ATTACHMENT A
END-USER AGREEMENT

This End-User Agreement ("**Agreement**") is an integral part and bound to the terms of the Master Cloud Services Partner Reseller Agreement (the "**Main Agreement**") effective as of February 28, 2023 (the "**Effective Date**") by and between Incode Technologies, Inc., a Delaware corporation, with an address at 221 Main Street, Suite 520, San Francisco, CA 94105 ("**Incode**") and Frankie Financial Pty Ltd, an Australian company with an address at 121 King Street, Melbourne, VIC 3000 ("**Partner**").

Partner agrees that, pursuant to Section 1.1 of the Main Agreement, Partner will require each Client to be bound by a written agreement with Partner (collectively the "**Client Agreement**") that contains (i) substantially similar mandatory "flow down" provisions as included herein that are at least as favorable to Incode, with respect to the Incode Software and Services, as the terms in this Attachment A; (ii) a verbatim copy of Attachment A.1 which shall be incorporated in any and all Client Agreements entered into by Partner and Client, and although Partner is not required to monitor each Client compliance with using such language in their Service, Partner hereby agrees to "flow down" such consent language to the Clients so it can implement it; and (iii) substantially similar "flow down" the terms of the Data Processing Agreement ("**DPA**"), as required in a given Territory and, except in relation to the transfer mechanism applicable to Incode Data in the DPA ("Incode Transfer Mechanism) which shall also be accepted by Client as verbatim. If Partner considers that it will not be able to comply with the afore requirements, prior to entering into a Client Agreement, Partner must request Incode's approval of any deviations whatsoever from Attachment A.1 and/or the Incode Transfer Mechanism. For the avoidance of doubt it's the Partner's sole responsibility to enter into the applicable data processing agreement with its Clients, which ensure terms consistent with the DPA entered into by Incode and Partner; otherwise Partner shall ensure it has obtained Incode's prior written acceptance to such terms prior to entering into the Client Agreement. Failure to do so may result in Incode's refusal to provide Services to Clients. To the extent used in this Attachment, "**Service(s)**" shall mean the applicable Incode Software and Services provided by Incode to Partner in connection with the Client Agreement. All other capitalized terms that are not defined herein shall have the meaning set forth in Main Agreement.

1. **License Grant.** During the Term, Incode hereby grants Client a nonexclusive, limited, personal, non-sublicensable, nontransferable right and license to use and access the Services, only for the internal business purposes of Client and only in accordance with Incode Documentation (as defined herein below). No other rights or licenses are granted except as expressly and unambiguously set forth herein. Incode Documentation means Incode's usage guidelines and standard technical documentation for the Software, the current version of which is available at:

- iOS SDK Sample: https://github.com/Incode-Technologies-Example-Repos/Incode-Welcome-Example-iOS
- Android SDK Sample: https://github.com/Incode-Technologies-Example-Repos/Incode-Welcome-Android-example
- Web SDK Sample: https://docs.incode.com/docs/web/sample-tutorials/Example_Implementation

2. **License Restrictions.** Client shall not (and shall not permit any third party to), directly or indirectly: (a) reverse engineer, decompile, disassemble, or otherwise attempt to discover the underlying structure of the Service (except to the extent applicable laws specifically prohibit such restriction); (b) modify, translate, or create derivative works based on the Service; (c) transfer or encumber rights to the Service; (c) use the Service for the benefit of a third party; (d) remove or otherwise alter any proprietary notices from the Service or any portion thereof; (e) use the Service to build an application or product that is competitive with any Incode product or service; (f) interfere or attempt to interfere with the proper working of the Service or any activities conducted on the Service; (g) bypass any measures Incode may use to prevent or restrict access to the Service (or other accounts, computer systems or networks connected to the Service); (h) use the Service for the design or development of nuclear, chemical or biological weapons or missile technology, or for terrorist activity, without the prior permission of the United States government; or (i) allow any third party to remove or export from the United States or Mexico or allow the export or re-export of any part of the Software or any direct product thereof (i) into (or to a national or resident of) any embargoed or terrorist-supporting country, (ii) to anyone on the U.S. Commerce Department's Table of Denial Orders or U.S. Treasury Department's list of Specially Designated Nationals, (iii) to any country to which such export or re-export is restricted or prohibited, or as to which the United States government or any agency thereof requires an export license or other governmental approval at the time of export or re-export without first obtaining such license or approval or (iv) otherwise in violation of any export or import restrictions, laws or regulations of any United States or foreign agency or authority. The Software may incorporate third-party open source software

(“OSS”). To the extent required by the OSS license, that license will apply to the OSS on a stand-alone basis. Client is responsible for all of Client’s activity in connection with the Service, including but not limited to uploading Client Data onto the Service. Client shall warrant that it is not located in, under the control of or a national or resident of any such prohibited country or on any such prohibited party list. Client: (A) shall use the Service in compliance with all applicable laws, treaties and regulations in connection with Client’s use of the Service, and (B) shall not use the Service in a manner that violates any third party rights. **This provision shall survive any expiration or termination of the Client Agreement.**

3. **Client Data.** Client, is solely responsible for the accuracy, integrity, and legality of Client Data. Client represents and warrants that it owns all right, title and interest in and to the Client Data or otherwise has sufficient rights to such data to permit its use as contemplated hereunder. Incode is not responsible to Client, for unauthorized access to Client Data or the unauthorized use of the Service. The parties acknowledge and agree that any data personal and specific to an individual is owned by such individual. Client acknowledges and agrees that Incode may use the Client Data to (i) provide the Services to Client; and (ii) improving or modifying Incode´s technology (including its algorithms) for the purposes included in Incode - Privacy Notice, provided it has an appropriate legal basis (as set out in Attachment A.1 herein, which Client undertakes to includes on the Client end-user flow and provide the results of the same to Incode directly and in real time) from the Clients end-users’ before any end-user accesses the Services and prior to the collection of the end-users selfie and government issued identification document, (this shall be considered “Incode Data”) and (iii) freely use and make available Aggregated Anonymous Data for Incode’s business purposes (including without limitation, for purposes of improving, testing, operating, promoting and marketing Incode’s products and services) notwithstanding anything herein to the contrary. “Aggregated Anonymous Data” means data submitted to, collected by, or generated by Incode in connection with Client’s use of the Service in aggregated, anonymized form which cannot be linked to Client or identifies any individual person. **This provision shall survive any expiration or termination of the Client Agreement.** Client shall acknowledge and agree that Client shall be solely responsible for requesting individuals the end-users’ consent for the afore purposes.

4. **Infrastructure services.** Client acknowledges and agrees that the Service may use services provided by third parties. Any exchange of data or other interaction between Client and a third party provider is solely between Client and such third party provider and is governed by such third party’s terms and conditions.

5. **Suspension of Services; Effect of Termination.** Incode may suspend or limit Client’s access to or use of the Service if Client’s use of the Service results in (or is reasonably likely to result in) damage to or material degradation of the Service which interferes with Incode’s ability to provide access to the Service to other Incode customers. Upon expiration or earlier termination of the [Client Agreement], all license granted to Client will cease, and Client must immediately cease using the Software and delete (or, upon request, return) all copies of the Software. At Incode’s request, Partner will ensure that Client deletes all of Incode’s Confidential Information. Confidential Information may be retained in the Incode’s standard backups after deletion but will remain subject to the Agreement’s confidentiality and non-use restrictions. **This provision shall survive any expiration or termination of the Client Agreement.**

6. **Disclaimer of Warranties.** THE SERVICE IS PROVIDED “AS IS” AND “AS AVAILABLE” AND ARE WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES IMPLIED BY ANY COURSE OF PERFORMANCE, USAGE OF TRADE, OR COURSE OF DEALING, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. INCODE DOES NOT WARRANT ANY THIRD PARTY SERVICES OR THAT CLIENT’S OR CLIENT’S PARTNER (AS THE CASE MAY BE), USE OF THE SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE OR THAT ANY SECURITY MECHANISMS IMPLEMENTED BY THE SERVICE WILL NOT HAVE INHERENT LIMITATIONS. **This provision shall survive any expiration or termination of the Client Agreement.**

7. **Limitation of Liability.** EXCEPT FOR CLIENT’S BREACH OF THE LICENSE RESTRICTIONS OF THE AGREEMENT IN NO EVENT SHALL EITHER PARTY, NOR ITS DIRECTORS, EMPLOYEES, AGENTS, PARTNERS, SUPPLIERS OR CONTENT PROVIDERS, BE LIABLE UNDER CONTRACT, TORT, STRICT LIABILITY, NEGLIGENCE OR ANY OTHER LEGAL OR EQUITABLE THEORY WITH RESPECT TO THE SUBJECT MATTER OF THE AGREEMENT (A) FOR ANY LOST PROFITS, DATA LOSS, COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR SPECIAL, INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES OF ANY KIND WHATSOEVER, SUBSTITUTE GOODS OR SERVICES (HOWEVER ARISING), (B) FOR ANY BUGS, VIRUSES, TROJAN HORSES, OR THE LIKE (REGARDLESS OF THE SOURCE OF ORIGINATION), OR (C) FOR ANY DIRECT DAMAGES IN EXCESS OF

(IN THE AGGREGATE) THE FEES PAID (OR PAYABLE) TO INCODE WITH RESPECT TO THE LICENSE GRANTED HEREUNDER IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO A CLAIM HEREUNDER. **This provision shall survive any expiration or termination of the Client Agreement.**

8. **Force Majeure.** Incode will not be liable for any delay or failure to perform the Service due to events beyond its reasonable control, such as a strike, blockade, war, act of terrorism, riot, infrastructure services provided by third party providers, Internet or utility failures, refusal of government license or natural disaster.

9. **Federal End Users.** The Services are "commercial products" (as defined at Federal Acquisition Regulation (FAR) 2.101) and are "commercial computer software" (as defined at FAR 2.101). If the Client or end user of the Services is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Services, Software or any related Documentation of any kind, including technical data and manuals, is restricted by the terms of Federal End User Agreement in accordance with FAR 12.212 for civilian agency use and Defense Federal Acquisition Regulation Supplement (DFARS) 227.7202 for agencies within the Department of Defense. All other use is prohibited.

ATTACHMENT A1
CONSENT REQUEST

CLIENT DATA AND INCODE'S CONSENT REQUEST

This document contains the Parties agreement with respect to the applicable conditions for Incode to process Client Data and is applicable to the licensing of Incode Services to Client under the applicable agreement. Client understands that compliance with the terms below, as applicable, is material for Incode to properly process the Client Data under the Agreement and though any breach by Client of the conditions below will be considered a material breach under the Agreement. Any terms not defined herein shall have the meaning set forth in the applicable agreement.

I. CONSENT TERMS AND CONDITIONS.

1. **Definitions:**
   "End User" means an individual that is authorized by Client to use and/or access its products or services.

2. **Consent in respect of End Users in the United States of America.** Before any End-User accesses the Services and prior to the collection of their selfie and government issued identification document: (i) Client agrees to display the joint consent language included in part II a. herein below ("Joint Consent Language"), on its website and/or application, to End-Users located in the United States. In case an End-User does not provide consent to Client verifying their identity through the Services (by ticking the first checkbox of the Joint Consent Language), Client shall not allow such End-User to access the Services and doing otherwise shall be a material breach of this Agreement by Client. Biometric Information (as defined in the consent language below), shall be deleted by Incode immediately upon the cessation of the provision of Services to End-Users to comply with Applicable Laws and that therefore, depending on the Services purchased by Client, additional consent to process Biometric Information for the purpose of providing the Services may be required by the parties in the future. (ii) Simultaneously with Client, Incode shall be entitled to process the End-User's personal data, including Biometric Data (i.e. Incode Data) provided it has obtained the End-Users' affirmative consent to improve its products and services, including the Services, through the second checkbox of the Joint Consent Language. For the avoidance of doubt, Incode shall only process Incode Data in the event the End-User has provided their consent to Incode. Notwithstanding the foregoing, Incode may retain Incode Data, including Biometric Data, for such longer period as permitted under Applicable Laws. Client must provide Incode with the End-User affirmative consents required in sections 2(i) and 2(ii) herein in real-time for Incode's record keeping purposes and provision of Services.

3. **Consent in respect of End Users in the rest of the World**. Before any End-User accesses the Services and prior to the collection of their selfie and government issued identification document: (i) If in a given Territory Client is required to request consent from its End-users to be able to process their personal data pursuant to applicable laws, Client shall not allow the End-user to access the Services if such consent is not obtained and doing otherwise shall be a material breach of this Agreement by Client, however if Client has a legitimate basis to process the Client Data in accordance with clause 3 of the agreement, Client must immediately inform Incode and then only the following section (ii) shall apply; (ii) Client acknowledges and agrees to display the Incode consent wording set forth in section II b below for the purpose of developing, modifying and improving the Incode products and services, including the Services with Incode Data, in accordance with the agreement. For the avoidance of doubt, Incode shall only process personal data, including Biometric Data, for the purposes in this section 3(ii) so long as the End-user has provided its consent to Incode. Client must provide Incode with the End-User affirmative consents required in sections 3(i) and 3(ii) herein in real-time for Incode's record keeping purposes and provision of Services.

4. As defined in applicable data protection laws, Incode shall be a (sub-)Processor of Client Data for the purposes of section 3.2(i) and an independent Controller of Incode Data for the purposes of section 3.2(ii). Client acknowledges and agrees to display the consent language herein (as applicable to the Territory) for

such purposes and to make the consent acceptance or denial available to Incode before the processing of any Client Data or Incode Data by Incode pursuant to the provisions herein.

5. **Consent Implementation.** For the implementation of the applicable consent under any of the situations in sections 2 and 3 above, Client agrees as follows:
   i) If implementation is done via SDK, Client agrees to enable "Incode Consent Module" into the flow in order to get End User Consent as detailed above so that Incode can receive a record of such consents in real- time.
   ii) If implementation is done through APIs, Client acknowledges and agrees that it will include within its web flow a screen with the applicable consent wording as described above and it will include the record of the applicable consent provided by the End User together with the Client Data sent to Incode for processing via APIs. Client acknowledges that inclusion of the consent record is mandatory for Incode to process the applicable Client Data.
      a. **In the case of API implementation, Client shall ensure to delete all Incode Data immediately upon transmission to Incode**

6. **Updates to the language.** If the consent wording herein needs to be amended for a specific Territory, the Parties will work together in implementing such adjustments, in the understanding that the Services will not be provided by Incode until required adjustments are made to comply with Applicable Laws in such territories. However, Incode shall not require the Client consent to amend the Incode consent wording for processing of Incode Data.

II. CONSENT LANGUAGE.

a. **United States.** In accordance with clause 3 of the Agreement and the terms and conditions of this Attachment A.1, the Client agrees to include the following consent modules before End-users may access the Services in the United States, through an un-checked/ checkbox module:

Consent and Written Release for the Collection, Use, Disclosure and Storage of Personal Data, including Biometric Information

In order to verify that you are the person depicted in your government-issued identification, [CLIENT'S LEGAL NAME] (hereinafter, "[client dba name]") uses third-party technology from Incode Technologies, Inc. (hereinafter "Incode") to collect personal data and/or information from or about you, including biometric information and biometric identifiers such as your faceprint ("**Biometric Information**"), a selfie, and government-issued identification, including information obtained by scanning the barcode (collectively with Biometric Information, "**Personal Data**"). Specifically, [client dba name] and/or Incode will ask you to take a selfie through the Incode Omni Powered by Incode platform through [client dba name]'s web and/or native application. Incode will then scan and map your facial features in comparison with the picture on your government-issued identification to allow you to create and/or access your account with [client dba name]. Incode may also share your Personal Data, including your Biometric Information, with a third-party identification service provider or the Department of Motor Vehicles to verify your identity.

Biometric Information: [client dba name] and Incode may use your Personal Data, including Biometric Information for the following purposes (as applicable), in each case as further described in [client dba name] Privacy Policy [INSERT LINK] and/or Incode's Privacy Policy:

- To provide the services for which the Personal Data was provided;
- To improve or modify Incode's products and services; and
- To comply with [client dba name] or Incode's obligations under applicable law.

Note that [client dba name]and/or Incode may disclose your Biometric Information to [client dba name]'s and/or Incode's service providers, and as otherwise required under applicable law.

You can request that [client dba name] and/or Incode delete your Personal Data, including your Biometric Information at any time by emailing [client dba name] at [client email] or Incode at legalcompliance@incode.com. If you request deletion of your Personal Data, Incode will not be able to recover it at a later point. [client dba name] will permanently delete Biometric Information that it processes (if any) for its own purposes by the earlier of: (i) the time at which the purpose for which it was collected has been satisfied; or (ii) three years after your last interaction with Incode. Incode will permanently delete Biometric Information that it processes on behalf of [client dba name] as instructed by [client dba name], or for Incode's own purposes, by the earlier of: (i) the time at which the purpose for which it was collected has been satisfied; or (ii) three years after your last interaction with Incode.

Government Identification Information: Using Incode Omni on the [client dba name] website and/or application requires Incode to take a picture of the front and back of: (1) your driver's license or state-issued identification card; or (2) your U.S. passport. This allows Incode to compare the photo with the image of you that Incode will capture through the "Let's Take a Selfie" function. Incode will also collect other information that is on the front and back of your driver's license, state-issued identification card, or U.S. passport, including by scanning the barcode and collecting information derived from the barcode (e.g., name, date of birth, height). We use this information primarily to verify your identity and to prevent fraud. We may also us this information to improve our products and services.

Consent:

□ By ticking this box and providing [client dba name] with your Personal Data, including your Biometric Information and government identification information, you consent to [client dba name]'s and Incode's collection, storage, retention, use and disclosure of such information to provide the identity verification services, consistent with [client dba name] Privacy Notice which you may find at [INSERT LINK] and consistent with [client dba name] Terms of Use which you may find at [INSERT LINK]. Even if you consent, you can subsequently withdraw consent at any time.

□ By ticking this box and providing Incode with your Personal Data, including your Biometric Information and government identification information, you consent to and provide a written release to Incode for the collection, storage, retention, use and disclosure of such information to improve or modify Incode's products or services, consistent with Incode's Privacy Notice. Your consent is voluntarily given, and you are under no obligation to consent. Even if you consent, you can subsequently withdraw consent at any time. If you do not provide consent to Incode, Incode will not process your Personal Data for purposes of improving Incode's products or services, even if you consented to use of your Personal Data for identity verification services which you may still receive.

b. **All countries except the United States of America.** In accordance with section 3(ii) above and the terms of the agreement, Client hereby acknowledges and agrees that Incode is entitled to request consent from End-users following Client's own consent request (where necessary), through an un-checked/ checkbox module:

[ ] I hereby give my consent to the collection, use and storage by Incode Technologies, Inc. ("Incode") of my personal data, including a digital map of my unique facial features (a type of biometric data), for the purposes of improving or modifying Incode's technology (including its algorithm) and updating its products and services, in accordance with its Privacy Notice. You can exercise your rights, including withdrawal of consent, contacting legalcompliace@incode.com.

IMPORTANT: Your consent is voluntary, even if you do not consent, you will still be able to access the [Client dba name] services.