable efforts to promptly provide notice of any such claims to Entrust Datacard.

8. IP & FEEDBACK.

8.1. IP Rights in the Service. Entrust Datacard retains all right, title, and interest in and to the Service, including without limitation all Licensed Software used to provide the Service and all graphics, user interfaces, logos, and trademarks reproduced through the Service. This Agreement does not grant Customer any intellectual property license or rights in or to the Service or any of its components, except to the limited extent that this Agreement specifically sets forth Customer license rights to Licensed Software, or Documentation and access rights to the Cloud Components. Customer recognizes that the Service and its components are protected by copyright and other laws.

8.2. Feedback. "Feedback" refers to Customer's and its' End Users' and other employees' and contractors' suggestions, comments, or other feedback about the Service or other Entrust Datacard products and services. Even if designated as confidential, Feedback will not be subject to any confidentiality obligations binding Entrust Datacard. Customer hereby agrees that Entrust Datacard will own all Feedback and all associated intellectual property rights in or to Feedback, and Customer hereby assigns to Entrust Datacard all of Customer's 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 five (5) years thereafter, Receiving Party will not use Confidential Information (both as defined in Section 1.4 (*Confidential Information*)) for any purpose other than as reasonably required in connection with the Services and/or this Agreement (the "Purpose"). Receiving Party: (a) will not disclose Confidential Information to any employee or contractor (including any Entrust Datacard service provider) of Receiving Party unless such person needs access in order to facilitate the Purpose and is bound by confidentiality obligations with Customer that are no less restrictive than those of this Article 9 *(Confidential Information)* and Receiving Party remains responsible for its representatives' 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 1.4). 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)*, for Entrust Datacard, Receiving Party and Disclosing Party are deemed to include Entrust Datacard and its affiliates.

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 this 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 8 *(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 of this 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 14.7 (TOKENS), CUSTOMER ACCEPTS THE SERVICE, THE TOKENS, IF ANY, AND ANYTHING PROVIDED IN CONNECTION WITH THIS AGREEMENT "AS IS" AND AS AVAILABLE. ENTRUST DATACARD AND ITS SUPPLIERS 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 DATACARD MAKES NO REPRESENTATIONS, CONDITIONS OR WARRANTIES REGARDING ANY THIRD-PARTY SERVICE WITH WHICH THE SERVICE MAY INTEROPERATE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING: (A) ENTRUST DATACARD DOES NOT REPRESENT OR WARRANT THAT THE SERVICE WILL PERFORM WITHOUT INTERRUPTION OR ERROR; AND (B) ENTRUST DATACARD DOES NOT REPRESENT OR WARRANT THAT THE SYSTEM IS SECURE FROM HACKING OR OTHER UNAUTHORIZED INTRUSION OR THAT CUSTOMER DATA WILL REMAIN PRIVATE OR SECURE.

10.2. No Hazardous Environments. Customer 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 will not use the Service or Tokens for any purpose listed in this Section 10.2 *(No Hazardous*

Environments) and any attempt to do so will be at Customer's own risk.

11. INDEMNIFICATION.

11.1. Indemnification by Customer. Customer will indemnify, defend and hold harmless Entrust Datacard and its Indemnified Associates (as defined below in Section 11.3 (*Litigation & Additional Terms*)) from and against any and all third party claims, demands, suits, or proceedings (each a "Claim"), arising out of or related to Customer's breach of the Agreement, Customer Data, or Customer's alleged or actual use of, misuse of, or failure to use the Service, including without limitation: (a) Claims by Customer's Clients or other Users or by Customer's or Customer's Clients' employees or agents; (b) Claims related to unauthorized disclosure or exposure of Personal Information or other private information as well as Customer Data; (c) Claims related to infringement 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 Customer's account, including without limitation by Customer Data; and (c) 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 or of any of its agents, subcontractors, or employees. Notwithstanding the foregoing, Customer will have no obligation to indemnify, defend and hold harmless Entrust Datacard and its Indemnified Associates from any Claim covered by Section 11.2 (*Indemnification by Entrust Datacard*) below.

11.2. Indemnification by Entrust Datacard. Entrust Datacard will defend Customer and Customer's Indemnified Associates against any and all Claims brought against Customer or Customer's Indemnified Associates alleging that the Service infringes any valid third party intellectual property right. Entrust Datacard 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 Datacard's obligations set for in this Section 11.2 do not apply to the extent that the Claim arises from: (i) a breach of the Agreement, (ii) the Service being used in an manner not authorized pursuant to this 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 Datacard; (iv) the combination of the Service with hardware or software not provided by Entrust Datacard; (v) the use of any version of the Service other than the current, unaltered release, if such Indemnified Claim would have been avoided by the use of a current unaltered release of the Service; (vi) any third-party service, software or other product on which the Service relies (e.g. Amazon Web Services). The foregoing states Entrust Datacard'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 Datacard*) and Section 11.4 (*Mitigation by Entrust Datacard*) will not apply to any Services provided (or licensed) for no fee including without limitation any free trial or evaluation of the Service. For clarity, for purposes of Article 11 and 12, the Service includes the Licensed Software.

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 Indemnified 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 Datacard and/or Entrust Datacard's Indemnified Associates may participate in the defense of any Claim for which they are indemnified under this Article 11 at their sole expense. "Indemnified Associates" are officers, directors, shareholders, parents, subsidiaries, agents, successors, and assigns.

11.4. Mitigation by Entrust Datacard. If (i) Entrust Datacard is subject to (or is believes it may be come subject to) an actual or potential Claim, or (ii) Customer provides Entrust Datacard with notice of an actual or potential Claim, Entrust Datacard 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 subscription fee for the affected Service on a pro-rata basis.

12. LIMITATION OF LIABILITY.

12.1. Exclusion. IN NO EVENT WILL ENTRUST DATACARD 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 USE OF THE SERVICE AND/OR TOKENS OR THIS AGREEMENT.

12.2. Dollar Cap. ENTRUST DATACARD'S TOTAL CUMULATIVE LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, AND THE SERVICES AND/OR TOKENS PROVIDED HEREUNDER WILL NOT EXCEED THE FEES PAID TO ENTRUST DATACARD FOR THE SERVICE 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 DATACARD 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 FAIL OF THEIR ESSENTIAL PURPOSE. If applicable law limits the application of the provisions of Article 12 *(Limitation of Liability)*, Entrust Datacard's liability will be limited to the maximum extent permissible. For the avoidance of doubt, Entrust Datacard's liability limits and other rights set forth in this Article 12 *(Limitation of Liability)* apply likewise to Entrust Datacard's affiliates, licensors, agents, directors, officers, employees, consultants, and other representatives.

13. TERM, TERMINATION & SUSPENSION.

13.1. Term. This Agreement will commence on the Effective Date and unless otherwise terminated pursuant to this Agreement, will expire when the last Customer Order for the Service expires (the

"**Term**"). Customer can renew subscriptions by issuing a corresponding purchase order to Entrust Datacard prior to subscription expiration.

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

13.3. Effects of Termination. Upon termination of a Customer Order or this Agreement, all applicable licenses and access rights will immediately terminate, and where no other Orders are in place Customer will cease all use of the Service, and delete, destroy, or return all copies of Entrust Datacard's Confidential Information, the Documentation and Licensed Software in its possession or control. Entrust Datacard may retain Authentication Records for up to seven years following termination. The following provisions will survive termination or expiration of this 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 of this Agreement 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 from any obligation to pay Entrust Datacard any and all fees or other amounts due under this Agreement.

13.4. Support. If Customer's Order calls for support, any such support be will provided pursuant to the 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 reseller will provide support, then such support will be provided by the authorized reseller (and not Entrust Datacard).

14. MISCELLANEOUS.

14.1. Conflicts. In the event of any conflict among the main body of this Agreement and the attachments to this Agreement or the policies and other documents incorporated herein by reference, this main body will prevail.

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 may make commitments on the other's behalf. The parties agree that no Entrust Datacard employee or contractor is or will be considered an employee of Customer.

14.3. Publicity. Customer agrees to participate in Entrust Datacard's press announcements, case studies,

trade shows, or other marketing reasonably requested by Entrust Datacard. During the Term and for thirty (30) days thereafter, Customer grants Entrust Datacard the right, free of charge, to use Customer's name and/or logo, worldwide, to identify Customer as such on Entrust Datacard's website or other marketing or advertising materials.

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

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

14.6. Customer Using Service Provider Functionality for its Affiliates. Where Entrust Datacard enables and Customer chooses to utilize the "service provider" functionality in respect of its Affiliates, (i) Customer will be permitted to the allocate the aggregate number of subscriptions set out on its Order Form between Customer and its Affiliates, and (ii) each of Customer's Affiliates to which subscriptions are allocated will be deemed to be Customer for purposes of this Agreement and bound by the terms and conditions of this Agreement as if such Affiliate was Customer itself. Customer agrees to be jointly and severely liable for the performance (or lack thereof) of this Agreement by each of such Affiliates including, without limitation, any breach of this Agreement, any and all indemnification obligations contained within this 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 Datacard with prior written notice (email to suffice) before adding any Affiliate. Such notice will include each Affiliates 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 take best efforts in co-operating with Entrust Datacard. Customer will remain responsible for payment for all fees set out on its Order Form.

14.7. Third-Party Service Providers. Customer consents to and will obtain all Users' consents necessary for Entrust Datacard's use of third-party service providers, including without limitation the hosting provider (who may further utilize subcontractors) in the provision of the Service. Customer acknowledges and agrees that Customer Data and other data or information used by the Service may be transmitted to, processed by and/or reside on computers operated by the Entrust Datacard authorized third parties (e.g. Entrust Datacard's hosting provider, currently Amazon Web Services) who perform services for Entrust Datacard. These third parties may use or disclose such Customer Data to perform the Services on Entrust Datacard's behalf or comply with legal obligations. Entrust Datacard has no responsibility or liability for any of the consents or disclosures described in this Section 14.6 *(Third Party Service Providers)*.

14.8. Hardware. If Customer's Order calls for Tokens (or if Customer purchases Tokens through an Entrust Datacard 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 Datacard (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 Datacard as Customer's point of contact for Token warranty inquiries, and E) as an express condition of the sale, Customer acknowledge that Customer is only permitted to use Tokens and Tokens with the Services and Customer is expressly prohibited from using and agree not to use Tokens with any other 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 Datacard. If in conjunction with the Services, any third-party hardware is sold and distributed by Entrust Datacard (including through an authorized reseller), such hardware will be sold distributed pursuant to the applicable manufacturer's shrink-wrap/clickwrap agreement which accompanies or is embedded in such third party hardware product. Entrust Datacard's exclusive liability and Customer's exclusive remedy for breach of this Section 14.7 is for Entrust Datacard at its option is to repair or replace the Token, or take return of the Token and refund the price paid for the Token.

14.9. Notices. All notices to Entrust Datacard under this 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. All notices to Customer under this 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 Datacard and will be deemed to have been duly given when sent. For Entrust Datacard, all notices must be sent Attention: Legal Department.

14.10. Force Majeure. No delay, failure, or default, other than a failure to pay fees when due, will constitute a breach of this 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.

14.11. Assignment & Successors. Customer may not assign, transfer or sublicense this Agreement or any of its rights or obligations hereunder without Entrust Datacard's express written consent. An assignment will be deemed to include any merger of Customer with another party, whether or not Customer is the surviving entity, the acquisition of more than 50% of any class of Customer's voting stock by another party, or the sale of more than 50% of Customer's assets. Except to the extent forbidden in this Section 14.9 *(Assignment & Successors)*, this Agreement will be binding upon and inure to the benefit of the parties' respective successors and assigns.

14.12. Severability. To the extent permitted by applicable law, the parties hereby waive any provision of law that would render any clause of this Agreement invalid or otherwise unenforceable in any respect. In the event that a provision of this 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 this Agreement will continue in full force and effect.

14.13. No Waiver. Neither party will be deemed to have waived any of its rights under this 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 this Agreement will constitute a waiver of any other breach of this Agreement.

14.14. Choice of Law & Jurisdiction: If Customer is located in the United States, this Agreement will be governed solely by the internal laws of the State of Minnesota, United States, otherwise this 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: (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; 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 14.12 (*Choice of Law & Jurisdiction*) governs all claims arising out of or related to this Agreement, including without limitation tort claims.

14.15. Construction. The parties agree that the terms of this Agreement result from negotiations between them. This Agreement will not be construed in favor of or against either party by reason of authorship.

14.16. U.S. Government End-Users. The Services and Documentation are provided with Restricted Rights. Use, duplication, or disclosure for or by the government of the United States, including without limitation any of its agencies or instrumentalities, is subject to restrictions set forth, as applicable: (i) in subparagraphs (a) through (d) of the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19; or (ii) in similar clauses in other federal regulations, including the NASA FAR supplement and the DFAR's. The contractor or manufacturer is Entrust Datacard. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in the Services or Documentation or on any packaging or other media associated with the Services or Documentation. Customer shall require that its government Users of the Services and Documentation agree to and acknowledge the provisions of this 14.14, in writing.

14.17. Technology Export. Customer 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 use of the Service. Customer represents and warrants that: (a) Customer is not located in, under the control of, or a national or resident of any country to which the export of the software or related information would be prohibited by the applicable laws, rules or regulations of the United States or Canada or applicable jurisdiction; (b) Customer is not an individual to whom the export of the Software or related information would be prohibited by the laws of the United States or Canada or applicable jurisdiction; and (c) Customer has and will comply with applicable laws, rules and regulations of the United States and Canada or applicable jurisdiction and of any state, province, or locality or applicable jurisdiction governing exports of any product or service provided by or through Entrust Datacard. Customer 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.

14.18. Entire Agreement. This 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.

14.19. Amendment. Subject to Section 2.4 (*Cloud Component Revisions*), this Agreement and the Documentation, SLA and Privacy Statement may be amended by Entrust Datacard from time to time by posting a new version and such new version will become effective on the date it is posted except that if Entrust Datacard modifies the main body of this Agreement in a manner which significantly reduces Customer's rights or increases Customer's obligations and such changes are not required for Entrust Datacard to comply with law, the changes to the main body of this Agreement will become effective sixty (60) days after Entrust Datacard 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 main body of this Agreement will become effective at the end of Customer's current subscription. Notwithstanding the foregoing provisions of this Section 14.18 (*Amendment*), amendment of the AUP, is governed by the AUP.