Entrust Identity Verification Schedule

The Agreement for Identity Verification Services (formerly Onfido) is made up of these terms (the "Identity Verification Services Schedule"), Entrust's General Terms and Conditions available at https://www.entrust.com/general-terms.pdf, and a duly executed Order for such Identity Verification Offering. Capitalized terms not defined herein have the meanings given to them in the General Terms and Conditions.

1. **Definitions**

1.1. **Accurate Volume Projections**: means for each individual Service purchased: (i) quarterly volume forecasts six weeks in advance to a degree of accuracy within 10% of the actual monthly volumes; and (ii) notice at least seven days in advance of any major volume spikes, i.e. where the number of checks in a given hour exceeds three standard deviations from the average number of hourly checks in a given month.

1.2. **App**: means the application owned and developed by Customer into which Customer will integrate the Software.

1.3. **Authorized User**: means Customer's employees, consultants, contractors, agents, and affiliates who are authorized by Customer to access and use the Hosted Services under the rights granted to Customer pursuant to this Schedule.

1.4. **Baseline Tolerance**: means within 25% of the baseline volume commitment notified by Customer to Entrust as at the Effective Date (as defined in the Order), apportioned pro rata monthly over the Offering Term and any Renewal Term(s).

1.5. **Brand Features**: means the trade names, trademarks, logos, and other distinctive features of the applicable party.

1.6. **Content**: means any information, text, graphics, or other materials uploaded, downloaded, or appearing as part of the Services.

1.7. **Customer Data**: means information supplied by a User or Customer in connection with this Schedule (including Customer Personal Data, and metadata), but excludes Feedback.

1.8. **Dashboard**: means a graphical user interface to Entrust's API, as further described in the API documentation.

1.9. **Product Privacy Notice** means Entrust's Identity Verification Services Product Privacy Notice available at https://www.entrust.com/sites/default/files/documentation/licensingandagreements/product-privacy-notice-identity-verification-services.pdf, as may be amended and updated from time to time.

1.10. **Export Controls and Sanctions Laws:** means any applicable export control, trade or financial sanctions laws, regulations, orders, directives, licenses and requirements of any governmental or other relevant authority with jurisdiction over activities undertaken in connection with this Schedule including but not limited to those listed in the Compliance with Applicable Laws clause of the General Terms (each such listed authority being a "Sanctions Authority").

1.11. **External Data Providers** means any third party, institution, organization, corporate entity, or government agency responsible for the provision of data or information in relation to the Services.

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

1.13. **FCRA** means the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.

1.14. **Feedback**: means any feedback or suggestions provided by Customer under this Schedule in relation to the Services.

1.15. **Fraud Database Service Provider** means a government body or other third party service provider that checks whether an identity document has been previously identified to them as lost, stolen, fraudulent, or otherwise compromised.

1.16. **Hosted Services**: means, in this Schedule, the Identity Verification Services cloud-based Offering.

1.17. **Maintenance Release**: means a release of the Software that corrects faults, adds functionality, or otherwise amends or upgrades the Software.

1.18. **Permitted Purpose**: means legitimate, professional, informational, internal business operations purposes and not in any event for the reselling or otherwise making the Services available to any third parties, except as otherwise expressly permitted in the Agreement.

1.19. **Reports**: means a summary at a User level containing one or more of the checks outlined in the Order.

1.20. **Sandbox Environment**: means a test environment for Customer to simulate API requests and to test their integration with the Software.

1.21. **Services**: means the services and/or products offered by Entrust from time to time under this Schedule and as more particularly detailed in the applicable Order (including, as the case may be, the Reports, Content, Software, Site, and API).

1.22. **Site**: means www.Entrust.com, its subdomains, or websites hosted by Entrust used in the provision of the services, which may be updated from time to time.

1.23. **SLA**: means Entrust's standard service level agreement for the Hosted Service, as may be modified from time to time, available at https://www.entrust.com//sites/default/files/documentation/licensingandagreements/entrust-identity-verification-sla-terms.pdf.

1.24. **Software**: means any software provided by Entrust, including the software development kit (or "SDK") and any Maintenance Release which is being made available to Customer as part of the Services.

1.25. **Source Code Materials**: means the source code of the Software, and all technical information and documentation required from Entrust to enable Customer to integrate the Software into the App.

1.26. **User**: means any person whose identity is being verified by Customer using the Services.

2. SDK License, Access and Use of the Hosted Services, and Entrust Obligations

2.1. Entrust grants to Customer a personal, limited scope, non-exclusive, non-transferable, non-sub-licensable license to use the Software in the App for the Permitted Purpose, for the Offering Term, provided that:

2.1.1. use of the Software will be restricted to use of the Software in object code form for the purpose of running document and facial recognition checks as part of the App only;

2.1.2. to the extent the Software includes components covered by open source software ("OSS") licenses (a) the terms of such OSS license(s) are available at https://github.com/onfido or such other location notified by Entrust from time to time and will, in the event of any conflict with the terms and conditions set out herein, prevail in respect of Customer's use of such OSS; and (b) any restrictions prohibited by such OSS license that are contained within this Schedule will not apply to the applicable OSS;

2.1.3. Customer will not allow the Software to become the subject of any charge, lien, or encumbrance;

2.1.4. If Customer becomes aware of any or suspects any unauthorized access or use of the Software by any person, it shall notify Entrust immediately.

2.2. Entrust will make available one copy of the Software electronically to Customer. Customer will be responsible for the integration of the Software into the App and all compatibility issues between the Software and the App. Entrust will provide Customer with reasonable, limited assistance and guidance with the integration of the Software and the App. Customer will carry out appropriate testing and satisfy themselves with the results before making the App available in a live environment.

2.3. Upon reasonable advance notice by request, Customer will permit Entrust to inspect and have access to any records kept in connection with this license, for the purposes of ensuring that Customer is complying with the terms of this license.

2.4. Entrust hereby grants Customer, during the Offering Term, a personal, non-exclusive, non-transferable right to access and use the Hosted Services for the Permitted Purpose by Authorized Users in accordance with the terms and conditions herein.

2.5. Entrust shall, during the Offering Term, provide the Services with reasonable skill and care and in accordance with the SLA. The parties will provide each other with all necessary co-operation in relation to this Schedule and reasonable access to such information as may be required in order to render and receive the Services.

3. Services, Maintenance, and Support

3.1. Entrust will provide Customer with all Maintenance Releases generally made available to its customers. Entrust warrants that no Maintenance Release will adversely affect the then existing facilities or functions of the Software but will not be responsible for any necessary integration or re-integration with the App following a Maintenance Release, or any incompatibility issues. Customer will install all Maintenance Releases as soon as reasonably practicable after receipt, but in any event within nine (9) months of Maintenance Release (the 'Upgrade Obligation'). Entrust will not be in breach of any clause of this Schedule to the extent that the Customer breaches its Upgrade Obligation.

3.2. Customer shall use a maintained version of the Maintenance Release. If Customer fails to do so, Entrust shall not be liable to Customer for any malfunctions, security breaches, or application certification issues.

3.3. In the event of a fault or defect in the Software, Entrust will provide support and incident resolution in accordance with the escalation procedures and severity levels set out in the Support Terms available at https://www.entrust.com//sites/default/files/documentation/licensingandagreements/entrust-identity-verification-support-terms.pdf.

3.4. If and to the extent Customer has purchased a Customer Success Package, Entrust will provide such services in accordance with the Customer Success Packages Terms available at: https://www.entrust.com//sites/default/files/documentation/licensingandagreements/entrust-identity-verification-customer-success-packages-terms.pdf.

3.5. If and to the extent Customer has purchased a Onboarding Package, Entrust will provide such services in accordance with the Onboarding Packages Terms available at: https://www.entrust.com//sites/default/files/documentation/licensingandagreements/entrust-identity-verification-onboarding-packages-terms.pdf.

3.6. If and to the extent Customer has purchased a Professional Services Package, Entrust will provide such services in accordance with the Professional Services Package Terms available at: https://www.entrust.com/sites/default/files/documentation/licensingandagreements/entrust-identity-verification-professional-services-packages-terms.pdf.

4. Customer Obligations and Restrictions

4.1. Customer is solely and fully responsible for ensuring that all User's data is accurate, complete and captured in a form that the Entrust can process to maximize the quality of Service, and Customer agrees that if any Personal Data is not provided as such, any resulting impact on the quality of the Services shall not cause Entrust to be in breach of this Schedule or any SLA.

4.2. Customer: (i) may download, view, copy and print Content and use the Services for the Permitted Purpose only; (ii) agrees that the Reports, Services, the Site and Content may not be sold, transferred, sublicensed, commercially exploited or otherwise made available to, or used for the benefit of, any third party other than Customer; (iii) will not amend or remove any Entrust Brand Features from the Services, Site, or Software; (iv) will not make use of the Entrust API without prominently displaying "powered by Onfido" or "powered by Entrust" language, as specified by Entrust in its sole discretion, that is clearly visible to Users; (v) will not make the Services available or otherwise use the Services in any jurisdiction such that Entrust's provision of the Services would require Entrust to physically store data (of any kind) in that jurisdiction, without first obtaining Entrust's prior written consent; (vi) will not make the Services available or otherwise use the

Services in any jurisdiction where the Services are not permitted by applicable law; and (vii) where required by applicable law, agrees to provide Users with human intervention in respect of any disputed Reports.

4.3. Customer is responsible for maintaining the confidentiality and security of any password(s), access credentials, or security routines used to access the Services, including those issued to its Users. Customer shall take reasonable steps to prevent unauthorized access to or use of the Services and is fully responsible for all activities that occur under its credentials or those of its Users, whether authorized or not. Customer agrees to notify Entrust immediately of any accidental or unauthorised access to or use of the Services, whether suspected or confirmed, and shall use best efforts to mitigate and stop any breach or unauthorized use. In the event of a suspected or confirmed security incident impacting Customer's use of the Services or other exigent circumstances, Entrust reserves the right to immediately withdraw or suspend access to the Services and to alter or reset Customer's password(s) without prior notice.

5. Pricing and Payment

5.1. Customer acknowledges that Entrust reserves the right to modify the fees for the Services subject to ninety (90) days' notice prior to the end of the initial Offering Term or Renewal Term. Within the initial Offering Term but no more than annually, upon ninety (90) days' notice Entrust may adjust the fees by a percentage equal to the average increase in the Consumer Price Index All Urban Consumers (CPI-U), as calculated by the U.S. Bureau of Labor Statistics, over the prior twelve (12) months.

5.2. Where: (i) any External Data Provider increases an existing charge and/or changes the basis on which it provides information, or confirmation of qualifications or membership; and (ii) the cost of Entrust providing a check under this Agreement increases as a direct result (each a "Cost Increase"), Entrust may increase the agreed fees set out in the Order by the Cost Increase provided that Entrust will use reasonable endeavors to notify Customer of the Cost Increase prior to implementing the Cost Increase. Notwithstanding the foregoing, Customer is responsible for all Cost Increases provided that these are properly incurred by Entrust.

5.3. Subscription Services. The following payment terms apply to subscription based services, as set forth in the applicable Order Form:

5.3.1. The User Limit (as set forth in the applicable Order Form), represents the maximum number of unique Users that may access and use the Services during any given month without incurring additional charges. Customer is responsible for managing its user accounts to remain within the applicable User Limit.

5.3.2. If, at any point in any calendar month during the Offering Term, the number of unique Users with active access to the Services exceeds the User Limit (a "User Overage"), Customer shall incur an overage fee for that month (an "Overage Charge"). Each Overage Charge shall be calculated as follows: User Overage x 1/12 of the then-current per-user, per-year rate.

5.3.3. Overage Charges will be invoiced monthly in arrears and each month shall be assessed independently. For example, if Customer exceeds the User Limit in one month and returns to or below the User Limit in a subsequent month, Overage Charges will only apply to the month(s) in which the User Limit was exceeded.

5.3.4. Customer acknowledges and agrees that deactivation or removal of Users after exceeding the user Limit shall not entitle Customer to any refund, credit, or waiver of Overage Charges incurred in prior months.

6. Disclaimer of Warranties

6.1. If within the terms of the license to the Software granted in this Schedule and through no fault of its own (or any of its third parties or subcontractors) Customer notifies Entrust of any material defect or fault in the Software, Entrust will at its sole discretion: repair, replace, correct the Software.

6.2. Customer acknowledges and agrees that the veracity of any information transmitted through the Site and in relation to the Services is the sole responsibility of the originator from which the content originated (for example, data suppliers) and Entrust will not be liable for omissions in content or errors or false statements, including in respect of data provided by third parties. The Services are not intended to be used as the sole basis for any business decision (including where those business decisions concern a User). Customer agrees and acknowledges that Entrust does not monitor or police information submitted by or on behalf of the Customer through its Services and has no liability for any inaccuracy, incompleteness or other error in the Services (including the Site, the Reports and the Content) which arises as a result of data provided by the Customer or any third party. Subject to the Entrust's obligations to provide the Services with reasonable care and skill, Customer assumes sole responsibility for workflows and conclusions drawn from use of the Services (including the Reports, the Content and the Site).

6.3. Cloud Risks. Customer understands that the Service is a cloud-hosted service. Although Customer content may be encrypted, Customer acknowledges that there are inherent risks in storing, transferring and otherwise processing data in the cloud, and that Entrust will have no liability to Customer for any unavailability of the Services except as expressly provided in this Schedule, or for any damage, theft, unauthorized access, compromise, alteration, or loss occurring to Customer content or any data stored in, transferred to or from, or otherwise processed by the Service, including in transit.

6.4. Customer acknowledges and agrees that the Services, including any associated workflows made available therein, are configurable and may be customized by Customer at its discretion. Customer assumes sole responsibility for ensuring that both (i) the Service, as provided by Entrust; and (ii) any Customer-directed customizations, configurations, or implementations comply with all applicable laws, regulations, and industry standards to which Customer is subject.

Entrust makes no warranty that the Services will meet your requirements. Entrust shall have no responsibility or liability for any erroneous, fraudulent, or synthetic data introduced into the Services by Customer, its Users, or other third party. Customer further acknowledges and agrees that any such data-related errors originating from Customer, any User, or from third party data shall not constitute a breach of any warranty or obligation of Entrust. This provision is in addition to, and shall not limit or modify, any other disclaimers, limitations of liability, or representations and warranties set forth elsewhere in the Agreement.

6.5. Entrust is not a consumer reporting agency and none of the information provided through the Service constitute a "consumer report" as such term is defined in the Fair Credit Reporting Act. The Services are expressly limited to providing supplemental information in support of Customer's anti-fraud and identity verification businesses only. In no event does Entrust, directly or indirectly, whether through any results or outcomes presented by the Services, provide any guidance, opinion, guarantee, or other statement regarding the legality or authorization of any individual person to engage or not engage in any given activity.

6.6. To the extent configured via the Services and not withstanding anything to the contrary in this Agreement, Customer acknowledges and agrees that (a) the Fraud Database Service Providers may retain identity documents that are suspected to be fraudulent for the purpose of identifying fraud in the future; (b) Entrust is not responsible for Fraud Database Service Provider's use and retention of such identity documents, and (c) Entrust is not responsible to flow-down or contractually bind Fraud Database Providers to any terms and conditions. Entrust waives all responsibility and liability for Fraud Database Service Provider's acts and omissions.

6.7. In the event that Customer elects to access the Services through a third-party interface, integration, or similar ("third Party Integration"), such third-party Integration will be outside the scope of this Schedule and shall remain the sole responsibility of Customer. Customer will contract directly with such third party and Entrust shall: (i) have no liability in respect to such third party, or third-party Integration; and (ii) not be in breach of the Agreement to the extent such breach is caused by the third-party Integration.

6.8. Fraud Information Sharing. Customer may provide timely Feedback and information to Entrust in relation to the Services or beta features, in particular, reporting to Entrust via the API or (if agreed) the Dashboard any: (1) fraud not identified by Entrust in its provision of the Services that is later identified by Customer; (2) Users or checks identified as fraudulent by Entrust which are not fraudulent; and (3) Users who commit fraud against Customer ("**Fraudulent Users**"). Entrust may use the reported information and associated fraud data to improve the Entrust Identity Verification services.

6.9. Test Environment. To the extent that Customer elects to use a sandbox environment provided by Entrust, Customer understands that Entrust does not review any data uploaded or transferred into the sandbox environment, and Customer agrees (i) to only use the sandbox environment to test Customer's integration with the Software; (ii) to not upload or transfer any Personal Data into the sandbox environment and (iii) Entrust shall have no obligations or liability as to any data uploaded or transferred to the sandbox environment.

7. Intellectual Property Rights

7.1. As between Entrust and Customer, all intellectual property rights in and to Customer Data will be owned by Customer. Customer owns or has otherwise obtained all necessary rights, title and interest in and to the Customer Data and grants to Entrust, its Affiliates, and third party service providers a license to copy, modify, repackage, distribute, resell, share, deliver, transfer or otherwise make available, and to create or develop derivative works from, Customer Data for the purposes of providing or enhancing the Services.

8. Evaluation, Beta, Demo

8.1. Beta Features. From time to time, Entrust may invite Customer to participate in a new version or service feature that Entrust has not made generally available to clients for production use and that is designated as beta, pilot, limited release, pre-release, non-production, evaluation or similar designation which does not form part of the Services ("**Beta Features**"), free of charge in return for Customer providing Entrust with Feedback. This invitation will be communicated to Customer through the Entrust Dashboard and Customer may accept or decline the invitation in its sole discretion. Beta Features are for Entrust evaluation and testing purposes, not for production use, not supported, not subject to availability or security obligations and may be subject to additional terms. For the sake of clarity, Entrust will have no liability for any harm, damage or losses of any kind arising out of or in connection with Beta Features, and Customer uses them at its own risk. Entrust does not warrant that the operation of the Beta Features will be uninterrupted or error-free. Customer acknowledges and agrees that all Beta Features are made "as is" and are provided without any warranties, whether express or implied. Entrust may discontinue Beta Features at any time in its sole discretion and may choose not to make them generally available.

8.2. Evaluation. To the extent that Customer has executed an Order for a free trial of a feature provided or made available pursuant to this Schedule, the terms and conditions of this Schedule along with the applicable product specific terms apply, with the following exceptions: Entrust will have no liability for any harm, damage or losses of any kind arising out of or in connection with evaluation features, and Customer uses them at its own risk. Entrust does not warrant that the operation of the evaluation features will be uninterrupted or error-free. Customer acknowledges and agrees that all evaluation features are made "as is" and are provided without any warranties, whether express or implied. Entrust may discontinue or terminate the trial any time in its sole discretion. Customer further acknowledges and agrees that Entrust will own all Feedback and all associated intellectual property rights in or to Feedback, and Customer hereby assigns to Entrust all of Customer's right, title, and interest thereto.

9. Additional Data Protection Provisions

9.1. Relationship to DPA. The provisions of this Section (Additional Data Protection Provisions) apply in addition to the provisions of the Data Protection Addendum between Entrust and Customer ("**DPA**"). Capitalized terms used in this Section shall have the meaning given to them in the DPA. In the event of any inconsistency between the DPA and this Section, the provisions of this Section shall prevail to the extent of the inconsistency.

9.2. Processing as Controller under GDPR and UK GDPR. In addition to Processing Customer Personal Data for the purpose of providing the Services as described by the DPA, Customer agrees and acknowledges that Entrust shall Process Customer Personal Data relating to Users as Controller under GDPR and UK GDPR

in order to: (a) detect and prevent fraud; (b) develop and improve the Entrust Identity Verification services, including machine-learning technologies (provided such does not include building or modifying consumer profiles to provide services to other customers or correcting or augmenting data acquired by another source); (c) pseudonymise, aggregate and, where feasible, anonymise Customer Personal Data to compile statistics, benchmarking and analytics regarding the Services; (d) comply with applicable law or regulation; and/or (e) exercise legal rights or defend legal claims. See the Product Privacy Notice for more information. Since Entrust has no direct relationship with Users, Customer shall inform Users that the Processing described in this subsection (Processing as Controller under GDPR/UK GDPR) takes place (for example, by directing them to the above-mentioned product privacy notice).

9.3. Deletion.

9.3.1. Subject to the immediately following [paragraph], on the earlier of (i) written instructions from Customer, which shall include changes to Customer's configuration within the Services, (ii) Entrust's maximum data retention period, or (iii) instruction from a User (but only with respect to numerical biometric information relating to a User's own Personal Data), Entrust will cease Processing and delete Customer Personal Data processed for the provision of the Services (unless storage of any such data is required for the purposes described in (a)-(e) of the Section headed "Processing as Controller under GDPR and UK GDPR", in which case Entrust may retain such Customer Personal Data provided it remains protected in accordance with the terms of the DPA and applicable Data Protection Law).

9.3.2. All other Customer Personal Data processed by Entrust (including Customer Personal Data processed for backup and logging purposes) or on behalf of Entrust (including Customer Personal Data processed by Sub-processors) is deleted in accordance with Entrust's sub-processor list available at https://www.entrust.com/legal-compliance/data-privacy/sub-processors.

9.4. Excluded Data (Exception). Notwithstanding anything to the contrary in the General Terms, the parties acknowledge that the provision of the Services may require the Customer to provide or transfer, or cause to be provided or transferred, Excluded Data (as that term is defined in the General Terms). The Excluded Data that may be required for the provision of the Services is described in the Product Privacy Notice.

9.5. Additional Obligations regarding U.S. Users. To the extent Customer makes available to a User who is located in, or resident of, the United States ('US User") any of the Entrust Identity Verification services listed in the section of the Product Privacy Notice headed "Additional Obligations regarding U.S. Users (each a "Relevant Service"), the Additional Obligations regarding U.S. Users Exhibit available at https://www.entrust.com/sites/default/files/documentation/licensingandagreements/entrust-identity-verification-additional-obligations.pdf, is hereby incorporated by reference.

10. **Indemnification**.

10.1. Customer agrees to defend, indemnify, and hold harmless, on an unlimited basis, Entrust, its Affiliates and licensors, and each of their respective officers, directors, employees, agents, consultants, and other representatives against any and all claims, demands, judgments, actions, suits, proceedings, demands, liabilities, costs, losses, damages, settlement fees, and expenses (including investigation costs, attorneys' fees, and disbursements), arising out of or relating to (i) Customer's failure to comply with applicable U.S. Biometric Data Protection Laws, including but not limited to failing to provide necessary notices or obtain necessary consents; (ii) Customer's breach of Section Additional Obligations regarding U.S. Users, or (iii) Customer's use of the Services, provided and to the extent that such claims are not due to any breach of this Agreement by Entrust.

11. **Artificial Intelligence**

11.1. The parties acknowledge and agree that Entrust uses Artificial Intelligence, i.e. computer algorithms and machine learning systems that can analyze, process, and make decisions based on data inputs, without the need for direct human intervention ("AI") technology, for certain Identity Verification service offerings as

detailed in the Product Privacy Notice. Entrust will employ AI in a manner informed by evolving industry standards and best practices, striving to ensure the accuracy, reliability, and security of the AI systems it employs, and will from time to time, to the extent required by laws and regulations applicable to Entrust and otherwise in its discretion, make available details of its AI use in the Product Privacy Notice. While Entrust is committed to the responsible and ethical use of AI, Customer acknowledges that AI-driven decisions are fallible. Therefore, Customer agrees to exercise reasonable judgment when relying on AI-generated information and to use human intervention where feasible for decisions made by AI that may negatively impact data subjects, taking into account the particular uses and contexts in which Customer is considering using AI-generated outputs of the applicable Entrust Identity Verification service offering. Entrust will comply with all relevant data protection and privacy laws concerning the collection, processing, and storage of personal information used in conjunction with AI as further outlined in data protection provisions above. Customer will not, and will not allow third parties to, use the Services (or any content, data, output, or other information received or derived from the Services) to directly or indirectly create, train, test, or otherwise improve any machine learning algorithms, automated decision-making processes, or AI systems, or input or upload any Entrust confidential information to an AI system or application.

12. **Product Specific Terms**

12.1. If and to the extent that Customer has purchased the Mastercard Identity, the Mastercard Identity Terms, available at: https://www.entrust.com//sites/default/files/documentation/licensingandagreements/entrust-identity-verification-mastercard-identity-terms.pdf, is hereby incorporated by reference.

12.2. If and to the extent that Customer has purchased the ETSI Certified Identity Verification services, the ETSI Certified Identity Verification Terms, available at: https://www.entrust.com//sites/default/files/documentation/licensingandagreements/entrust-identity-verificatio-netsi-certified-identity-verification-terms.pdf, is hereby incorporated by reference.

12.3. If and to the extent that that Customer has purchased the Qualified Electronic Signature services, the Qualified Electronic Terms, available at: https://www.entrust.com//sites/default/files/documentation/licensingandagreements/entrust-identity-verification-qualified-electronic-signature-terms.pdf, is hereby incorporated by reference.

12.4. If and to the extent that Customer has purchased any additional services as set forth in the Additional Product Specific Terms, such applicable terms, available at: https://www.entrust.com//sites/default/files/documentation/licensingandagreements/entrust-identity-verification-additional-product-specific-terms.pdf, is hereby incorporated by reference.

12.5. If and to the extent that Customer has purchased the AES Signing services, the AES Signing Terms, available at: https://www.entrust.com//sites/default/files/documentation/licensingandagreements/entrust-identity-verification-aes-signing-terms.pdf, is hereby incorporated by reference.

12.6. If and to the extent that Customer has purchased the UK DVSTF Certified Identity Verification services, the UK DVSTF Certified Identity Verification Terms, available at https://www.entrust.com/sites/default/files/documentation/licensingandagreements/entrust-identity-verification-uk-dvstf-certified-identity-verification-terms.pdf, is hereby incorporated by reference.