THIRD PARTY TERMS

Third Party	Product Function	OneSpan Product	Location	Flow Down Terms
Belgian Mobile ID	Mobile authentication and Qualified Electronic Signature	OneSpan Sign, Secure Agreement Automation, Identity Verification	Belgium	Set forth below
Mitek Systems, Inc. ("Mitek")	Identity document verification	Secure Agreement Automation (optional)	Europe, United States	Set forth below
Jumio Corporation	Identity document verification	Secure Agreement Automation (optional), Identity Verification (optional)	United States, India, Columbia and such other countries as Jumio may require	Set forth below
Lexis Nexis Risk Solutions	Knowledge base authentication services	OneSpan Sign OneSpan Notary Knowledge Based Authentication	United States	Set forth below
OCR Labs	Identity document verification	OneSpan Sign	Primarily Australia	https://www.onespan.com/ocr-labs-terms-and-conditons
SmartComms, LLC	SmartCOMM- customer communications management SmartIQ – forms automation	OneSpan Sign	For Customers in the following territory: United States, Canada, United Kingdom, Ireland, France, Germany, Spain, Italy, Australia, and New Zealand	Set forth below
Swisscom Trust Services Ltd ("STS")	Qualified Electronic Signature	OneSpan Sign	Switzerland, EU	Set forth below
Telesign Corporation	SMS for authentication and notification purposes	OneSpan SaaS products and certain software products	Europe	Set forth below
Twilio Inc.	SMS for authentication and notification purposes	All OneSpan SaaS products	United States	Set forth below
Veridas Digital Authentication Solutions S.L.	Identity document verification	OneSpan Identity Verification	European Economic Area and the United States of America depending on customer location	Set forth below
Workato, Inc.	Integration platform as a Service (iPaaS) that OneSpan employs to enhance the integration capabilities between OneSpan Sign and other third-party applications used by customers.	OneSpan Sign	United States	Set forth below

To the extent applicable to Customer's use of the Supplier Product, Customer agrees to comply with the following additional terms which form an integral part of the Contract and/or Order Form concluded between Customer and the Supplier:

Belgium Mobile ID (itsme)

Customer obligations

1. Customer will display the itsme® Brand in accordance with Belgian Mobile ID's branding guidelines or
2. instructions,
3. Customer will notify Supplier of any disputes or claims from an End-User concerning an Operation, and,
4. Customer will comply with instructions and guidelines from Belgian Mobile ID regarding the
5. presentation and functioning of the itsme® Services.

Intellectual property rights:

In its capacity as licensee of the itsme® Brand, Supplier grants to the Customer a non-exclusive, non-assignable, non-transferable right (without the right to sub-license) to use, for the duration of the Contract, the itsme® Brand(s) for the sole purpose of the Customer's exercise of its rights or performance of its obligations under the Contract.

The Customer is only allowed to use the itsme® Brand(s) in accordance with Belgian Mobile ID's guidelines and instructions (including the branding guidelines), as may be amended from time to time by Belgian Mobile ID and as notified by Supplier to Customer. The Customer shall not display the itsme® Brand(s) in any manner that could jeopardize the validity, distinctiveness or reputation of the itsme® Brand(s) or that could be detrimental to Belgian Mobile ID or to Belgian Mobile ID's products and services. The Customer shall not, either during the term of the Contract or after termination thereof, (seek to) register or use any trademark, logo, trade name, other distinctive sign or design or other artwork that is identical or similar to or derived from the itsme® Brand. The items® Brand may not be used in connection with any illegal activity, or in connection with any other activity as may be notified by Belgian Mobile ID from time to time. Any and all goodwill associated with the itsme® Brand shall inure to the benefit of Belgian Mobile ID unless otherwise provided.

Definitions

1. "Itsme® Brand(s)" means the word and figurative trademarks which are registered in the Register of the Trade Marks and Design Registration Office of the European Union under filing number 15761752 and 16876187 and in the Register of the Benelux Office for Intellectual Property under number 994231 and 994230 and all names, logos, trade names, logotypes, trade designations, and other designations, symbols, and marks, that Belgian Mobile ID own, manage, license, or otherwise control now or in the future, anywhere in the world, whether registered or not.
2. "End-User" means any user of the itsme® App.
3. "itsme® App" means the Mobile App developed by Belgian Mobile ID.
4. "itsme® Services" means the authentication or Qualified Electronic Service offered by Belgian Mobile ID.
5. "Operation" means any use of the itsme® Services by the End User (Login, Share ID, Approval or Sign)

Jumio

Customer obligations

1. Supplier and not Jumio Corporation ("Jumio) is the provider of the Jumio services offerings provided through Supplier's Service (the "Jumio Solutions"), and Customer must look solely to Supplier with respect to any warranty, support and maintenance and/or any other issues or claims associated with Customer's use of the Jumio Services;
2. Customer my only use the Jumio Solutions for its internal business purposes;
3. In no event shall Jumio be liable to Customer or any third party for any loss profits, indirect, special, incidental or consequential damages or for interruption of use or loss or corruption of data with respect to Customer's receipt and use of the Jumio Solutions.

LexisNexis Risk Solutions FL Inc.

Customer's usage of the LexisNexis Risk Solutions FL Inc. ("LN") knowledge base authentication ("KBA") services (the "LN Service(s)") is subject to the following terms:

1. Customer represents and warrants that it is a registered business under applicable state laws.

2. If Customer receives a "pass/fail" status indicator (a "Pass/Fail Report", Customer may only use such Pass/Fail Report for its own internal business use and not for purposes of marketing, reselling, or brokering.

3. Unless Customer has expressly opted out of receiving such data, some of the information contained in the LN Services may be "nonpublic personal information," as defined in the Gramm-Leach-Bliley Act, (15 U.S.C. § 6801, et seq.) and related state laws (collectively, the "**GLBA**"), and is regulated by the GLBA ("**GLBA Data**"). Customer shall not obtain and/or use GLBA Data through the LN Services in any manner that would violate the GLBA, or any similar state or local laws, regulations and rules. Customer acknowledges and agrees that it may be required to certify its permissible use of GLBA Data falling within an exception set forth in the GLBA at the time it requests information in connection with certain LN Services and will recertify upon request. Customer certifies with respect to GLBA Data received through the LN Services that it complies with the Interagency Standards for Safeguarding Customer Information issued pursuant to the GLBA.

4. To the extent that the LN Services accessed by Customer include information or data described in the Risk Supplemental Terms contained at: https://risk.lexisnexis.com/terms/supplemental. Customer agrees to comply with the Risk Supplemental Terms set forth therein.

5. Customer acknowledges that the information available through the LN Services may include personally identifiable information and it is Customer's obligation to keep all such accessed information confidential and secure. Accordingly, Customer shall (a) restrict access to LN Services to those employees who have a need to know as part of their official duties; (b) ensure that none of its employees shall (i) obtain and/or use any information from the LN Services for personal reasons, or (ii) transfer any information received through the LN Services to any party except as permitted hereunder; (c) keep all user identification numbers, and related passwords, or other security measures (collectively, "**User IDs**") confidential and prohibit the sharing of User IDs; (d) immediately deactivate the User ID of any employee who no longer has a need to know, or for terminated employees on or prior to the date of termination; (e) take all commercially reasonable measures to prevent unauthorized access to, or use of, the LN Services or data received therefrom, whether the same is in electronic form or hard copy, by any person or entity; (f) maintain and enforce data destruction procedures to protect the security and confidentiality of all information obtained through LN Services as it is being disposed; (g) purge all information received through the LN Services within ninety (90) days of initial receipt; provided that Customer may extend such period if and solely to the extent such information is retained thereafter in archival form to provide documentary support required for Customer's legal or regulatory compliance efforts; (h) be capable of receiving the LN Services where the same are provided utilizing "secure socket layer," or such other means of secure transmission as is deemed reasonable by LN; (i) not access and/or use the LN Services via mechanical, programmatic, robotic, scripted or other automated search means, other than through batch or machine-to-machine applications approved by LN; (j) take all steps to protect their networks and computer environments, or those used to access the LN Services, from compromise; (k) on at least a quarterly basis, review searches performed by its User IDs to ensure that such searches were performed for a legitimate business purpose and in compliance with all terms and conditions herein; and (l) maintain policies and procedures to prevent unauthorized use of User IDs and the LN Services. Customer will immediately notify Supplier if Customer suspects, has reason to believe or confirms that a User ID or the LN Services (or data derived directly or indirectly therefrom) is or has been lost, stolen, compromised, misused or used, accessed or acquired in an unauthorized manner or by any unauthorized person, or for any purpose contrary to the terms and conditions herein. Customer shall remain liable for all costs to the extent arising from Customer's failure to prevent such impermissible use or access of User IDs and/or the LN Services, or any actions required as a result thereof, and shall reimburse OneSpan for any expenses it incurs thereof. Furthermore, in the event that the LN Services provided to the Customer include personally identifiable information (including, but not limited to, social security numbers, driver's license numbers or dates of birth), the following shall apply: Customer acknowledges that, upon unauthorized acquisition or access of or to such personally identifiable information, including but not limited to that which is due to use by an unauthorized person or due to unauthorized use (a " **Customer Security Event**"), Customer shall, in compliance with law, notify (the individuals whose information was potentially accessed or acquired that a Customer Security Event has occurred), and shall also notify any other parties (including but not limited to regulatory entities and credit reporting agencies) whose notification is required under applicable law and Supplier's reasonable discretion. Customer agrees that such notification shall not reference LN or the product through which the data was provided, nor shall LN be otherwise identified or referenced in connection with the Customer Security Event, without prior notification to Supplier and Supplier's provision of LN's express written consent which shall not be unreasonably withheld, prior to disclosing LN or the LN Services to any third party including notices to the public at large. Customer shall be solely responsible for any other legal or regulatory obligations which may arise under applicable law in connection with such a Customer Security Event and shall bear all costs associated with complying with legal and regulatory obligations in connection therewith. Customer shall remain liable for claims that arise from a Customer Security Event, including, but not limited to, costs for litigation (including attorneys' fees), and reimbursement sought by individuals, including but not limited to, costs for credit monitoring or allegations of loss in connection with the Security Event, and to the extent that any claims are brought against LN, shall indemnify LN for damages and costs of litigation (including attorney's fees) finally awarded against LN by a court of competent jurisdiction or agreed upon by Customer in a settlement in the action, but only if (i) LN notifies Customer promptly in writing that the claim or demand was received by LN or may be asserted, (ii) Customer has sole control over the defense of the claim and any negotiation for its settlement of compromise, and (iii) LN takes no action that , in Customer's judgment, is contrary to Customer's interests. Customer shall provide samples of all proposed materials to notify consumers and any third-parties, including regulatory entities, to Supplier who will provide to LN for review and approval prior to distribution. Customer shall provide Supplier who will provide to LN a written summary of the foregoing, with sufficient detail to permit LN to confirm compliance with applicable law. In the event of a Customer Security Event, Supplier may, in its sole discretion, take immediate action, including suspension or termination of Customer's account, without further obligation or liability of any kind.

6. Customer agrees that Supplier may maintain for a period of five (5) years a complete and accurate record (including consumer identity, purpose and, if applicable, consumer authorization) pertaining to every access to GLBA Data, Drivers Privacy Protection Act (18 U.S.C. § 2721 et seq.) and related state laws data, and motor vehicle record data.

7. Supplier will use commercially reasonable efforts to deliver the LN Services requested by Customer and to compile information gathered from selected public records and other sources used in the provision of the LN Services; provided, however, that the Customer accepts all information "**AS IS**". Customer acknowledges and agrees that LN obtains its data from third party sources, which may or may not be completely thorough and accurate, and that Customer shall not rely on the accuracy or completeness of information supplied through the LN Services. Supplier reserves the right to add materials and features to, and to discontinue offering any of the materials and features that are currently a part of, the LN Services provided Customer is given notice prior to such discontinuation.

8. Notwithstanding anything to the contrary in the Contract, Customer agrees that Supplier will purge all information received through the LN Services within ninety (90) days of initial receipt.

9. Provisions hereof related to release of claims; indemnification; use and protection of LN Services; LN's use and ownership of Customer's search inquiry data; disclaimer of warranties and other disclaimers; security; customer data and governing law shall survive any termination of the license to use the LN Services.

10. Notwithstanding anything to the contrary in the Contract with regard to Customer's use of private keys, a condition precedent to the KBA services is that Supplier may require use of its own key with regard to all KBA services.

Mitek

Personal Data and information (including Data and the identity document images) ("Mitek Data") will be purged and permanently erased from Mitek's systems within ninety (90) days from the date such Mitek Data is provided to Mitek. "Exception" data may be retained by Mitek for an additional ninety (90) days if necessary to ensure the accuracy and functionality of the Subscription Services. "Exception" data is defined as submitted Mitek Data where the expected Mitek Data was not properly extracted or verified by the Service.

SmartComms, LLC

Customer's usage of SmartComms, LLC ("SmartCom") products (the "SmartCom Service(s)") is subject to the following additional terms below which shall take precedence over any conflicting terms in the Contract.

1. Definitions

   With regard to these SmartCom Services terms, the following definitions apply:

   a. "Affiliate" means any entity which directly or indirectly controls, is controlled by, or is under common control of the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than fifty percent (50%) of the voting interests of the subject entity;

   b. "Ancillary Data" means data which may include Personal Data (limited to name, username, email address and telephone number) concerning Users which shall be submitted by Supplier to SmartCom on Customer's behalf for the Ancillary Purposes. For the avoidance of doubt, Ancillary Data does not include Data;

   c. "Ancillary Purposes" means use of Ancillary Data by SmartCom and its Affiliates for the purposes of providing the SmartCom Services and administrative functions including, but not limited to billing, finance and SmartCom Services administration;

   d. "Applicable Law" means: (i) any statute, regulation, by-law or subordinate legislation in force from time to time to which a party is subject and/or in any jurisdiction that the SmartCom Services are provided to or in respect of; and (ii) the common law and laws of equity as applicable to the parties from time to time;

   e. "CMS" or "Content Library" means the area(s) of a Tenancy that store or process: (i) content management system, including templates, styles, layouts and related resources; and/or (ii) projects and their associated resources;

   f. "CMS Data" means data uploaded to the CMS (excluding Transaction Data);

   g. "Data" means all electronic data or information submitted by Supplier to SmartCom on Customer's behalf in the course of using the SmartCom Services including Transaction Data and CMS Data but not including Ancillary Data;

   h. "Hack" means attempt to gain unauthorized access to, interfere with, adversely impact, or disrupt the integrity or performance of the SmartCom Services, the data contained therein, or their related systems or networks, including but not limited to a DOS attack;

   i. "Intellectual Property Rights" means patents, trademarks, service marks, registered designs, applications for any of those rights, trade and business names, unregistered trademarks and service marks, copyrights, know-how, database rights, rights in designs and inventions and all other rights of the same or similar effect or nature, including all renewals, applications and registrations (and the right to apply for registration) relating to any of the foregoing;

   j. "Privacy Laws" means any laws and regulations in relating to privacy or the use or processing of data relating to natural persons, including: (a) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (b) EU Regulation 2016/679 ("GDPR"); (c) the Data Protection Act 2018; (d) any laws or regulations ratifying, implementing, adopting, supplementing or replacing GDPR; (e) CCPA; and (f) The Health Insurance Portability and Accountability Act of 1996;

   k. "Privacy Policy" means SmartCom's privacy policy currently available at: https://www.smartcommunications.com/external-privacy-policy/ ;

l. “SmartCom Entities” means: (i) Platinum Topco Limited and any company or entity including joint venture in which it holds fifty percent (50%) or more of the shares or voting power; and (ii) the officers, employees and contractors of the entities referred to in (i) above;

m. "SmartCom Technology” means all proprietary technology belonging to or used by SmartCom Entities (including software, hardware, products, processes, algorithms, user interfaces, know-how, techniques, designs and other tangible or intangible technical material or information) which is made available Customer under an applicable Order Document or is otherwise used by SmartCom to provide the Services;

n. "Tenancy” means the facility within the SmartCom Technology made available to Customer as part of the SmartCom Services;

o. "Third Party Applications” means any online applications and offline software products that interoperate with the SmartCom Services that are not provided by SmartCom through Supplier under an applicable Order Document. Third Party Applications include Supplier Products;

p. “Transaction Date” means all electronic data or information (including any Personal Data therein) submitted by Reseller to the SmartCom Services on behalf of Customer (and for the avoidance of doubt excludes Ancillary Data);

q. "Unlawful Materials” means material or content that is infringing, obscene, libelous, spam or otherwise duplicative or unsolicited messages in violation of Applicable Law or otherwise unlawful or tortious, or is in violation of third party privacy rights or applicable Privacy Laws;

r. “User” means the number of natural persons specified in an applicable Order Document to use the particular components of the SmartCom Services; and

s. “Virus” means, without limitation, any automatic restraint, viruses, worms, time bombs, trojan horses and other harmful or malicious code, files, scripts, agents or programs that interfere with the provision of the SmartCom Services

2. Usage, Restrictions, and Customer Obligations:

a. Customer shall make no other use of the SmartCom Service(s) other than as permitted in this Contract, either for itself or the benefit of any other person or entity, or permit any third party to do the same.

b. Customer may only use the SmartCom Service for internal business purposes.

c. Customer is expressly prohibited from reselling, leasing, renting or otherwise making available the SmartCom Service as part of any outsourcing or similar arrangement by or for the benefit of any third party.

d. Customer is responsible for the legality of the Data and Ancillary Data, the means by which Customer acquired Data and Ancillary Data and the lawfulness of transmitting Data and Ancillary Data to SmartCom.

e. Customer will use reasonable efforts to prevent unauthorized access to the SmartCom Service and will notify Supplier promptly of any such unauthorized access or use.

f. Customer will be liable for any acts or omissions in relation to this section and will be responsible for ensuring that it does not (i) store or transmit Unlawful Materials; (ii) knowingly store or transmit Viruses; or (iii) Hack the SmartCom Services. If at any time Customer contravenes any of the prohibitions listed in this section, Supplier may in its sole discretion suspend Customer and/or User access to the SmartCom Services, and may where possible, provide Customer with notice of such suspension. Supplier may further treat a contravention of this section as an irremediable and material breach, entitling Supplier to terminate the SmartCom Services with immediate effect. Prohibited activities shall also include any use of the SmartCom Services for or in connection with online gaming or gambling, IRC (Internet Relay Chat) or related bot as reasonably determined by Reseller in its sole discretion.

g. Customer accepts that Third Party Applications will, in order to operate with the SmartCom Services, access Data. Customer agrees that SmartCom is not responsible for any disclosure, modification or deletion of Data resulting from any such access by Third Party Applications.

h. Customer acknowledges that the availability and use of the SmartCom Services is conditional upon Customer having a valid subscription to use the relevant Third Party Application, where applicable.

i. Customer shall promptly furnish Supplier with written certification verifying that the SmartCom Services are being used in accordance with the contract, including the number of Users. Customer shall give SmartCom reasonable access to its records are appropriate to verify that the SmartCom Services are being used in accordance with the terms of this Contract.

j. Customer is responsible for the input and maintenance of the CMS Data and for maintaining effective back-up procedures as may be necessary to replace any CMS Data in the event of loss, as the CMS is not intended to be or designed to be a system of record. Supplier and SmartCom shall not be responsible or liable for any loss or damage to or failure to store the CMS Data. Customer consents, agrees and acknowledges that SmartCom may send/store Ancillary Data outside the United States of America for the Ancillary Purposes in accordance with the Privacy Policy. SmartCom shall not transfer Transaction Data outside of the SmartCom Services hosting location or deployment arrangement.

k. Customer is prohibited from providing Data that would infringe the Intellectual Property Rights of any Third Parties.

l. Customer warrants that it has secured all necessary rights, licenses and permissions (such as font licenses and rights to disclose data received by Customer which is included in Data) so that Reseller and SmartCom can use the same when providing the SmartCom Services.

m. Upon expiry or early termination of a SmartCom Term (as defined in the Master Terms), Customer shall cease to be entitled to use the SmartCom Services and shall immediately de-install any SmartCom Technology used to access and or use the SmartCom Services and, at SmartCom's option, either return or destroy the same and upon request certify in writing to Reseller that it has complied with this provision. Customer also acknowledges that SmartCom will delete all Data within thirty (30) days after termination and or expiry of the Term. Customer acknowledges that SmartCom may retain and use Ancillary Data beyond termination of the MSA and/or an applicable Order Document for the Ancillary Purposes, but in any event in compliance with Privacy Laws.

n. Customer agrees that SmartCom may (i) identify Customer as a user of the SmartCom Services and (ii) use Customer's logo on SmartCom's website for such purposes only.

3. SmartCOMM Service - Customer Communications Management Tool ("CCM Service(s)") Service Description

a. Definitions:

"AWS" means hosting of the Services on Amazon Web Services located in the U.S.;

"Batch" means groups of Output submitted to the CCM Services on a batch basis via the batch APIs;

"File Storage" means input files, output files and log files relating to Batch;

"Final Output" means Output generated by the CCM Services that is no longer editable via the CCM Services and may be issued by Customer to third parties;

"Generated Document" means Final Output generated by the CCM Services from a single template design in a single output format;

"Interactive Page" means a Page which can be only edited by Customer using the CCM Services prior to it being Final Output;

"Interim Output" means any Output except Final Output;

"Non-Interactive Page" or "On-Demand Page" means a Page which once created by Customer using the CCM Services cannot be further edited;

"Order Year" means each twelve (12) month consecutive period beginning from the commencement of the License Term;

"Output" means a Page created through Customer's use of the CCM Services;

"Overage Unit" means blocks of 10 Users or 1 million Pages;

"Page" means each: (i) physical page face/side (or electronic equivalent) conforming to ISO 216 or ANSI/ASME Y14.1 generated or recorded Remotely or (ii) an email, SMS, or XML file generated or recorded Remotely;

"Page Allowance" means the number of Pages which Customer is authorized to process in an Order Year in consideration of the annual fees, all being specified or otherwise referred to in an Order Document;

"Remote" or "Remotely" means location of SmartCom owned or controlled infrastructure upon which the SmartCom Technology operates;

"Storage Allowance" means the space as specified in an Order Document which is available on SmartCom's systems for storage of Data.

b. Pricing:

i. CCM subscriptions are priced on a Page Allowance basis. Additional fees will be charged for usage in excess of the annual Page Allowance.

ii. Unused Pages cannot be carried over to the next Order Year.

iii. Non-finalized Interactive Pages are the total number of Interactive Pages that have been created but are not Final Output. At the end of each Order Year, non-finalized Interactive Pages will be deemed Final Output for the purpose of calculating whether the total number of Interactive Pages are within the Page Allowance.

iv. Each Page processed by Migration Studio shall be deemed to be a Remote Non-Interactive Page for the purposes of determining if the Volumes exceed the Page Allowance. Reseller reserves the right to restrict usage of Migration Studio to not more than 5,000 Pages in any twenty-four (24) hour period.

v. Non-prepaid fees such as fees for excess usage and excess storage are invoiced quarterly in arrears; however, Supplier may elect to aggregate these fees over more than one quarter prior to invoicing for administrative convenience.

c. Allowances:

i. Customer's Storage Allowance is 1GB per Tenancy. Additional storage usage will be charged an additional fee.

ii. Customer is permitted to process up to 200 Pages per minute for each million Pages of Page Allowance. For example, if the Page Allowance is 10 Million Pages, then up to 2,000 Pages per minute are permitted. Maximum concurrent requests are 1 per million Remote Pages of Page Allowance. If Customer exceeds the above limits by 100% on any single occasion, or on three or more occasions in a calendar month, Supplier reserves the right to restrict Customer's throughput to levels set forth herein.

4. SmartCom Service - SmartIQ ("SmartIQ Service(s)") Service Description

a. Definitions:

"Finalized Transaction" means each Transaction that is finalized by a User or external invitee executing the submit

function of the SmartIQ Services;

"Interim Transaction" means each Transaction that is not a Finalized Transaction;

"Local" or "Locally" means locations owned or otherwise controlled by Customer at which Data is processed;

"Order Year" means each twelve (12) month consecutive period beginning from the commencement of the License Term;

"Overage Unit" means blocks of ten percent (10%) of the Transaction Allowance;

"Remote" or "Remotely" means location of SmartCom owned or controlled infrastructure upon which the SmartCom Technology operates;

"Session" means each instance where a User or external invitee creates or accesses a Transaction;

"SmartIQ External User" means any User with access to SmartIQ Produce other than a SmartIQ Internal User;

"SmartIQ Internal User" means a User who is an employee or agent of Customer or its Affiliates granted access to SmartIQ Produce;

"SmartIQ Produce" means the run-time capability of the SmartIQ Services for the processing of Transactions currently branded as 'Produce';

"SmartIQ Solution" means SmartCom's solutions branded as 'SmartIQ' as at the Effective Date;

"SmartIQ Tenancy" means a single Tenancy running the SmartIQ Solution;

"Storage Allowance" means the amount of storage provided in each SmartIQ Tenancy;

"Transaction" means each instance where a User or external invitee initiates a workflow process or interview

process within the SmartIQ Solution,

"Transaction Allowance" means the number of Finalized Transactions which Customer is authorized to process in an Order Year in consideration of the Annual Fee, all being specified or otherwise referred to in an Order.

b. Pricing:

i. CCM subscriptions are priced on a Transaction Allowance basis. Additional fees will be charged for usage in excess of the annual Transaction Allowance.

ii. Unused Pages cannot be carried over to the next Order Year.

iii. At the end of each Order Year, each Interim Transaction shall be deemed a Finalized Transaction for the purposes of determining whether the Volumes exceed the Transaction Allowance.

iv. Non-prepaid fees such as fees for excess usage and excess storage are invoiced quarterly in arrears; however, Supplier may elect to aggregate these fees over more than one quarter prior to invoicing for administrative convenience.

c. Allowances:

i. Customer's Storage Allowance is 5GB per SmartIQ Service Tenancy. Additional storage usage will be charged an additional fee.

ii. The total number of Sessions in any twenty-four (24) hour period may not exceed five percent (5%) of the Transaction Allowance. If Customer exceeds the Peak Allowance, Supplier reserves the right to restrict Customer's throughput to the levels set forth herein.

Swisscom Trust Services Ltd.

These terms and conditions are applicable to all purchases of Swisscom Trust Services Ltd ("STS") Products ("STS Products") from Supplier (the "STS Terms"). Notwithstanding anything to the contrary, the STS Terms take precedence over any conflicting terms.

1. Customer agrees to the applicable STS Product service description ("Product Description") and "STS basic document dated 01.04.2021" at https://trustservices.swisscom.com/en/downloads. Supplier expressly does not promise services more extensive than those defined by STS in the Service Description.
2. Customer shall not assert a contractual claim against STS, Swisscom (Switzerland) LTD or Swisscom IT Services Finance S.E.
3. Orders for STS Products are not valid until STS approves of the order between Supplier and STS.
4. Orders for recurring services shall be concluded for an indefinite term with regard to the continuous obligation contained therein and may be terminated at any time unless otherwise provided, subject to three (3) months' written notice, to take effect at the end of a calendar month. If a minimum contract term has been agreed upon, termination is possible at the earliest at the end of the term. It is also possible to terminate only individual partial services, subject to compliance with the notice period in force in each case.
5. Supplier may terminate the STS Products without notice for good cause. Good cause shall exist in situations including but not limited to the following:

   a) the occurrence of events or circumstances that make continuing the agreed cooperation under the relevant contracts unreasonable for the terminating Party, including but not limited to the persistent serious breach of material contractual duties by the other Party;
   b) the official publication of an application for bankruptcy in respect of the other Party or a moratorium granted to it.
   c) the incomplete payment of an advance payment or of other contractually owed collateral;
   d) failure to comply with the rectification deadlines and failure to rectify any serious non-conformity identified in the context of the certification or trust service (according to the recognition authority's assessment scheme pursuant to the applicable signature legislation);
   e) any failure on the part of Customer to comply with material obligations set forth in the Service Description or any other obligations that may trigger a liability case for the trust services.

   If a breach of contract can be remedied by a party, the other party must warn such party in writing and grant it a period of 60 calendar days to remedy the breach before declaring the termination.

6. Customer warrants that it is located in Switzerland, the European Union, or the European Economic Area.
7. **Trust service of Swisscom**. The technical provisioning and the operation of the All-in Signing Service is done by Swisscom in Switzerland. Swisscom (Switzerland) Ltd is an accredited provider in Switzerland of certification services in accordance with the Federal Act on Electronic Signatures (ESigA) ZertES and Swisscom IT Services Finance S.E. is an accredited provider in Austria of trust services in accordance with the eIDAS Regulation. Supplier acts as a reseller of Swisscom services to the Customer. In view of the above, the Customer agrees that Supplier may disclose to Swisscom the contents of the AIS Contract as well as personal and technical Customer data for the purpose of the provisioning and operation of the All-in Signing Service, to the extent necessary for the implementation of the commercial and technical aspects between Supplier and Swisscom.
8. **Valid declaration of configuration and acceptance of Swisscom contracts as prerequisites**.

   The Customer must provide a written declaration of configuration and acceptance to the provider of the trust service, i.e. to Swisscom (Switzerland) Ltd or Swisscom IT Services Finance S.E. This permits Swisscom to activate the service for the Customer and to make the necessary arrangements for this purpose. Depending upon the type of identification process selected by the Customer, additional contracts may need to be concluded between the Customer and Swisscom (hereafter referred to as "Additional Contracts"), including in particular:
   - If using the RA app: an RA agency contract (including provisions concerning data protection).
   - If registration authority activity is carried out by the Customer: a contract for the delegation of personal identification (including provisions concerning data protection, based on the Customer's implementation concept).
   - If there are other processes agreed upon specifically for the individual Customer: an agreement regarding the process in question, based on the Customer's implementation concept.

   This Contract shall be valid subject to the condition precedent of acceptance by Swisscom, on the one hand, of the declaration of configuration and acceptance, and on the other hand, of the Additional Contracts and implementation concepts as required pursuant to applicable regulations:
   - Implementation concepts required pursuant to applicable regulations shall be deemed to have been accepted by Swisscom upon its express confirmation either in writing or by email.
   - The Additional Contracts required pursuant to applicable regulations are accepted by Swisscom upon its signature thereof.

- The declaration of configuration and acceptance shall be deemed to have been accepted unless it is objected to due to deficiencies within 14 days of its receipt by Swisscom or if following an initial objection due to deficiencies, it is expressly accepted either in writing or by email.

In view of the above, the Customer confirms that it has received the documents applicable to its Subscriber application.

9. Information obligations

Except as prohibited by statutory or contractual confidentiality obligations, each of the parties shall inform the other of any developments, incidents, and findings that may be relevant for the other party in connection with the performance of the contract or for the contractual relationship as a whole.

10. Proprietary and usage rights

Supplier grants to Customer, for use by Customer itself, a non-transferrable, non-exclusive right, which shall be limited to the duration of this Contract, to use the services of Supplier specified in the contracts.

All rights to intellectual property existing or arising at the time of performance of the Contract (copyright, patent rights, know-how, etc.) relating to services of Supplier shall be retained by Supplier or the third party rights holder (such as e.g. Swisscom). Neither is restricted in otherwise exploiting or using this intellectual property, nor is either under any duty to Customer in respect of the same. If the parties have developed intellectual property jointly, they authorise each other permanently to use and exploit these rights independently of each other without restriction, subject to confidentiality obligations. The Customer acknowledges the legal validity of the intellectual property rights of Supplier and of any third parties (such as e.g. Swisscom) regarding the services performed by Supplier and shall take no actions that might impair the value of the same. It shall take all actions within its means to prevent any unauthorised use. This paragraph shall survive the termination of the contracts.

TeleSign

1. "Licensed Data" means the results returned to Client by or on behalf of TeleSign in response to Client submitting Client Data as part of the Services.
2. Customer obligations
   a) Customer will comply with, and will ensure that its users ("Customer Uses") will comply with: obligations regarding use of the Telesign services as set out in TeleSign's Acceptable Use Policy for review at https://www.telesign.com/acceptable-use-policy, and with all applicable laws and data privacy laws.
   b) Users' use of the Service may be conditional to Users' consent to terms of use set out by third party telecommunications operators, international aggregators, and/or carriers ("Carrier"), or to the Carriers' consent to Users' use of said third party operators' service. Customer acknowledges that each Carrier may have different regulations, whereupon the Carriers' service terms may be paramount.
3. Customer will reasonably cooperate with TeleSign to confirm Customer's or Users' consent to disclosure of Customer data to Carriers for the limited purpose of enabling the provision of the Service and for TeleSign's compliance with the terms of its agreements with the Carriers.
4. As applicable, Customer authorizes TeleSign to provide its identification information ("Caller ID") to relevant Carriers for the Caller ID Management Service and TeleSign may disclose the Caller ID with respect to a specific subscriber in response to a call.
5. Customer shall provide all Users with any disclosure or explanation required by applicable laws concerning the Customer's use of the Services, and obtain, maintain and secure any necessary consent and authorizations from Users that may be required by applicable laws in order to authorize TeleSign's provision of the Telesign services, or otherwise procure lawful use by the Users of TeleSign services, and cooperate with TeleSign in ensuring lawful processing of User data, including any Personal Data, for the provision of the Telesign services.
6. In its use of the Services, it will: (a) comply with Telesign's Acceptable Use Policy; (b) use the Telesign services and the Licensed Data in compliance with all Applicable laws and applicable data privacy laws.
7. Upon termination of the Service or the Contract, TeleSign may retain, use, and disclose Customer usage data: (a) for the duration of TeleSign's accounting, tax, billing, audit, and compliance purposes; (b) to investigate fraud, spam, or unlawful use of the Telesign services; and/or (c) as required and for the limited duration allowed by applicable law.

Twilio

Customer obligations

1. Customer will comply with Twilio's Acceptable Use Policy located at: https://www.twilio.com/legal/aup;
2. Customer is responsible for ensuring that the phone numbers used for the Twilio services are up to date. Failure to do so will result in failed SMS text messages, for which Customer must pay SMS authentication charges;
3. Customer agrees to provide Supplier and Twilio reasonable cooperation regarding information requests from law enforcement, regulators, or telecommunications providers;
4. Customer instructs Supplier and Twilio to use and disclose Twilio Data to: (a) provide the Services consistent with Twilio's then-current Privacy Policy available at https://www.twilio.com/legal/privacy, including detecting, preventing, and investigating security incidents, fraud, spam, or unlawful use of the Services and (b) respond to any technical problems or Customer queries and ensure the proper working of the Twilio services;

5. Subject to the DPA between Customer and Supplier, Customer agrees that Supplier may grant Twilio a right to retain, use, and disclose Twilio Usage Data: (a) for the duration of Twilio's accounting, tax, billing, audit, and compliance purposes; (b) to investigate fraud, spam, or unlawful use of the Services; and/or (c) as required by applicable Law in accordance with the durations fixed by Law, provided that the retention, use, and disclosure of such Customer Usage Data for the foregoing purposes is subject to the confidentiality obligations as set forth in Customer's agreement with Supplier. Supplier contractually requires that Twilio anonymize or otherwise delete Twilio Usage Data when Twilio no longer requires it for the foregoing purposes;
6. Twilio may retain Twilio Content or any portion thereof if required by applicable law; and
7. If Customer records or monitors telephone calls, SMS messages, or other communications using the Twilio services, then Customer will comply with all applicable laws prior to doing so at all times. Customer must obtain prior consent to record or monitor communications using the Twilio services. Customer agrees to indemnify Supplier in accordance to the indemnification requirements located in the Master Terms for claims arising out of or related to Customer's acts or omissions in connection with recording or monitoring telephone calls, SMS messages, or other communications, whether such claims arise under contract, tort, statute of other legal theory.

Definitions:

a) "Twilio Content" means (a) content exchanged by means of use of the Twilio Services, such as text, message bodies, voice and video media, images, and sound; and (b) data stored on Customer's behalf via the Twilio services such as communication logs.

b) "Twilio Data" means the Users' phone numbers, one-time pass codes, and any other information contained in the authentication SMS text provided as part of the SMS Authentication Component that is processed through the Twilio authentication service.

c) "Twilio Usage Data" means data processed by Twilio for the purposes of transmitting, distributing or exchanging Twilio Content; including data used to trace and identify the source and destination of a communication, such as individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the Twilio Services, and the date, time, duration and the type of communication.

Veridas Digital Authentication Solutions S.L.

Veridas Digital Authentication Solutions S.L. ("Veridas") provides identity document verification services to OneSpan for its OneSpan Identity Document Verification Product ("IDV"). The following terms apply to the provision of the Veridas service (the "Veridas Service"):

1. Product Testing:
   The Veridas Service is available for testing in IDV's Staging/Testing and Development environment. When used in the Staging/Testing and Development environment, it is not subject to the Service Levels and data security requirements; as such, Customer acknowledges that Personal Data and production Data provided as testing data:
   - IS NOTWITHSTANDING ANYTHING IN THIS CONTRACT, PROVIDED "AS-IS", WITHOUT ANY WARRANTY, SERVICE LEVELS, LIABILITY OR INDEMNITY OBLIGATIONS;
   - may be accessed by OneSpan and third party personnel; and
   - may be accessed, processed and stored by a third party service provider in the US and the European Economic Area.
2. Product Support:
   Support for the Veridas Service may include the provision of support services by Veridas and OneSpan personal who may access, process, and store Data from the US and/or Europe.
3. **Customer acknowledges that the Veridas Service has an associated error rate that makes it impossible, by the very state of the art, to guarantee total reliability. There are methods for generating false documents, images and audio files with a level of sophistication that makes their detection virtually impossible**.

Workato, Inc.

The following terms apply to the provision of the OneSpan Sign Integration Platform service:

1. Customer agrees to be bound by Workato's Embedded Software Supplement Terms located at: https://www.workato.com/legal/embedded-software-supplemental-terms
2. You hereby agre that Workato may collect, use, share, and protect the personal information it collects about individuals according to the Workato Services Privacy Policy ("**Privacy Policy**"), found at https://www.workato.com/legal/privacy-policy/services-privacy-policy.
3. If Supplier reasonably determines that Customer is in breach of Workato's Embedded Software Supplement Terms or otherwise engaging in any actions that threaten the security, integrity, availability or stability of the Workato Embedded Edition, Supplier may immediately suspend the applicable Customer account.