Additional Product Specific Terms

If and to the extent Customer has purchased the additional services set forth below, such terms apply solely with respect to those products and services.

Product Terms:

1. Autofill.
    a. For the purposes of Autofill, the Customer acknowledges that the list of supported documents will be notified from time to time, and do not currently include all Documents, and that in the event a document is unsupported, Autofill will not be available.
2. Watchlist AML Ongoing and Watchlist Standard Ongoing.
    a. Any rolling deletion may be deactivated by Entrust at Customer account level in order to provide this Service.
3. EEA – Manual Review Processing.
    a. Entrust will configure third party human analysts providing first time manual review as part of Document Check and Facial Similarity Check from the European Economic Area.
4. Local Storage.
    a. Customer represents and warrants that it has taken all required steps to ensure that Entrust may lawfully store and retrieve the encrypted biometric token from the User's device (including by having obtained all necessary consents, where required) in accordance with electronic communication laws, including Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 ("e-Privacy Directive") as transposed into applicable domestic legislation.
5. Authentication Motion
    a. Customer represents and warrants that it has taken all required steps to ensure that Entrust may lawfully store and retrieve the encrypted biometric token from the User's device (including by having obtained all necessary consents, where required) in accordance with electronic communication laws, including Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 ("e-Privacy Directive") as transposed into applicable domestic legislation.
    b. Customer acknowledges that Authentication Motion is designed to be utilized for re-authentication of Users after a User has undergone a separate initial biometric identity verification check through an on-boarding process. Customer represents and warrants that it will not utilize Authentication Motion as a User's initial biometric identity verification check.
6. Query Country Databases (DVS)
    a. In order to access the Australian Government Document Verification Service to enable the Customer to submit DVS information match requests via the DVS ("**Document Verification Service"** or "**DVS**") the Customer represents and warrants on a continuing basis that:
        i. it is a legal entity and lawfully carrying on business in Australia and/or New Zealand;
        ii. it is subject to Australian law (including the Privacy Act 1988 (Cth) if operating in Australia, and/or New Zealand law if operating in New Zealand, in connection with its use of the Services; and
        iii. all information provided by the Customer to Entrust in connection with DVS access including as part of any DVS onboarding or approval process is true, complete and up to date.

b. The Customer acknowledges and agrees that:

i. no DVS matching checks may be initiated until the Customer has completed and returned to Entrust the DVS onboarding form in the form required by Entrust; and

ii. the availability of the DVS to the Customer is subject to approval granted by or on behalf of the Attorney-General's Department ("DVS Approval") which is outside of Entrust's control. Where DVS Approval is not granted or is withdrawn, including as a result of the Customer's failure to adhere to section 1(c) above, Entrust may suspend or discontinue the DVS matching checks and any such suspension or discontinuation shall not constitute a breach of the Agreement. In such circumstances, the remainder of the Services shall continue unaffected. Entrust will notify Customer of any suspension or discontinuation as soon as reasonably practicable.

c. The Customer must obtain the User's express consent before submitting any DVS check and must provide any notices required by applicable privacy laws (including Australian Privacy Principle 5) in connection with the collection and verification of identity information. On reasonable request, the Customer must provide Entrust with evidence of compliance with this clause, including copies of relevant notices.