

## GLOBAL APPLE ACCESS PARTNER+ AGREEMENT

This Global Apple Access+ Partner Agreement (this “Agreement”) effective on the date last signed below (“Effective Date”) sets out the terms and conditions on which Apple Inc. (“Apple”) and Alert Enterprises Inc. having a place of business at the address set forth below (the “Access Partner”). Apple and Access Partner may each be referred to herein as a “Party” or collectively as the “Parties”.

### Access Program Requirements

1. **Apple Responsibilities.** This Agreement establishes the terms and conditions under which Apple will make available Apple Technology and the Apple Access Platform to Access Partner and will provision Credentials, managed by Access Partner and/or sold to Participating Providers by Access Partner, to enable Users to securely use Provisioned Credentials to make Transactions on Enabled Devices in the Territory (“Program”).
2. **Access Partner Responsibilities.** Subject to the terms and conditions of this Agreement, Access Partner will be responsible for:
  - a. the applicable obligations set forth in the Integration Approach Exhibit (any references in this Agreement to the Integration Approach Exhibit will mean **Exhibit B (Credential Manager Integration Approach, Features and Functionality)** when Access Partner is acting as a Credential Manager or **Exhibit C (Credential Provider Integration Approach, Features, and Functionality)** when Access Partner is acting as a Credential Provider);
  - b. providing the services set forth in this Agreement to a Participating Provider, including the Provisioned Credentials and/or Access Service Partner and Access Partner’s readers used to support the Program in accordance with the **Integration Approach Exhibit, Exhibit H (Supported Reader Models), Exhibit I (Credential Asset Management Program) and Exhibit M (Terminal/Reader Procurement)**);
  - c. ensuring the inclusion of a provision in each Participating Provider Agreement related to the Program that nothing contemplated under such agreement will result in a breach by a User of a User Agreement, including that the Participating Provider will amend its User Agreements if required to ensure there is no such breach;
  - d. where this Agreement identifies activities to be performed by a Participating Provider (including Sections 4 (Cooperation of the Parties), 10 (Confidentiality); 11 (Data Protection and Information Security) and 26 (Suspension and Termination), procuring that relevant Participating Providers perform such activities in accordance with applicable Law;
  - e. Access Partner, when acting as a Credential Manager, requiring that each Participating Provider receives and executes the Participating Provider Pass-Through Terms set forth in **Exhibit J-1**, as the same may change from time to time. Prior to sending the Participating Provider Pass-Through Terms to a party, Access Partner, when acting as Credential Manager, will ensure that each Participating Provider (and where applicable the relevant Service Provider):: 1) is not directly or indirectly controlled by or designated as a sanctioned party by any government

regulatory authority (including, but not limited to, the Office of Foreign Assets Control (OFAC)), and 2) has entered into confidentiality terms with Access Partner or where applicable, Access Partner's Service Provider that protects the confidentiality of the Program on terms at least as restrictive as those herein, including as provided in Section 10. Access Partner, when acting as Credential Manager, will provide written notice to Apple prior to the Participating Provider Pass-Through Terms being sent to any party requesting to participate in the Program. Access Partner, when acting as Credential Manager, will provide Apple a list of all new Participating Provider that have executed Participating Provider Pass-Through Terms on the 1st of the month after such terms are executed.

- f. implementing clear and user-friendly provisioning methods for Users in accordance with the reasonable instructions provided by Apple as well as the requirements set forth in the Integration Approach Exhibit;
- g. ensuring that the Provisioned Credentials are a safe and secure authentication method for Participating Providers and Users;
- h. ensuring that all NFC readers used to support the Program will support all Apple requirements for security and user experience as outlined in the Integration Approach Exhibit;
- i. implementing the marketing commitments to support of the Program within the Territory as sets forth in **Exhibit N (Marketing Commitment)**;
- j. ensuring that Transactions are not processed or declined, and Accounts or Credentials are not activated or suspended, solely on the basis of the use of the Program; and
- k. provide the following customer service and support:
  - i. support User provisioning of Credentials, the use of Provisioned Credentials and any activities of Access Partner in connection with such Provisioned Credentials;
  - ii. provide a level of customer service and operation support for the use of Provisioned Credentials, and the activities of Access Partner in connection with such Credentials (both in quality and the types of transactions that can be supported) reasonably comparable to the customer service that Access Partner provides for credentials, including physical credentials, as well as comparable inquiries on physical card transactions (whether such card used for such transactions had been provisioned or not) on Competing Platforms, taking into account any relevant differences in features and functionality of such credentials or transactions on the Competing Platforms;
  - iii. support availability, system availability, and up-time service availability for provisioning methods implemented in accordance with this Section 2 will be no lower than comparable availability for mobile and on-line Apple Access Services offered by the Access Partner on Competing Platforms; and

- iv. support each Access Service Partner or Participating Provider in the provision of the foregoing.

**3. Personnel and Subcontractors.**

- a. Either Party's personnel assigned to perform obligations under this Agreement on the other Party's premises will observe that other Party's security and safety policies and procedures while working on such premises. Such rules will be provided to a Party's personnel in reasonable time prior to the relevant personnel coming on such other Party's premises. Upon the hosting Party's request, the other Party will promptly replace any of its personnel performing any such duties on such premises. Each Party further agrees that upon the hosting Party's request it will acknowledge its compliance with the hosting Party's security policies and procedures in writing.
- b. It is acknowledged and agreed that, subject to Sections 10 (Confidentiality) and 11 (Data Protection and Information Security), either Party may use its Affiliates or Service Providers to perform functions of such Party hereunder in accordance with such Party's obligations under this Agreement; provided, however, no Party will be relieved of any obligations under this Agreement by virtue of having any such obligations performed by a Service Provider and that the Service Provider Party will:
  - i. perform thorough due diligence on any proposed Service Provider to ensure compliance with the applicable terms of this Agreement (which due diligence may include background checks, site visits, financial research and other investigation, as required);
  - ii. require in its agreements with Service Providers confidentiality and security measures at least as stringent as those herein, including as provided in Sections 10 (Confidentiality) and 11 (Data Protection and Information Security);
  - iii. provide any cooperation necessary to enable Apple and Access Partner to cooperate in accordance with this Agreement, including Section 4 (Cooperation of the Parties); and
  - iv. be responsible for the functions performed by Service Providers to the same extent such subcontracting Party would be responsible if it performed such obligations itself.
- c. Where required by Apple in its sole discretion, Access Partner will engage in quarterly reviews of the Program. Where applicable, such reviews may be held in person, via telephone, or via videoconference, provided that at least two (2) of such meetings occur in person each year.

**4. Cooperation of the Parties.**

- a. The Parties will work together to determine the Program Launch Date.

- b. Apple and Access Partner will cooperate in good faith to ensure (i) a superior experience for Users and Participating Providers, (ii) the proper functioning of the Apple Technology with Credentials issued by, or on behalf of, Participating Provider, and (iii) the proper and secure functioning of the Credential and products manufactured by Access Partner and used in the Program with effect from the Launch Date.
- c. Access Partner will provide written notice to Apple prior to Access Partner implementing changes to its respective systems, procedures, processes or functionality, which, as the case may be, may reasonably be expected to result in changes to or otherwise impact the Program (these changes to systems, procedures, processes or functionality are referred to as “System Changes”). In addition, and not by way of limitation, Access Partner will notify Apple not less than thirty (30) days prior to any System Changes that Access Partner reasonably believes will disable core functionality of the Apple Technology or introduce material additional security exposure to Apple, Users or Participating Providers; provided, the Parties will work in good faith to address any bona fide concerns of Apple with regard to such proposed change. If Apple objects to any System Changes, Apple may initiate the Executive Review process set forth in Section 29 (Executive Review) below.
- d. Apple will provide general guidelines on system testing, and with Access Partner’s cooperation, will develop a plan that provides coordinated delivery, testing, and overall project timelines. Access Partner will provide Apple with Credentials for testing in accordance with **Exhibit I (Credential Asset Management Program) and Exhibit M (Terminal/Reader Procurement)**.

5. **Marketing and Branding.**

- a. **Access Partner Trademark License.**
  - i. Subject to the terms of this Agreement, Access Partner (on behalf of itself and each of its Affiliates) hereby grants Apple and each of its Affiliates and Service Providers, during the Term, a non-exclusive, non-assignable (subject to Section 27 (Assignment)), non-transferable (subject to Section 27 (Assignment)), non-sublicensable, royalty-free, fully paid-up, worldwide right and license to use, reproduce, have reproduced, display, and have displayed any of the Access Partner Marks: (A) in connection with the use and display of the Apple Access Platform in Apple Products, including the right to embed and display any of the Access Partner Marks within such Apple Products; (B) in the marketing, advertising, and promotion of the Apple Access Platform and the Program in any medium, including the right to use screen shots and images of any of the Access Partner Marks, including use in instructional materials, training materials, marketing materials, and advertising in any medium; and (C) in a publicly disclosed list of the access partners that have entered into an agreement with Apple for the use of the Apple Access Platform in the applicable jurisdiction in the Territory. Use of the Access Partner Marks by Apple, its Affiliates or Service Providers will be pursuant to, and in accordance with, this Agreement and the Access Partner Brand Guidelines, unless otherwise agreed in writing by the Parties.

- ii. Apple acknowledges that: (A) the Access Partner Marks, all rights therein, and all goodwill associated therewith, are, and will remain, the exclusive property of Access Partner or one or more of its Affiliates; (B) neither Apple nor any of its Affiliates will take any action that can reasonably be expected to adversely affect Access Partner's or any of its Affiliates' exclusive ownership of the Access Partner Marks or the goodwill associated with the Access Partner Marks; (C) neither Access Partner nor any of its Affiliates will seek to register any Apple Mark, any colorable imitation thereof, or any Mark confusingly similar thereto; and (D) any and all goodwill arising from use of the Apple Marks pursuant to this Agreement will inure solely to the benefit of Apple and its Affiliates. Nothing in this Agreement will give Apple or any of its Affiliates any proprietary interest in or to any of the Access Partner Marks, except the limited right to use the Access Partner Marks in accordance with this Agreement, and neither Apple nor any of its Affiliates will contest, cause any other Person to contest, or assist any other Person in contesting Access Partner's or any of its Affiliates' title in and to any of the Access Partner Marks.
  - iii. Nothing in this Agreement will limit Apple's rights to freely market its own products and services. Apple will have no obligation to display or use any of the Access Partner Marks on or in connection with any Apple products or services or any Apple marketing, advertising or promotional materials for any Apple Products or services.
- b. **Apple Trademark License.**
- i. Subject to the terms of this Agreement, Apple (on behalf of itself and each of its Affiliates) hereby grants Access Partner and each of its Affiliates and Service Providers, during the Term, a non-exclusive, non-assignable (subject to Section 27 (Assignment)), non-transferable (subject to Section 27 (Assignment)), non-sublicensable, royalty-free, fully paid-up, worldwide right and license to use, reproduce, have reproduced, display, and have displayed any of the Apple Marks solely for the purposes of announcing and promoting Access Partner's participation in the Program, subject in all cases to Apple's prior written consent. Use of the Apple Marks by Access Partner, its Affiliates or Service Providers will be pursuant to, and in accordance with, this Agreement and the Apple Brand Guidelines, unless otherwise agreed in writing by the Parties. For the avoidance of doubt, in the event Access Partner wishes to use any of the Apple Marks in any paid advertising, Access Partner must first obtain Apple's written consent for such advertising.
  - ii. Access Partner acknowledges that: (A) the Apple Marks, all rights therein, and all goodwill associated therewith, are, and will remain, the exclusive property of Apple or one or more of its Affiliates; (B) neither Access Partner nor any of its Affiliates will take any action that can reasonably be expected to adversely affect Apple's or any of its Affiliates' exclusive ownership of the Apple Marks or the goodwill associated with the Apple Marks; (C) neither Access Partner nor any of its Affiliates will seek to register any Apple Mark, any colorable imitation thereof, or any Mark

confusingly similar thereto; and (D) any and all goodwill arising from use of the Apple Marks pursuant to this Agreement will inure solely to the benefit of Apple and its Affiliates. Nothing in this Agreement will give Access Partner or any of its Affiliates any proprietary interest in or to any of the Apple Marks, except the limited right to use the Apple Marks in accordance with this Agreement, and neither Access Partner nor any of its Affiliates will contest, cause any other Person to contest, or assist any other Person in contesting Apple's or any of its Affiliates' title in and to any of the Apple Marks.

- iii. Nothing in this Agreement will limit Access Partner's rights to freely market its own products and services. Access Partner will have no obligation to display or use any of the Apple Marks on or in connection with any Access Partner products or services or any Access Partner marketing, advertising or promotional materials for any Access Partner products or services.
- c. Subject to terms as specified in Section 26 (Suspension and Termination), upon the expiration or termination of this Agreement for any reason, each Party will promptly cease, and, as applicable, cause each of its Affiliates and Service Providers to promptly cease, all use of the other Party's Marks under this Agreement and will take prompt action to remove any reference to such Marks from both print and electronic media, including for marketing, promotional, and advertising purposes.
- d. In connection with the launch of Access Partner's participation in the Program, Apple may issue a press release announcing Access Partner's participation in the Program. Except as otherwise set forth in the preceding sentence, neither Party may issue a press release regarding Access Partner's participation in the Program without the other Party's prior written consent. Access Partner will not distribute any material communications to existing or prospective Users regarding major support issues for Apple Access Platform or new Apple Access Platform features without Apple's prior written consent.
- e. Except for general informational statements about the use of credentials on Competing Platforms, in no event will Access Partner promote or advertise the Program with any Competing Platform without Apple's prior written consent.

## 6. **Quiet Period.**

- a. During the period from thirty (30) calendar days prior to the Program Launch Date, to the date thirty (30) Calendar Days after the Program Launch Date, Access Partner will not promote, advertise, or participate in any public event launching (a) a new Competing Platform or (b) a major customer facing feature expansion on a Competing Platform, in each case to be offered in, or made available to customers resident in the Territory.
- b. Access Partner will not (without Apple's prior written consent) promote or advertise a Competing Platform within thirty (30) days of an Apple led initiative such as a press release or marketing campaign associated with the Credential service (an "Apple Initiative"). Apple will provide reasonable notice to Access

Partner of Apple Initiatives and the dates associated with Apple Initiatives. Access Partner will use best efforts to work with Participating Providers and other mobile wallet providers to avoid the release of any Competing Platform marketing materials within thirty (30) days of an Apple Initiative. Apple acknowledges that Access Partner will support, including promoting and advertising, mobile credentials on Competing Platforms. The Parties will work together in good faith to address any concerns or challenges in operationalizing the requirements in this provision.

**7. Fees.**

- a. Access Partner will pay the Fees in accordance with Section 8 (Payment) below, and the terms of **Exhibit G (Commercial Addendum)**, if applicable.
- b. For the avoidance of doubt, Access Partner agrees and acknowledges that in the event the Fees are disclosed to Participating Provider by Access Partner (or where applicable Access Partner's Service Provider), the Fees will be disclosed on a per Participating Provider basis. Access Partner shall not, and shall ensure that its Service Providers do not make any misrepresentation about such Fees to Participating Provider. Neither Access Partner, nor Access Partner's Service Provider, nor any Participating Provider, will charge Users any additional fees related directly to and solely for their participation in the Program.
- c. Access Partner will not and shall ensure that its Service Providers do not impose any Program-specific fees or other commercial terms on Participating Providers for such Participating Providers' use of, or participation in the Program, where such fees or terms would reasonably be expected to discriminate against Apple as compared to other fees or commercial terms imposed by Access Partner (or where relevant, Access Partner's Service Provider) on Participating Providers with respect to a Competing Platform.
- d. Except as otherwise set out in this Agreement, each Party will bear its own development and operation expenses for participation in the Program.
- e. All Fees quoted in this Agreement are exclusive of any taxes required to be accounted for on that Fee (such as direct or indirect taxes, levies, imports, duties, charges, fees and withholdings of any nature now or hereafter imposed by any governmental, fiscal or other authority or any Withholding Tax payable pursuant to Section 8(b)).

**8. Payment.**

- a. Access Partner (where Access Partner also is the Credential Manager) will report billing-related metrics in the form set out in **Exhibit E (Billing Reports)** (or as otherwise agreed between the Parties) to Apple not later than the fifteenth (15th) Calendar Day after the end of each month during the Term. Access Partner will make payment to Apple of the applicable amount (in accordance with payment instructions to be provided by Apple and in compliance with Section 8.d) within thirty (30) days of the end of each calendar month. The Parties may agree at any time during the Term to adjust the interval for reporting and payment (e.g., from a monthly basis to quarterly basis).

- b. Subject to Section 8.c), all Fees payable under this Agreement must be paid in full by an electronic payment method agreed to by the Parties in US Dollars free and clear of all deductions, withholdings, set-offs or counterclaims whatsoever, save only as may be required by law. If any deductions or withholdings are required by law in respect of any payment payable from Access Partner to Apple under this Agreement, Access Partner will be obliged to pay to Apple such additional amounts as will ensure that Apple receives in total an amount which (after such deduction or withholding has been made) is no more and no less than it would have been entitled to receive in the absence of any such deduction or withholding.
- c. Either Party may dispute in good faith any amount within Access Partner's billing report or any portion thereof by written notice given to the other no later than six (6) months after the due date of the amount as reflected on the applicable report or invoice. Access Partner may withhold payment for any charge that it disputes in good faith prior to the date payment is due for such charge. The notice of dispute will describe, in reasonable detail, the basis for the dispute. Upon such dispute, each of Access Partner and Apple will diligently pursue an expedited resolution of all disputed charges and make a good faith effort to make its relevant records available to the other Party to help determine the correct charge. If it is ultimately determined that Access Partner is required to pay an amount it had withheld pursuant to this Section 8, the payment thereof will be made within two (2) Business Days of such determination. For the avoidance of doubt, any payment pursuant to this Section 8 will not be deemed a waiver of, or in any other way limit, a Party's right to pursue any dispute with respect to such payment within two (2) years of the due date for such charge and in accordance with the terms of this Agreement.
- d. During the Term, and for twelve (12) months following the date of termination of this Agreement, and upon no less than fifteen (15) days' prior written notice, Access Partner will provide Apple's independent external auditors with reasonable access during normal business hours solely to the books and records necessary for purposes of confirming the accuracy and correct calculation of the amounts owed hereunder. If any such audit reveals an underpayment by Access Partner during the preceding twelve (12) month period, Apple may dispute the monies owed by Access Partner in accordance with this Section 8. Access Partner will promptly pay Apple the amount of any underpayment, and Apple will promptly pay or issue a credit to Access Partner for the amount of any overpayment, revealed by any such audit. If any such audit reveals an underpayment of more than two percent (2%) in the aggregate during the audited period, Access Partner will in addition promptly pay to Apple all reasonable costs and expenses of such audit not to exceed the amount of the underpayment during the audited period, and Apple may perform additional audits of similar scope to the minimum extent necessary for revealing additional underpayment, no more than twice a calendar year (or as required by applicable Law), at Access Partner's expense, until an audit shows no underpayment. Subject to any increased audits permitted under this Section 8, Apple may exercise its audit rights under this Section 8 no more than two (2) times during each calendar year (or as required by applicable Law) with follow-up to confirm resolution of any issues identified as necessary.



9. **Reporting data.**

Access Partner (where Access Partner also is the Credential Manager) will provide to Apple or its Affiliates information and reports related to Access Partner's participation in the Program (the "Reports"). Access Partner will work with Participating Providers to provide Apple with necessary data and statistics related to the performance of the Program as set forth in **Exhibit E (Billing Reports) and Exhibit F (Data to be included in Reports)**. Access Partner, on behalf of itself and its Affiliates and their respective successor in interest and assigns, hereby grants Apple and its Affiliates the right and license to use any information contained in the Reports for purposes of Apple (i) performing its obligations and exercising its rights under this Agreement and (ii) improving the Apple Technology.

10. **Confidentiality.**

- a. "**Confidential Information**" means: (i) either Party's product plans and roadmaps; (ii) the terms and conditions of this Agreement; and (iii) any other information disclosed by a Party or its Affiliates to the other Party or its Affiliates in connection with this Agreement, or the development of the Parties' or their respective Affiliates' respective systems in connection with the activities contemplated by this Agreement, and designated by the disclosing Party as confidential in writing or, if disclosed orally, designated as confidential at the time of disclosure; *provided, however,* that Confidential Information will not include information that: (A) is now or subsequently becomes generally known or available to the public through no fault or breach on the part of the receiving Party or its Affiliates; (B) the receiving Party can demonstrate to have had rightfully in its possession or the possession of its Affiliates prior to disclosure from the disclosing Party or its Affiliates (that is not precluded from being disclosed as a result of confidentiality obligations owed to a third party); (C) is independently developed by the receiving Party or its Affiliates without use of or reliance in any way on the disclosing Party's Confidential Information; (D) the receiving Party or its Affiliates rightfully obtain from a third party who has the right to transfer or disclose it to the receiving Party or its Affiliates without any obligation of confidentiality; or (E) is released for publication by the disclosing Party or its Affiliates in writing.
- b. Each Party will protect the other Party's Confidential Information obtained pursuant to this Agreement from unauthorized dissemination and use with the same degree of care that such Party uses to protect its own like information. Except as expressly set forth herein, neither Party will use the other Party's Confidential Information for purposes other than those necessary to directly further the purposes of this Agreement. Except as expressly permitted under this Agreement, neither Party will disclose to third parties the other Party's Confidential Information without the prior consent of the other Party. The receiving Party will limit its internal distribution of any Confidential Information of the disclosing Party to its and its Affiliates' employees and agents, including its attorneys, financial advisors, and consultants, who have a need to know and who are subject to a written confidentiality agreement or professional obligation of confidentiality that protects such Confidential Information to at least the same extent as this Agreement. The Parties may disclose Confidential Information if required by law as part of a judicial or regulatory proceeding so long as the Party required to disclose takes all reasonable steps available to obtain protective treatment and, if permitted by applicable Laws, notifies the other Party prior to disclosure in sufficient time to

enable such Party to seek protective treatment. All information provided hereunder is provided “AS IS” and without any warranty, express, implied or otherwise, regarding its accuracy or performance.

11. **Data Protection and Information Security.**

- a. The Parties acknowledge and agree that Access Partner is required, as a data processor for each Participating Provider, to comply with the provisions of the **General Data Protection Regulation 2016/679 (the “GDPR”)**, where applicable, and all other applicable Data Protection Laws with regard to the processing of Personally Identifiable Information. The Parties acknowledge that Access Partner does not act as a data processor for Apple in this respect.
- b. In this respect Access Partner will implement industry leading policies and procedures, and safeguard all Access Partner and Access Partner Personnel facilities, systems, applications, servers, and networks including all Systems relating to Services or Confidential Information, or that access any Apple system or network, or that host or process Confidential Information, as well as Systems that process Personal Data controlled by Participating Provider, and in accordance with its instructions.
- c. Both Access Partner and Apple will maintain written operating standards and security procedures for their data centers, data management, security, handling and protection practices that comply with all applicable Laws (including data protection laws) and apply industry standards in the case of Apple and apply commonly acceptable standards within the industry in the case of Access Partner, and will use its commercially reasonable efforts to secure personal data of Users through the use of appropriate physical and logical security measures including appropriate network security and encryption technologies.
- d. Each Party will comply with all legal obligations related to data protection as required by applicable Law. The Parties agree to enter into any further data protection agreements necessary for compliance with applicable Law, including with regard to cross-border data transfers.
- e. Each Party will use commercially reasonable efforts to correct any issues or technical errors related to the Apple Technology, Apple Access Platform, Apple Access Platform or Program within its control, including any failure to comply with the Specifications. For the avoidance of doubt, in no event will Apple be required to modify the Apple Technology, Apple Access Platform, or Specifications as a means of “correcting” any issues or technical errors unless all other Access Platform Participants, if any, of access credentials or Participating Provider which have the same function and capabilities as the Credentials are encountering the same issues or technical errors. Issues materially impacting User functionality will be corrected as promptly as possible. Each Party will notify the other as promptly as practicable after any material issue has been identified and include an estimated time of resolution. If the Parties are unable to resolve any material issue within thirty (30) days of discovery, the non-offending Party may initiate the Executive Review process set forth in Section 29 (Executive Review).

- f. Subject to applicable Law, Apple and Access Partner will promptly notify each other in the event a Party learns or has reason to believe that any Person has breached security measures relating to the Apple Technology (including in the case of Apple any security measures included in the software or hardware on an Enabled Device and any Apple Access Services-related data contained therein), or gained unauthorized access to any Apple Provisioning Data or Participating Provider Data, respectively (an “Information Security Breach” and in the case of a breach of Access Partner’s security measures, a “Access Partner Security Breach”, in the case of a breach of Apple’s security measures, an “Apple Security Breach”, and in the case of a breach of Participating Provider's security measures, a “Participating Provider Security Breach”). An Information Security Breach will not include a ping or other broadcast attack on a Party’s firewall, port scans, unsuccessful log-on attempts, denial of service, interference with a system, or any combination of the above or equivalent tactics, so long as such incident does not result in unauthorized access to, use or disclosure of User PII or Apple Provisioning Data.
- g. Upon any discovery of an Information Security Breach, the Party responsible for the Information Security Breach (i.e. Apple in case of Apple Security Breach, or Access Partner in case of an Access Partner Security Breach) will, at its cost, (i) appropriately investigate, remediate, and mitigate the effects of the Information Security Breach and (ii) provide the other Party with assurances reasonably satisfactory to such Party that appropriate measures have been taken to prevent such Information Security Breach from recurring. Additionally, if and to the extent any Information Security Breach or other unauthorized access, acquisition or disclosure of User PII, Apple Provisioning Data, or Access Partner occurs and if the other Party reasonably determines that notices or other remedial measures (including notice, credit monitoring services, fraud insurance and the establishment of a call center to respond to customer inquiries) are warranted, subject to Section 11.h) below, the Party who is subject to such Information Security Breach will, at its cost and expense, upon the other Party’s reasonable request, undertake such notices and remedial actions.
- h. Except as required by applicable Law, no Directed Party (as the term is defined in Section 18 (Government Authority)) will make (and Access Partner will procure that no Participating Provider makes) any public announcement in respect of an Information Security Breach for which the other Party is responsible unless and until it has consulted with and has obtained the approval of the other Party. In the event such approval is not given, the requesting Party may invoke the Executive Review process set forth in Section 27, provided, however, that the thirty (30) day time period set forth in Section 29.e (Executive Review) will be reduced to ten (10) days for purposes of this Section 11.h. If a Party does not give such approval even after the Executive Review, such Party will cooperate on a good faith and commercially reasonable basis with the requesting Party in order to take alternative measures to minimize the requesting Party’s risks (including reputation risks) discussed in the Executive Review.

## 12. **Intellectual Property Rights.**

- a. Access Partner and its Affiliates own or have the right to use all Access Partner Technology (and all Intellectual Property Rights therein or thereto). Apple and its

Affiliates own or have the right to use all Apple Technology (and all Intellectual Property Rights therein or thereto).

- b. Except as expressly granted under this Agreement, or otherwise agreed in writing by the Parties, no other rights or licenses to exploit (in whole or in part), in any manner, form or media, any of the Technology, Intellectual Property Rights or Marks of the other Party are granted. For the avoidance of doubt, this is not a “work made for hire” agreement, as that term is defined in the United States Copyright Act, 17 U.S.C. § 101 or any similar legislation in the Territory, nor will it be considered as equivalent to a work made for hire under any similar provision elsewhere in the world. Nothing contained in this Agreement will be construed as constituting a transfer or an assignment to a Party by the other Party of any of the Technology, Intellectual Property Rights or Marks of such other Party or any of its Affiliates. Each Party’s Technology, Intellectual Property Rights and Marks are being licensed hereunder, not sold. Each Party and its Affiliates and Service Providers, as applicable, must reproduce the copyright and all other proprietary notices displayed on the other Party’s Technology on all copies of such materials.

**13. Jointly Developed Technology.**

- a. The Parties are not obligated to jointly develop any Technology in connection with or in relation to this Agreement. If the Parties, in their sole respective discretion, determine to jointly develop any Technology, the Parties will first enter into a separate and binding written agreement confirming the scope of such joint development efforts and the respective rights of the Parties in any jointly developed Technology, including ownership of the Intellectual Property Rights in (and, if applicable, any Marks for) any such jointly developed Technology.
- b. No Party may file or attempt to file any application for a patent design, utility model, or anything similar to the foregoing, or register or attempt to register any Mark or copyrightable work for any jointly developed Technology, without the prior written approval of all parties involved in such joint development.

**14. IP Licenses.**

- a. Apple Technology and Patent License. Apple hereby grants to Access Partner and each of its Affiliates and Service Providers during the Term, a limited, non-exclusive, royalty-free, fully paid up, non-assignable (subject to Section 27 (Assignment)), non-transferable (subject to Section 27 (Assignment)), non-sublicensable, worldwide right and license:
  - i. to use the Specifications, and to incorporate the corresponding APIs into Access Partner’s products and services, solely for the purpose of enabling Users to participate in the Program;
  - ii. in respect of Intellectual Property Rights and Technology other than those referred to in Section 14.a.i) above, and other than Patent Rights owned, controlled or otherwise licensable by Apple or any of its Affiliates (including such Intellectual Property Rights and Technology sublicensable by Apple from other Access Platform Participants), to use, make, have made, have operated, import, reproduce, modify, create derivative works

of, perform, display, transmit, and otherwise exploit any Apple Technology (other than the Specifications) that Apple has provided to Access Partner in connection with the Program; in each case solely to the extent necessary to perform and comply with Access Partner's rights and obligations under this Agreement in connection with the Program, *provided, however*, that no rights are being granted herein to modify or make derivative works of the Specifications or any operating system software of Apple or its Affiliates; and

iii. in respect of Patent Rights owned, controlled or otherwise licensable by Apple or any of its Affiliates (including Patent Rights sublicensable by Apple from other Access Platform Participants), to use, copy, make, have made, have operated, import, reproduce, modify (but not the Specifications), create derivative works of (but not the Specifications), perform, display, transmit, and otherwise exploit the Apple Technology solely to the extent necessary to perform and comply with Access Partner's rights and obligations under this Agreement in connection with the Program.

b. Access Partner Technology and Patent License. Solely to the extent necessary to operate the Apple Access Platform and enable other Access Platform Participants to use the Apple Access Platform, Access Partner, on behalf of itself, its Affiliates and their respective successors-in-interest and assigns, hereby grants to Apple and each of its Affiliates and Service Providers, under this Agreement, a limited, sublicensable (only by Apple and each of its Affiliates solely to other Access Platform Participants for the period of their participation in the Apple Access Platform), non-exclusive, royalty-free, fully paid-up, non-assignable (subject to Section 27 (Assignment)), non-transferable (subject to Section 27 (Assignment)), perpetual and irrevocable worldwide right and license:

i. in respect of Patent Rights owned, controlled or otherwise licensable by Access Partner or any of its Affiliates ("Access Partner Patent Rights"), to use, make, have made, have operated, import, reproduce, modify, create derivative works of, perform, display, transmit, and otherwise exploit the Apple Access Platform; and

ii. in respect of Intellectual Property Rights owned, controlled or otherwise licensable by Access Partner or any of its Affiliates, other than Access Partner Patent Rights, to use, make, have made, have operated, import, reproduce, modify, create derivative works of, perform, display, transmit, and otherwise exploit any items of Access Partner Technology that Access Partner has provided to Apple in connection with the Program;

*provided*, the license granted in this Section 14.b (Access Partner Technology and Patent License) does not include any Access Partner Patent Rights or Access Partner Technology conceived, reduced to practice, authored or otherwise discovered, created or developed by Access Partner or any of its Affiliates after the expiration or termination date of this Agreement without the use of Apple's Confidential Information.

- c. If, after the Effective Date, any Person becomes a new direct or indirect parent of Access Partner (“New Parent”), Access Partner will (i) cause such New Parent to agree, in a writing executed by such New Parent within thirty (30) days of becoming such New Parent, to assume all obligations of Access Partner under this Section 14.b effective as of the date of becoming such New Parent and (ii) reasonably promptly provide a true and correct copy of such agreement to Apple.
- d. All of the rights and licenses granted to Access Partner and its Affiliates under this Agreement (including each of the limited licenses under Section 14.a (Apple Technology and Patent License) will expire and terminate in its entirety upon the later of:
  - i. the expiration or termination of Access Partner’s participation in the Program; or
  - ii. the expiration of any post-termination transition period provided for under this Agreement.

Upon the expiration or termination of such license, Access Partner will, at Apple’s discretion, return to Apple or destroy all copies of Apple Technology provided or made accessible to Access Partner under this Agreement (and any derivatives thereof), then in Access Partner’s possession or control (whether directly or indirectly). Should Apple determine that any or all copies of such Apple Technology (or derivatives thereof) should be destroyed, then Access Partner will arrange for such destruction to take place as soon as reasonably practicable and to be certified by an independent third party and will provide such certification to Apple immediately upon request.

- e. Apple hereby grants to Access Partner and each of its Affiliates and Service Providers a limited, non-exclusive, royalty-free, fully paid up, non-assignable, non-sub-licensable, non-transferable worldwide right and license to (i) use and modify the Sample Source Code and (ii) distribute the Sample Source Code (or any portion thereof) to a Service Provider with Apple’s prior written consent, in each case of (i) and (ii), solely to the extent necessary for the Access Partner or its Affiliates or Service Providers to facilitate the integration of Credentials with the Apple Access Platform. The Access Partner agrees not to (and will ensure that none of its Affiliates or Service Providers) use, modify, provide or make available to any Person (other than the Access Partner’s Affiliates and Service Providers) or otherwise exploit any of the Sample Source Code, except as provided in the license granted in this Section 14.e.
  - i. Subject to Apple’s rights, title and interest in and to the Sample Source Code, the Access Partner will own all modifications made by the Access Partner or any of its Affiliates or Service Providers to the Sample Source Code for the purpose set forth in the license granted in Section 14(e) (“Access Partner Source Code Modifications”).
  - ii. The Access Partner hereby grants to Apple and each of its Affiliates and Service Providers, a limited, non-exclusive, royalty-free, fully paid up, non-sub-licensable, non-transferable, perpetual, irrevocable, worldwide

right and license to use any Access Partner Sample Source Code Modifications solely to the extent necessary to operate the Apple Access Platform and to enable Access Partner to use the Apple Access Platform.

15. **Export Controls.** Access Partner may not use, export, re-export, import, sell, release, or transfer the Apple Software, Services, or Documentation except as authorized by United States law, the laws of the jurisdiction in which Access Partner obtained the Apple Software, and any other applicable laws and regulations. In particular, but without limitation, the Apple Software, Services, source code, technology, and Documentation (collectively referred to as “Apple Technology” for purposes of this Section) may not be exported, or re-exported, transferred, or released (a) into any U.S. embargoed countries or regions or (b) to a party sanctioned by the United States Government or other relevant foreign government authority with jurisdiction, without first obtaining appropriate government authorization. By using the Apple Technology, Access Partner represents and warrants that Access Partner is not located in any such country or region or on any such list. Access Partner also agrees that Access Partner will not use the Apple Technology, including any pre-release versions thereof, for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture or production of nuclear, missile, chemical or biological weapons or any other military end uses as defined in 15 C.F.R. § 744.
16. **Fraud Prevention.** Apple and Access Partner will cooperate in good faith and use all reasonably available efforts to provide assistance in each other’s fraud detection and prevention efforts. For Access Partner, this obligation will include a commitment to require Participating Providers and, if applicable, Access Service Partner to monitor for fraudulent activity at a transaction level (e.g., daily batch monitoring for behavior pattern of fraudulent reloads on Provisioned Credentials). Subject to each Party’s confidentiality obligations hereunder and subject to applicable Law, each Party agrees to keep the other Party reasonably informed of the progress of any fraud investigation to the extent it affects Apple Provisioning Data, User PII, the improper use of Provisioned Credentials, the improper provisioning of Credentials or any other rights, customers, or information of the other Party. In instances of suspected fraud in Access Partner’s network(s), system(s), and/or processes for which Access Partner has been given prompt written notice, Access Partner will immediately implement the appropriate restrictions and safeguards to protect suspected Accounts until such time as Access Partner has successfully verified control of such Account. In the event that the Parties identify instances of fraud involving Provisioned Credentials and such fraud is attributed to Access Partner’s network(s), system(s), and/or processes, Access Partner will use all reasonable efforts to remedy and further prevent any such instance of fraud.
17. **Compliance with Law.**
  - a. Each Party will comply with all applicable Laws related to the performance of its obligations under this Agreement. As part of its compliance obligations, Access Partner will be responsible for (i) adherence to applicable Law relating to the provisioning and use of the Accounts, use, management, suspension and termination of the Credentials; (ii) adherence to applicable Law relating to providing Access Partner Provisioning Data to Apple; and (iii) obtaining the agreement of each Participating Provider to take such steps as are required to be taken by such Participating Providers to enable the Program to be undertaken in compliance with all applicable Laws. Subject to the Party’s indemnification

obligations under Sections 21.a.i (Indemnification) and 21.b.ii (Indemnification), neither Party will be responsible for any fees, fines, penalties, or other assessments by any Governmental Authority against the other Party.

- b. Subject to Section 17.c, Access Partner takes full responsibility for all tax compliance or reporting obligations imposed on Access Partner as a result of Access Partner's participation in the Program, including the self-assessment of any indirect taxes as required under relevant tax legislation Access Partner is subject to in an applicable jurisdiction. In the event a relevant taxing authority requires the Program provider to charge any taxes under the terms of this Agreement, Apple will perform all such tax compliance obligations.
- c. Where any relevant taxation authority imposes any income tax on the Fees and requires Access Partner to withhold such tax ("Withholding Tax"), pursuant to Section 8.b (Payment), Access Partner will make its payments in accordance with Section 8.b (Payment). Access Partner will remit such Withholding Tax to the relevant taxing authority on behalf of Apple. In the event a reduced or nil Withholding Tax rate may apply on payments to Apple, Apple will furnish to Access Partner as soon as practicable documentation necessary to evidence the qualifications for the reduced rate of Withholding Tax. Upon request by Apple, Access Partner will furnish Apple with tax receipts or other documentation evidencing the payment of such Withholding Tax when available. Issuer will pay such amount to Apple which, after withholding the required Withholding Tax, leaves Apple in the same after-tax position as it would have been, had no Withholding Tax been required to be withheld.

## 18. **Government Authority.**

- a. In the event that any of Apple, Access Partner, Participating Provider or, if applicable, Access Service Partner (the "Directed Party") is notified by a Governmental Authority, or otherwise reasonably believes, upon advice of counsel, that it is not complying with applicable Law or that there is a security breach due to the processes used by a Directed Party, for use and provisioning of Credentials using the Apple Technology, the Parties, will, unless prohibited by law, promptly meet and work in good faith to determine together whether any such failure to comply with applicable Law has occurred or is occurring. Upon such determination, the Parties will work together in good faith to use reasonable measures to modify such processes (including the Program) to ensure compliance with applicable Law. Apple reserves the right to make changes to the Program that Apple deems necessary to comply with applicable Law. In the event of any audit or investigation by a Governmental Authority, the Parties will provide each other's legal counsel with assistance reasonably required to address any issues of non-compliance that may be raised by such audit or investigation, to the extent reasonably practicable.
- b. Notwithstanding anything to the contrary in this Agreement, in the event that a Directed Party receives a written supervisory communication, written guidance or written direction from a Governmental Authority ("Regulatory Guidance") that requires a modification to or suspension of the Program or a Participating Provider's participation therein in less than thirty (30) days, the Directed Party will:
  - (i) promptly memorialize such Regulatory Guidance in writing and, with the



consent of the Governmental Authority issuing the Regulatory Guidance, if such consent is required by applicable Law or is practically required, deliver such writing to the other Party, and (ii) deliver an officer's certificate that the Directed Party believes in good faith that such expedited action is required, based on advice received from legal counsel, and (iii) use practically reasonable efforts to clarify with the applicable Governmental Authority that the expedited action is required. Upon fulfillment of the foregoing (provided, however, that (i) is not required to be fulfilled if the Directed Party could not obtain the consent of the Governmental Authority despite its good faith and commercially reasonable efforts to obtain such consent), the Directed Party will have the right to immediately suspend the Program or a Participating Provider's participation therein, and the other Party will cooperate with the Directed Party to take any actions reasonably required to effect the suspension (where a Governmental Authority is involved, subject to the Parties agreeing on disclosure to each other pursuant to a common interest agreement between the Parties on reasonable terms and conditions). Any such suspension will be limited to the narrowest extent required (including scope and duration) by the Regulatory Guidance.

- c. Access Partner will ensure that Participating Provider or, if applicable, Access Service Partner will, *mutatis mutandis*, abide by and comply with the obligations and requirements in this Section 18.

## 19. Representations and Warranties.

- a. Access Partner represents and warrants that as of the Effective Date:
  - i. it is duly incorporated as a corporation under the laws of California and has the requisite power and authority and the legal right to conduct its businesses as now conducted and hereafter contemplated to be conducted, and enter into this Agreement;
  - ii. it has the requisite power and authority and the legal right to conduct its businesses as now conducted and hereafter contemplated to be conducted, enter into this Agreement;
  - iii. to its knowledge it has all licenses, permits and authorizations required by applicable Law or Governmental Authorities to issue and manage Credentials and to provide payment services in relation to Credentials;
  - iv. it has the right to grant all of the licenses and other rights granted to Apple and each of its Affiliates and Service Providers in this Agreement, including with respect to any Intellectual Property Rights owned, controlled or licensable by Access Partner or any of its Affiliates licensed under Section 14.b, and neither this Agreement nor any terms or conditions of this Agreement (including any of the licenses or other rights granted by Access Partner or any of its Affiliates in this Agreement) conflict, or will conflict, with any terms or conditions of any agreement to which Access Partner or any of its Affiliates is a party or to which it may be bound;
  - v. no Legal Proceeding (including any regulatory action) is pending or, to its knowledge, threatened against it that would reasonably be expected to

have a material adverse effect on its ability to perform its obligations under this Agreement.

- vi. except as would not reasonably be expected to have a material adverse effect on its ability to perform its obligations under this Agreement, (i) it is in compliance with all applicable Laws and (ii) it is not subject to any order or ruling that restricts in any respect its ability to perform its obligations under this Agreement.

b. Apple represents and warrants that as of the Effective Date:

- i. It is duly incorporated as a corporation under the laws of California and has the requisite power and authority and the legal right to conduct its businesses as now conducted and hereafter contemplated to be conducted, and enter into this Agreement;
- ii. it has the requisite power and authority and the legal right to conduct its businesses as now conducted and hereafter contemplated to be conducted, enter into this Agreement;
- iii. to its knowledge, it has all licenses, permits and authorizations required by applicable Law or Governmental Authorities to operate the Program in the Territory, provided, however, that Apple will conduct commercially reasonable investigation on required licenses, permits and authorizations to operate the Program in the Territory; and
- iv. it has the right to grant all of the licenses and other rights granted to Access Partner and each of its Affiliates and Service Providers in this Agreement, including with respect to any Intellectual Property Rights owned, controlled or licensable by Apple or any of its Affiliates under Section 14.a, and neither this Agreement nor any terms or conditions of this Agreement (including any of the licenses or other rights granted by Apple or any of its Affiliates in this Agreement) conflict, or will conflict, with any terms or conditions of any agreement to which Apple or any of its Affiliates is a party or to which it may be bound.

20. **No Other Warranties.** TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW AND EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, IMPLIED WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE OR IMPLIED WARRANTY OF NON-INFRINGEMENT, AND EACH PARTY HEREBY EXPRESSLY DISCLAIMS ALL SUCH WARRANTIES. WITHOUT LIMITING THE FOREGOING, NEITHER PARTY WARRANTS THAT THE USE OF ANY OF THE RESPECTIVE TECHNOLOGIES, SPECIFICATIONS, SYSTEMS OR PLATFORMS OF EITHER PARTY, OR ANY RELATED PRODUCTS OR SERVICES

CONTEMPLATED BY THIS AGREEMENT, WILL BE ERROR FREE OR UNINTERRUPTED.

21. **Indemnification.**

- a. **Indemnification by Access Partner.** Access Partner agrees to indemnify, defend, and hold harmless Apple, its Affiliates, and the shareholders, agents, employees, officers, and directors of each of Apple and its Affiliates (each, an “Apple Indemnified Party”), from and against any and all Indemnified Losses to the extent such Indemnified Losses arise out of, are connected with, or result from any Claim against any Apple Indemnified Party that arises out of, is connected with, or results from any of the following that occurs during the Term:
- i. any actual or alleged infringement of the trademark rights of any third party by (A) any of the Access Partner Marks or (B) any use of any of the Access Partner Marks by Apple, any of its Affiliates, or any of Apple’s Service Providers in accordance with this Agreement or as otherwise authorized by Access Partner in writing;
  - ii. Access Partner’s, any of its Affiliates’, or any of Access Partner’s Service Providers’ failure to comply with applicable Laws;
  - iii. any advertising, promotions, and marketing programs, or similar documents or materials conducted or created by or on behalf of Access Partner, any of its Affiliates, or any of Access Partner’s Service Providers in connection with the Program;
  - iv. any use of Apple Marks by Access Partner, any of its Affiliates, or any of Access Partner’s Service Providers in a manner not in accordance with this Agreement or not otherwise authorized by Apple in writing;
  - v. any breach of Section 11 (Data Protection and Information Security) by Access Partner, any of its Affiliates, or any of Access Partner’s Service Providers;
  - vi. any Access Partner Security Breach;
  - vii. any breach by Access Partner of any of its representations and warranties in Section 19.a;
  - viii. any breach by Access Partner or any of its Affiliates of any contract between Access Partner or any Access Partner Affiliate, as the case may be, and any third party (including any User or Participating Provider) related to Access Partner’s participation in the Program;
  - ix. the gross negligence, fraud, or willful misconduct of Access Partner, any of its Affiliates, or any of Access Partner’s Service Providers; or
  - x. any amount paid by Access Partner’s Affiliates, Access Partner’s Service Providers, Participating Providers, or Users for Unauthorized Transactions,

unless any such Unauthorized Transaction occurred due to Apple's or Apple Affiliate's willful misconduct or grossly negligent acts or omissions.

*provided, however,* in no event will Access Partner be obligated to indemnify any Apple Indemnified Party under this Section 21.a (Indemnification by Access Partner) against any Indemnified Losses to the extent such Indemnified Losses result from (A) any failure by Apple, any of its Affiliates, or any of Apple's Service Providers to comply with applicable Laws or (B) any fraud, willful misconduct or grossly negligent acts or omissions of Apple, any of its Affiliates, or any of Apple's Service Providers.

- b. **Indemnification by Apple.** Apple agrees to indemnify, defend and hold harmless Access Partner, its Affiliates, and the agents, employees, officers, and directors of each of Access Partner and its Affiliates (each, an "Access Partner Indemnified Party"), from and against any and all Indemnified Losses to the extent such Indemnified Losses arise out of, are connected with, or result from any Claim against an Access Partner Indemnified Party that arises out of, is connected with, or results from any of the following that occurs during the Term:
- i. any actual or alleged infringement of the trademark rights of any third party by (A) any of the Apple Marks or (B) any use of any of the Apple Marks by Access Partner, any of its Affiliates, or any of Access Partner's Service Providers in accordance with this Agreement or as otherwise authorized by Apple in writing;
  - ii. Apple's, any of its Affiliates', or any of Apple's Service Providers' failure to comply with applicable Laws;
  - iii. any use of any of the Access Partner Marks by Apple, any of its Affiliates, or any of Access Partner's Service Providers in a manner not in accordance with this Agreement or not otherwise authorized by Access Partner in writing;
  - iv. any breach of Section 11 (Data Protection and Information Security) by Apple, any of its Affiliates, or any of Apple's Service Providers;
  - v. any Apple Security Breach;
  - vi. any breach by Apple of any of its representations and warranties in Section 19.b;
  - vii. any breach by Apple or any of its Affiliates of any contract between Apple or any Apple Affiliate, as the case may be, and any third party (including any User or Participating Provider) related to Apple's participation in the Program; or
  - viii. the gross negligence, fraud, or willful misconduct of Apple, any of its Affiliates, or any of Apple's Service Providers.

*provided, however,* that in no event will Apple be obligated to indemnify any Access Partner Indemnified Party under this Section 21.b (Indemnification by

Apple) against any Indemnified Losses to the extent such Indemnified Losses result from (A) any failure by Access Partner, any of its Affiliates, or any of Access Partner's Service Providers to comply with applicable Laws or (B) any fraud, willful misconduct or grossly negligent acts or omissions of Access Partner, any of its Affiliates, or any of Apple's Service Providers.

## 22. Indemnification Procedures.

- a. **Notice.** If a Party receives notice of any Claim for which indemnification may be available under this Agreement (the "Indemnified Party"), the Indemnified Party must promptly notify the other Party (the "Indemnifying Party") in writing of the Claim, including, if possible, the amount or estimate of the amount of liability arising from it. The Indemnified Party will use commercially reasonable efforts to provide notice to the Indemnifying Party no later than fifteen (15) calendar days after receipt by the Indemnified Party in the event a suit or action has commenced, or thirty (30) calendar days under all other circumstances; *provided, however*, that the failure to give such notice will not relieve an Indemnifying Party of its obligation to indemnify except to the extent the Indemnifying Party is materially prejudiced by such failure.
  
- b. **Right to Defend Claims; Coordination of Defense.** The Indemnifying Party will have the right to defend any Claim for which indemnification may be available under this Agreement (excluding, other than with respect to Claims arising under Section 21.a.i or Section 21.b.i, any investigation or examination by any Governmental Authority) at its expense and in the name of the Indemnified Party and will select the counsel for the defense of such Claim as approved by the Indemnified Party, such approval not to be unreasonably withheld, conditioned or delayed, and will reasonably cooperate with the Indemnified Party in the conduct of the defense against such Claim. Notwithstanding the foregoing, the Indemnifying Party will not have the right to defend any such Claim if: (i) it refuses to acknowledge fully its indemnification obligations to the Indemnified Party (but only as to the obligations specific to the Indemnifying Party in the event such Claim gives rise to indemnification obligations of more than one party); (ii) it contests (in whole or in part) its indemnification obligations (but only as to the obligations specific to the Indemnifying Party in the event such Claim gives rise to indemnification obligations of more than one party); (iii) it fails to employ appropriate counsel approved by the Indemnified Party to assume the defense of such Claim or refuses to replace such counsel upon the Indemnified Party's reasonable request; (iv) the Indemnified Party reasonably determines that there are issues which could raise possible conflicts of interest between the Indemnifying Party and the Indemnified Party or that the Indemnified Party has claims or defenses that are separate from or in addition to the claims or defenses of the Indemnifying Party; or (v) such Claim seeks an injunction, cease and desist order, or other equitable relief against the Indemnified Party. In each such case described in subsections (i) through (v) of this Section 22.b, the Indemnified Party will have the right to direct the defense of the Claim and retain its own counsel, with either Party being entitled to initiate, after any time to appeal a final resolution of such Claim has expired, a separate determination of the extent to which the Indemnifying Party will be responsible for paying any of the reasonable cost of such defense of such Claim, including any judgment or settlement (as the case may be) and any reasonable attorneys' fees and expenses. The Parties agree to cooperate

in good faith to coordinate the defense of any Claim that may give rise to indemnification obligations of more than one party or that may include allegations that are not subject to indemnification.

- c. **Indemnifying Party Election.** If the Indemnifying Party elects and is entitled to compromise or defend a Claim pursuant to this Section 22 (Indemnification Procedures), it will within thirty (30) days after receiving the indemnity request for such Claim (or sooner, if the nature of such Claim so requires) notify the Indemnified Party in writing of its intent to do so, and the Indemnified Party will, at the expense of the Indemnifying Party, reasonably cooperate in the defense of such Claim. In such case, the Indemnified Party will have the right to participate in the defense of any Claim with counsel selected by it. Except as provided in this Section 22 (Indemnification Procedures), the fees and disbursements of such counsel will be at the expense of the Indemnified Party.
- d. **Settlement of Claims.** With respect to any Claim arising under Section 21.a.i or Section 21.b.i only, so long as the Indemnifying Party is providing a defense for such Claim pursuant to its indemnity obligations set forth in Section 22.b, the Indemnified Party may not settle such Claim without the prior written consent of the Indemnifying Party. With respect to all other Claims, the Indemnifying Party will have no obligation to pay the monetary amount of the settlement of any Claim entered into by the Indemnified Party without the prior written consent of the Indemnifying Party (which consent will not be unreasonably withheld or delayed). Notwithstanding the Indemnifying Party's right to direct the defense against any Claim, or part thereof, the Indemnifying Party will not have the right to compromise or enter into an agreement settling any Claim, or part thereof, without the prior written consent of the Indemnified Party (which consent will not be unreasonably withheld or delayed) that imposes liability or obligations on the Indemnified Party. Notwithstanding the foregoing, the Indemnifying Party may, upon prior written notice to and consultation with, the Indemnified Party, compromise or enter into a settlement agreement that involves solely the payment of money by the Indemnifying Party; *provided* such settlement includes a complete, unconditional, irrevocable release of the Indemnified Party with respect to such Claim, and provided, further, that, in the good faith judgment of the Indemnified Party, such settlement agreement is not likely to cause reputational damage to the Indemnified Party or establish a precedential practice adverse to the continuing interest of the Indemnified Party.
- e. **Subrogation.** The Indemnifying Party will be subrogated to any Claims or rights of the Indemnified Party as against any other Persons with respect to any amount paid by the Indemnifying Party under Section 21 (Indemnification) or this Section 22 (Indemnification Procedures). The Indemnified Party will reasonably cooperate with the Indemnifying Party, at the Indemnifying Party's expense, in the assertion by the Indemnifying Party of any such claim against such other Persons.

## 23. **Limitation of Liability.**

- a. Nothing in this Agreement will exclude or limit the liability of any Party for death or personal injury caused by negligence, for fraud or deceit or for any other liability that cannot be so excluded or limited under applicable Law.

- b. Subject to sub-section 21(a) above and except with respect to liability under Sections 6 (Quiet Period), 9 (Confidentiality), 11 (Data Protection and Information Security) , or 21 (Indemnification) (however, only with regard to liabilities of the Indemnified Party to the third party claimant) or with respect to Outages where the Party responsible has failed to use all reasonable efforts to cure the Outage, in no event will either Party be liable to the other Party for indirect, consequential, incidental, or special damages, whether in contract, tort (whether in negligence or strict liability) or other legal or equitable theory, or any loss of profits or revenue, regardless of whether such Party knew or should have known of the possibility of such damages.
  - c. Notwithstanding the foregoing, Apple will not be liable for any Unauthorized Transactions made by Users using Provisioned Credentials.
24. **Term.** The initial term of this Agreement will commence on the Effective Date and terminate at 11:59 p.m. Pacific Standard Time on the 3rd anniversary of the Launch Date (the “Initial Term”), unless terminated earlier as provided herein. Either Party may terminate this Agreement and Access Partner’s participation in the Program with effect from the date of expiry of the Initial Term or, as the case may be, any then-current Extension Term by providing the other Party with written notice of its intent to do so not less than six (6) months prior to the relevant date. In the event no such notice is given prior to the expiry date of the Initial Term or an Extension Term, this Agreement will automatically extend for an additional one (1) year term (each such one year period, an “Extension Term”) under the same terms and conditions.
25. **Program Change, Suspension, Discontinuation.**
- a. Apple reserves the right to:
    - i. suspend or delete and reactivate a Provisioned Credential on an Enabled Device: (A) at the User’s request (e.g. upon loss of the Enabled Device or service at an Apple Store); or (B) without the request of the User in the event (1) the User reports loss of the Enabled Device to Apple in person or by telephone, subject to verification of such User’s identification to Apple’s reasonable satisfaction, or (2) the User returns an Enabled Device or submits an Enabled Device for a product exchange or upgrade (or similar service) in accordance with Apple’s applicable return, exchange or upgrade policies; or
    - ii. to request that a Participating Provider or an Access Service Partner suspend provisioning for additional Credentials, processing for Provisioned Credentials, or any other services a Participating Provider or Access Service Partner may perform in connection with the Apple Technology, in the event that an underlying issue, pursuant to Sections 4.c, 11.h and 18, has occurred; provided, however, that any such suspension will be limited in scope and duration to the extent necessary to address the underlying issue giving rise to the request for suspension or termination.
  - b. Apple reserves the right to change, discontinue or suspend (for any period of time) any or all functionality, user interface, the Specifications (with respect to changes only) or any other aspect of the Apple Technology, Apple Access Platform, Apple

Access Platform or Program (whether software, hardware, or any part of the Apple Technology or Program) (a “Change”) at any time in the Territory, taking into consideration the high public nature of the Program, including suspension of provisioning and transaction usage. Notwithstanding anything to the contrary in this Agreement, Apple reserves the right to make Changes that Apple deems necessary to comply with applicable Law.

- c. Apple will provide Access Partner with written notice prior to implementing any Change that may reasonably be expected to result in changes to or otherwise impact Access Partner’s systems or processes; provided, however:
  - i. if the proposed Change is required to immediately remediate or prevent an Information Security Breach, Apple will have the right to implement the Change with ex-post facto notice in lieu of prior written notice; and
  - ii. Apple will not be required to notify Access Partner of non-public Changes to Apple’s user interface before such Changes become public.
- d. Subject to Section 25.c, Apple will provide Access Partner with reasonable advance notice of any such proposed Change. Each notice provided by Apple will include a description of the proposed Changes and all necessary information (as reasonably requested by Access Partner) to help Access Partner with the implementation of such Changes in a manner that complies with applicable Law.
- e. Following receipt of such notice, in the event that Access Partner: reasonably believes (upon advice of counsel) that the Change (1) fails to comply with applicable Law; or (2) causes or is reasonably likely to cause Access Partner to fail to comply with applicable Law, then Access Partner may request in writing that Apple modify the Change as it relates to Access Partner so as to remedy such failure (“Access Partner Change Compliance Request”). Promptly following the receipt of an Access Partner Change Compliance Request, Apple’s representatives will meet with Access Partner’s representatives, who will include legal counsel on the relevant applicable Law and discuss in good faith whether or not the Change fails to comply with applicable Law, or causes or is reasonably likely to cause the Participating Provider to fail to comply with applicable Law. If, after thirty (30) days of such discussions, Apple and Access Partner agree that there is a compliance issue that would require modification to the Changes, then Access Partner and Apple will discuss in good faith what modifications to the Changes are necessary to comply with applicable Law, and what modifications Apple is willing to implement. If, after thirty (30) days of such discussions, Apple has not agreed to implement modifications that, to Access Partner’s reasonable satisfaction, are required for Access Partner to support the Program in a manner that complies with applicable Law, then Access Partner may engage the Executive Review process set forth in Section 29 (Executive Review).
- f. Notwithstanding the above:
  - i. except as otherwise set forth in Section 25(c), the commitments in Section 25(d) will not apply to any changes, discontinuances, or suspensions related to a security breach or security vulnerability associated with the Apple Technology; and



- ii. in the event that any Change referred to in Section 25(d) adversely impacts the Participating Provider's terms and conditions related to the Provisioned Credential or will necessitate a commercially material change (including infeasible change) to or have a commercially material impact on Access Partner's systems or processes (including a material impact on Access Partner's technical ability to participate in the Program) (these impacts and changes will be referred to collectively as "Impact" in this Section 25), Apple and Access Partner will work together in good faith to minimize the impact of such Change pursuant to the process set forth in 25(g).
  
- g. In the event of the occurrence of the circumstances described in Section 25(f)(ii), Access Partner will provide Apple with written notice describing the Impact caused by any such Change. Upon receipt of such written notice, Apple's representatives will meet with Access Partner's representatives and discuss in good faith whether or not it is necessary to modify the Change. If, after thirty (30) days of such discussions, Apple and Access Partner agree that there is necessity of modification to the Changes, then Access Partner and Apple will discuss in good faith what modifications to the Changes are necessary, and what modifications Apple is willing to implement. If, after thirty (30) days of such discussions, Apple has not agreed to implement modifications that, to Access Partner's reasonable satisfaction, are required to sufficiently minimize the Impact, then Access Partner may engage the Executive Review process set forth in Section 29 (Executive Review).

**26. Suspension and Termination.**

- a. Prior to the end of the Term:
  - i. Access Partner's or a Participating Provider's participation in the Program may be suspended or this Agreement may be terminated by mutual written consent of the Parties;
  - ii. Access Partner's participation in the Program may be suspended by Apple in the event of Access Partner's material breach of this Agreement that is inherently incurable, or not otherwise cured within thirty (30) days of the Access Partner receiving notice of such breach;
  - iii. this Agreement may be terminated by either Party immediately upon written notice to the other Party, in the event of such other Party's material breach of this Agreement that is inherently incurable, or not otherwise cured within thirty (30) days of the breaching Party receiving notice of such breach;
  - iv. Access Partner's participation in the Program may be suspended or this Agreement may be terminated, by Apple immediately upon written notice to Access Partner in the event that Access Partner breaches Section 6 (Quiet Period);
  - v. Access Partner may suspend its participation in the Program immediately upon giving written notice to Apple in the event of a material Apple

Security Breach that results in a (A) significant compliance issue or risk under the applicable Law, or (B) significant unauthorized disclosure of User PII, provided that the Parties must observe the Executive Review process set out in Section 29 (Executive Review) prior to any termination of this Agreement;

- vi. Apple may suspend Access Partner's participation in the Program immediately upon giving written notice to Access Partner in the event of a material Access Partner or Participating Provider Security Breach that threatens to, or has had, a significant adverse effect on the Program or the Apple Technology related to the Program, provided that the Parties must observe the Executive Review process set out in Section 29 (Executive Review) prior to any termination of this Agreement; or
  - vii. Apple may suspend Access Partner's participation in the Program in the event that Access Partner fails to make a timely payment in accordance with Section 7 (Fees), Section 8 (Payment), or **Exhibit E (Billing Reports)** and fails to cure such payment default within ten (10) days following written notice from Apple.
  - viii. In the event that Access Partner's continued performance under the Agreement has a material adverse impact on Access Partner's ability to continue to function under the Program, Access Partner will have a right to terminate this Agreement without liability to Apple upon at least one-hundred eighty days' written notice to Apple and with an opportunity for Apple to resolve under the Executive Review process in Section 29 (Executive Review). of this Agreement. If, after the Executive Review is complete, the Parties are unable to determine a resolution that would allow Access Partner to continue participation under the Agreement, such termination will occur with immediate effect (unless a specified termination date is agreed to by the Parties).
- b. Termination of this Agreement will not relieve either Party of its obligation to pay any amounts payable under this Agreement as of the date of termination.
  - c. In the event of termination, the Parties will cooperate in good faith to ensure the orderly wind-down or transition of the Program, including providing all support to migrate Participating Providers to another Access Partner and such other transition support as reasonably requested by the other Party. To avoid disruption of services to Participating Providers and Users, the wind-down and transition period will be at least 1 year or longer as reasonably required. All terms and provisions of this Agreement, including any and all exhibits, addenda and amendments hereto, which by their nature are intended to survive any termination or expiration of this Agreement, will so survive, including Sections 1 (Apple Responsibilities), 7 (Fees) (to the extent applicable to Fees incurred during the Term), 12 (Intellectual Property Rights), 17 (Compliance with Law), 18 (Government Authority), 20 (No Other Warranties), 21 (Indemnification), 22 (Indemnification Procedures), 23 (Limitation of Liability), 27 (Assignment), 28 (Independent Parties), 30 (Governing Law), 31 (Miscellaneous), 34 (Arbitration) and **Exhibit A** (Definitions) in their entirety, as well as sub-sections 3.b, 11.d, 11.f, 11.g, 11.h (to the extent of Participating Provider De-Identified Data specific to the Program), 10.b, 13.a, 13.b

(with respect to any Technology jointly developed during the Term), 14.b, 14.d, 26.b and 29.c.

27. **Assignment.** The rights and obligations of Apple and Access Partner under this Agreement will be binding upon and inure to the benefit of the Parties' respective successors, executors and administrators, as the case may be. Neither Party may assign or delegate its rights or obligations under this Agreement, including Change of Control of the Access Partner, without the other Party's prior written consent. Any attempted assignment of this Agreement in violation of the foregoing will be null and void.
28. **Independent Parties.** The Parties hereto are independent contractors under this Agreement. Nothing in this Agreement will be construed to create a joint venture, partnership, employer-employee relationship, or agency or representative relationship between the Parties. Neither Party is authorized to represent, bind, obligate, or contract on behalf of the other or create liability against the other in any way or for any purpose. Accordingly, the Access Partner will in all correspondence and other dealings relating directly or indirectly to the provision of the Access Partner's services or the Apple Technology to Participating Providers clearly indicate that it is acting as a principal on its own account. In addition, the Access Partner must not:
- a. hold itself out as being an agent of Apple or as having authority to represent or act for or on behalf of Apple in any capacity whatsoever;
  - b. give any warranties or make any representations which are binding upon Apple in any way;
  - c. purchase or sell on any account of Apple whatsoever; or
  - d. incur any liability on behalf of Apple or in any way pledge or purport to pledge Apple's credit or accept any order or make any contract binding upon Apple.
29. **Executive Review.**
- a. A Party may initiate an executive review (an "Executive Review") where Executive Review is required or permitted by this Agreement, including a Party's exercise of any suspension or termination right in the Executive Review process is initiated pursuant to Section 4.c, 11.h, 11.e, 25.e, 25.g, 26.a.v, 26.a.vi or 26.a.viii.
  - b. To initiate an Executive Review, such Party must first refer, in writing, to the issue prompting such Party's request to the Senior Executives of both Parties for resolution (being Chief Executive Officer for Access Partner and the Vice President responsible for Apple Access (together, the "Senior Executives")).
  - c. The Senior Executives will meet at least once telephonically or in person and work in good faith to seek a resolution or remedy of the issue.
  - d. In the event of a breach, the Senior Executives will work in good faith to extend the cure period appropriately for the breach in question if (i) the remedy for the breach requires a technical solution that has been reasonably identified by the Parties, (ii) the Parties are making progress towards developing and deploying the technical solution within a commercially reasonable period of time, and (iii)

measures have been taken to prevent on-going loss or liability to the non-breaching Party until the deployment of such technical solution.

- e. If the resolution agreed to by the Senior Executives does not resolve or remedy the issue giving rise to Executive Review within thirty (30) days thereof, then the Senior Executives will determine whether any suspension is necessary, and in such event, the Senior Executives will use reasonable endeavors to seek the narrowest suspension (both in length and scope) that would (when applicable) allow the requesting Party to avoid incurring further loss or liability from the breach by the other Party.
  - f. Except where Executive Review is initiated pursuant to Section 25.d, in the event that the Senior Executives are unable to resolve or remedy the issue giving rise to Executive Review following suspension, the requesting Party may terminate the Agreement in its own discretion, provided that any such termination must be, in the requesting Party's good faith judgment, in the narrowest (both in length and scope) manner that would allow the requesting Party to avoid incurring further loss or liability from the breach by the other Party.
30. **Governing Law.** The validity, performance, construction, and interpretations of this Agreement will be governed by Delaware law, without giving effect to conflicts of laws principles. The Convention on Contracts for the International Sale of Goods will not apply to this Agreement.
31. **Miscellaneous.** In the event there is a conflict between the terms of this Agreement and the terms of any Exhibit referenced in this Agreement, the terms and conditions of the Exhibit will control to the extent of the conflict only.
32. **Notices.** Any notice required or permitted hereunder will be in writing. Such notice will be deemed given: upon personal delivery to the appropriate address; or five (5) Business Days after the date of mailing if sent by certified or registered mail; or three (3) Business Day after the date of deposit with a commercial courier service offering next Business Day service with confirmation of delivery.

Any notices to Apple will be sent to the address set forth below:

Apple Inc.  
Attention: Vice President, Apple Pay

With copies to:  
Apple Inc.  
One Apple Park Way  
Cupertino, California 95014  
Attention: Vice President, Apple Pay

Apple Inc.  
One Apple Park Way  
Cupertino, California 95014  
Attention: General Counsel

Any notices to Access Partner will be sent to the address set forth below:

Alert Enterprise .  
4350 Starboard Drive

Fremont, California 94538

Attention: Kaval Kaur

Alert Enterprise .  
4350 Starboard Drive

Fremont, California 94538

Attention: Legal Department

33. **Severability.** If at any time any provision of this Agreement is or becomes illegal, invalid or unenforceable in any respect under the law of any jurisdiction that will not affect or impair:

- a. the legality, validity or enforceability in that jurisdiction of any other provision of this Agreement; or
- b. the legality, validity or enforceability under the law of any other jurisdiction of that or any other provision of this Agreement.

34. **Arbitration.**

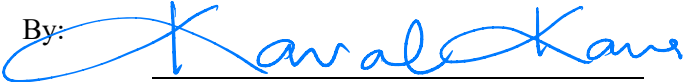
- a. All disputes arising out of or in connection with this Agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce by three arbitrators appointed in accordance with said Rules.
- b. The place of the arbitration shall be in order of preference - San Francisco, California. The language of the arbitration shall be English. In addition to the ICC Rules, the parties agree that the arbitration shall be conducted according to the IBA Rules on the Taking of Evidence in International Arbitration.
- c. The parties undertake to keep confidential the fact of any arbitration and all awards in the arbitration, together with all materials in the proceedings created for the purpose of the arbitration and all other documents produced by another party in the proceedings not otherwise in the public domain, save and to the extent that disclosure may be required of a party by legal duty, to protect or pursue a legal right or to enforce or challenge an award in legal proceedings before a court or other judicial authority.
- d. The arbitrators shall award to the prevailing party, if any, as determined by the arbitrators, its costs and expenses, including its attorneys' fees. The prevailing party shall also be entitled to its attorneys' fees and costs in any action to confirm and/or enforce any arbitral award in any judicial proceedings.

- e. This Agreement and any dispute arising under or in connection with this Agreement shall be governed by the laws of the State of Delaware, without regard to its choice of law principles except that this arbitration clause and any arbitration hereunder shall be governed by the Federal Arbitration Act, Chapters 1 and 2. The Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.
  - f. Nothing in this Agreement shall prevent either party from seeking provisional measures from any court of competent jurisdiction, and any such request shall not be deemed incompatible with the agreement to arbitrate or a waiver of the right to arbitrate. The parties hereby waive any requirements for security for obtaining any provisional relief.
  - g. Sovereign immunity (where applicable): To the extent that the Company may be entitled in any jurisdiction to claim for itself or its assets immunity (whether state or sovereign or otherwise) from service of process, jurisdiction, suit, judgment, execution, attachment (whether before judgment, in aid of execution, or otherwise) or legal process in respect of its obligations under this Agreement, or to the extent that, in any such jurisdiction, such immunity (whether or not claimed) may be attributed to it or its assets, the Company hereby irrevocably agrees not to claim, and hereby irrevocably waives, such immunity to the fullest extent permitted by the laws of such jurisdiction with the intent, inter alia, that such waiver of immunity shall have irrevocable effect.
35. **Rules of Interpretation.** The Parties have negotiated this Agreement with the advice, if desired, from their respective counsel. This Agreement will be fairly interpreted in accordance with its terms and without any strict construction in favor of or against either Party and no weight will be placed upon which Party or its counsel drafted the provision being interpreted. Except as otherwise expressly provided in this Agreement, the following rules will apply hereto:
- a. the singular includes the plural and the plural includes the singular;
  - b. “include”, “includes”, and “including” are not limiting;
  - c. unless the context otherwise requires or unless otherwise provided herein, references to a particular agreement, instrument, document, law, or regulation also refer to and include all renewals, extensions, modifications, amendments, and restatements of such agreement, instrument, document, law or regulation;
  - d. a reference in this Agreement to a Section or Exhibit is to the Section of or Exhibit to this Agreement unless otherwise expressly provided;
  - e. a reference to a Section in this Agreement will, unless the context clearly indicates to the contrary, refer to all subsections of such Section;
  - f. words such as “hereunder”, “hereto”, “hereof”, and “herein”, and other words of like import will, unless the context clearly indicates to the contrary, refer to the whole of this Agreement and not to any particular Section or subsection hereof;

- g. references to any statute will include any amendments thereto and its implementing regulations; and
- h. a reference to “or” is not exclusive.

IN WITNESS WHEREOF, Apple and Access Partner have executed this Agreement on the date set out below.

~~Alert Enterprises Inc.~~ ALERT ENTERPRISE INC

By: 

Name: KAVAL KAUR

Title: CFO

Date: May 29, 2024

**Apple Inc.**

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_



## Exhibit A

### Definitions

For the purposes of this Agreement, the following terms mean the following:

- a. “Access Guidelines” means documentation outlining the minimum program requirements and best practice guidelines that are required to support Apple Access Services and/or the Program, including such guidelines set forth in **Exhibit B (Credential Manager Integration Approach, Features and Functionality)** and **Exhibit C (Credential Provider Integration Approach, Features, and Functionality)**.
- b. “Access Partner” has the meaning set forth in the introduction of this Agreement.
- c. “Access Partner Brand Guidelines” means the guidelines of Access Partner provides to Apple in writing, plus any additional marketing and use guidelines provided by Access Partner in writing (including all amendments to any of the foregoing as may be furnished from time to time by Access Partner to Apple).
- d. “Access Partner Change Compliance Request” has the meaning set forth for such term in Section 25.e.
- e. “Access Partner Indemnified Party” has the meaning set forth for such term in Section 21.b.
- f. “Access Partner Marks” means all Marks set forth in **Exhibit I (Access Partner Marks)**, as may be amended in writing upon mutual agreement of the Parties from time to time.
- g. “Access Partner Patent Rights” has the meaning set forth for such term in Section 14.b.i.
- h. “Access Partner Security Breach” has the meaning set forth for such term in Section 11(f).
- i. “Access Partner Source Code Modifications” has the meaning set forth for such term in Section 14.e.i.
- j. “Access Partner Technology” means Technology owned, controlled or licensable by Access Partner or any of its Affiliates (other than Apple Technology).
- k. “Access Platform Participants” means Persons participating on the Apple Access Platform.
- l. “Access Service Partner” means an entity (other than Apple or Access Partner) that has entered into an agreement with Apple, and if Access Partner deems necessary, to act as a Credential Provider and/or Credential Manager in connection with the Program.

- m. “Account” means any account in the Territory under which a User may initiate any Access Service through a particular Participating Provider pursuant to a User Agreement.
- n. “Affiliate” means any Person that, now or in the future, during the Term Controls, is Controlled by, or is under common Control with either Party, but, in each case, only for so long as such Control exists.
- o. “API” means an application programming interface.
- p. “Apple Access Feedback” has the meaning set forth for such term in Section 10.c.
- q. “Apple Access Marketing Guidelines” means the marketing and use guidelines provided by Apple in writing (including all amendments to any of the foregoing as may be furnished from time to time by Apple to Access Partner).
- r. “Apple Access Platform” means Apple’s platform that utilizes Apple Technology, and may utilize Access Partner Technology pursuant to this Agreement, to enable Users to gain access to or authenticate virtually to use a physical space or controlled service using physical, digital or virtual access cards, credentials or account access devices and to access other related services using Apple Products designated by Apple or any of its Affiliates.
- s. “Apple Access Services” means the provisioning of Apple Access Technology to Participating Providers to enable Users to virtually authenticate to and/or to gain access to a physical space or service to utilize such physical space or service controlled or provided by a Participating Provider.
- t. “Apple Brand Guidelines” means the guidelines set forth at <http://www.apple.com/legal/trademark/guidelinesfor3rdparties.html> and <https://developer.apple.com/apple-pay/marketing>, as provided or made available to Access Partner by Apple, plus any additional marketing and use guidelines provided by Apple in writing (including all amendments to any of the foregoing as may be furnished or made available from time to time by Apple to Access Partner).
- u. “Apple Indemnified Party” has the meaning set forth for such term in Section 21.a.
- v. “Apple Initiative” has the meaning set forth for such term in Section 6.b.
- w. “Apple Marks” means all Marks set forth in **Exhibit D (Apple Marks)**, as may be amended in writing upon mutual agreement of the Parties from time to time.
- x. “Apple Metrics” means any metrics regarding Apple Access Platform or the Program (either specific to its own performance or providing any other metrics regarding the Program) in any format or context.
- y. “Apple Product” means any Technology, product, or service distributed under an Apple Mark, or used internally by Apple or any of its Affiliates.

- z. “Apple Provisioning Data” means any data supplied by Apple to Access Partner, a Participating Provider or, if applicable, Access Service Partner for the purpose of facilitating a Participating Provider’s provisioning path decision process.
- aa. “Apple Security Breach” has the meaning set forth for such term in Section 11(f).
- bb. “Apple Technology” means Technology owned, controlled or licensable by Apple or any of its Affiliates (other than Access Partner Technology).
- cc. “Business Day” means any day other than Saturday, Sunday and any banking or public holiday observed in the Territory.
- dd. “Calendar Day” means each day on the calendar beginning at 12:00 midnight, including Saturday, Sunday and any banking or public holiday observed in the Territory.
- ee. “Change” has the meaning set forth for such term in Section 25.b.
- ff. “Claim” means any claim (including counterclaim or cross-claim) or other assertion brought or threatened to be brought in a Legal Proceeding by a third party, or any investigation or any examination by a Governmental Authority.
- gg. “Competing Platform” means any Technology, other than the Apple Technology, that enables the use of a card or other access credential for the purposes of accessing a physical location, service, or conducting a payment transaction on personal electronic devices. For clarity, Access Partner’s existing Credential Technology using non-NFC technology will not be deemed a Competing Platform.
- hh. “Confidential Information” has the meaning set forth for such term in Section 10.a.
- ii. “Control” means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies on a Person, whether through the ownership of voting securities, by contract, or otherwise. For the avoidance of doubt, but not by way of limitation, the direct and indirect ownership of more than 50% of (a) the voting securities or (b) an interest in the assets, profits, or earnings of a Person will be deemed to constitute “control” of the Person.
- jj. “Credential” means any digital or virtual card, account access device, or other device capable of accessing an Account issued by Access Partner or an Access Service Partner at the request of a Participating Provider for the purposes of initiating a Transaction.
- kk. “Credential Manager” means Access Partner, where Access Partner assumes that role, or the Access Service Partner, where the Access Service Partner assumes that role, that contracts with Participating Providers to support and facilitate the integration of Credentials with the Apple Technology to send User information during Credential provisioning by Apple.
- ll. “Credential Provider” means Access Partner, where Access Partner assumes that role, or the Access Service Partner, where the Access Service Partner assume that

role, that contracts with Credential Manager and/or Apple to provide Credentials to Participating Providers.

- mm. “Credential Technology” means all Technology included in or used in connection with creating, issuing, provisioning, maintaining, authenticating, or protecting Access Partner’s or any of its Affiliates’ credentials and/or their interoperability with credential products or reader applications.
- nn. “De-Identified Data” means data that does not contain any information relating to an identified or identifiable natural person.
- oo. “Directed Party” has the meaning set forth for such term in Section 18.a.
- pp. “Dispute” has the meaning set forth for such term in Section 34.
- qq. “Enabled Device” means any Apple Product that has been enabled to store and/or transmit Provisioned Credentials.
- rr. “Executive Review” has the meaning set forth for such term in Section 29(a).
- ss. “Extension Term” has the meaning set forth for such term in Section 24.
- tt. “Fees” means the fees Access Partners owes to Apple as set forth and calculated in accordance with **Exhibit G (Commercial Addendum)**.
- uu. “GDPR” has the meaning set forth for such term in Section 11.a.
- vv. “Governmental Authority” means any domestic or foreign, federal, state, provincial, municipal or local government, any political subdivision thereof and any entity exercising executive, legislative, judicial, regulatory, or administrative functions of or pertaining to government, regardless of form, including any agency, bureau, court, tribunal, or other instrumentality.
- ww. “Impact” has the meaning set forth for such term in Section 25.f.ii.
- xx. “Indemnified Losses” means any and all liabilities, costs, and expenses (including reasonable fees and expenses for attorneys, experts and consultants, reasonable out-of-pocket costs, interest and penalties), settlements, equitable relief, judgments, offsets, or damages (including liquidated, special, consequential, punitive and exemplary damages) based on or resulting from any Claim.
- yy. “Indemnified Party” has the meaning set forth for such term in Section 20(a).
- zz. “Indemnifying Party” has the meaning set forth for such term in Section 20(a).
- aaa. “Information Security Breach” has the meaning set forth for such term in Section 11(f).
- bbb. “Initial Term” has the meaning set forth for such term in Section 24.
- ccc. “Integration Approach Exhibit” means **Exhibit B (Credential Manager Integration Approach, Features and Functionality)**, when acting as a Credential

Manager, or **Exhibit C (Credential Provider Integration Approach, Features, and Functionality)**, when acting as a Credential Provider.

- ddd. “Intellectual Property Rights” means the rights in and to all (i) patents and patent applications in any jurisdiction or under any international convention claiming any inventions or discoveries made, developed, conceived, or reduced to practice, including all divisions, divisionals, substitutions, continuations, continuations-in-part, reissues, re-examinations, renewals and extensions thereof; (ii) copyrights; (iii) confidential information and other proprietary information or data that qualifies for trade secret protection; (iv) semiconductor chip or mask work rights; (v) design patents or industrial designs, and (vi) other similar intellectual or other proprietary rights (excluding all Marks) now known or hereafter recognized in any jurisdiction.
- eee. “Launch Date” means the first date in the Territory that Apple Technology is available for use with Provisioned Credentials to conduct Transactions in the Territory.
- fff. “Laws” means all laws (including common law), codes, statutes, ordinances, rules, regulations, published standards, permits, judgments, writs, injunctions, rulings, administrative guidance or other regulatory bulletins or guidance, regulatory examinations or orders, decrees and orders of any Governmental Authority.
- ggg. “Legal Proceeding” means any judicial, administrative or arbitral action, suit, mediation, investigation, inquiry, proceeding, or claim (including counterclaim) by or before a Governmental Authority or arbitral body.
- hhh. “Marks” means all trademarks, service marks, trade dress, trade names, brand names, product names, business marks, logos, taglines, slogans, and similar designations that distinguish the source of goods or services, whether registered or unregistered, along with all registrations and pending applications for any of the foregoing.
- iii. “New Parent” has the meaning set forth for such term in Section 14.b.
- jjj. “Outage” means a material failure to provision Credentials or process Transactions on Provisioned Credentials.
- kkk. “Participating Provider” means (a) a customer of Access Partner or, if applicable, Access Service Partner or Access Partner’s Service Provider, that wishes to participate in the Program, and (b) is a party to a valid Participating Provider Agreement that is in full force and effect.
- lll. “Participating Provider Agreement” means an agreement between a Participating Provider and Access Partner (or where applicable Access Partner’s Service Provider) that incorporates the terms in **Exhibit J (“Participating Provider Pass-Through Terms”)**, which is otherwise in accordance with any requirements for a Participating Provider Agreement specified in this Agreement and which is in a format approved by Apple, in its reasonable discretion.
- mmm. “Participating Provider Data” means all information related specifically to an Account, Credential, Participating Provider, and/or User that is obtained, generated or created by or on behalf of such Participating Provider in connection with Account

- establishment, processing and maintenance activities, customer service, and Transaction data (as enumerated in the Access Guidelines).
- nnn. “Participating Provider De-Identified Data” means Participating Provider Data that does not consists of Personally Identifiable Information of Users.
- ooo. “Participating Provider Pass-Through Terms” means terms in **Exhibit J-1**.
- ppp. “Participating Provider Security Breach” has the meaning set forth for such term in Section 11(f).
- qqq. “Patent Rights” means rights in and to all patents and patent applications in any jurisdiction or under any international convention claiming any inventions or discoveries made, developed, conceived, or reduced to practice, including all divisions, divisionals, substitutions, continuations, continuations-in-part, reissues, re-examinations, renewals, and any extensions thereof.
- rrr. “Person” means any individual, corporation, limited liability company, partnership, firm, joint venture, association, trust, unincorporated organization, Governmental Authority or other entity.
- sss. “Personally Identifiable Information”, “Personal Data” or “PII” means any information that, when used alone or with other relevant data, can be used to identify an individual.
- ttt. “Program” has the meaning set forth for such term in Section 1.
- uuu. “Program Launch Date” means the date the Program is first made publicly available on a general basis by Apple and Access Partner to Participating Providers in the Territory for commercial use.
- vvv. “Provisioned Credential” means a Credential that has been provisioned to an Enabled Device so that the Enabled Device may be used to make Transactions using such Provisioned Credential.
- www. “Regulatory Guidance” has the meaning set forth for such term in Section 18.b.
- xxx. “Reports” has the meaning set forth for such term in Section 9.
- yyy. “Sanctioned Territory” means, at any time, a country or territory which is itself the subject or target to any sanction or embargo by the United States Government or other relevant foreign government authority with jurisdiction, without first obtaining appropriate government authorization.
- zzz. “Senior Executives” has the meaning set forth for such term in Section 29(b).
- aaaa. “Service Provider” means any subcontractor, independent contractor, or third party service provider engaged by a Party to provide a service on behalf of such Party.

- bbbb. “Sample Source Code” means the source code, and related source code documentation, owned by Apple and provided to Access Partner by Apple for the integration of Credentials with the Apple Access Platform.
- cccc. “Specifications” means all specifications, documentation, guidelines, and requirements associated with the Apple Access Platform, including the Apple Access Platform implementation and operation guidelines, provided or made available by Apple, as the same may be updated or supplemented by Apple from time to time.
- dddd. “System Changes” has the meaning set forth for such term in Section 4.c.
- eeee. “Technology” means any information, ideas, know-how, designs, drawings, specifications, schematics, software (including source and object codes), manuals and other documentation, data, databases, processes (including technical processes and business processes), or methods (including methods of operation or methods of production).
- ffff. “Term” means the Initial Term and any Extension Term (in each case as defined in Section 24).
- gggg. “Territory” means a country or territory that is not a Sanctioned Territory.
- hhhh. “Transaction” means using an Enabled Device to gain access to a physical space, or utilize a service controlled or provided by an entity that controls access to physical spaces, in locations agreed to by Access Partner, Participating Provider and Apple.
- iiii. “Unauthorized Transaction” means any Transaction initiated by a Person who is not authorized to make a Transaction on an Account, including any fraudulent use of any Transaction.
- jjjj. “User” means a Person that has entered into a User Agreement establishing an Account with a Participating Provider.
- kkkk. “User Account” means an Account that (a) is personalized with the User PII, (b) specifies access rights and authorizes/declines attempts to conduct Transactions, and (c) records Transaction history.
- llll. “User Agreement” means the agreement between a Participating Provider and a User (and any replacement of such agreement), establishing a User Account and governing the use of a Credential, together with any amendments, modifications or supplements that may be made to such User Agreement (and any replacement of such agreement).
- mmmm. “User PII” means Participating Provider Data that consists of Personally Identifiable Information of a User.
- nnnn. “Withholding Tax” has the meaning set forth for such term in Section 17.c.

## Exhibit B

### Credential Manager Integration Approach, Features, and Functionality

When Access Partner is acting as Credential Manager for the Program, the following integration approach, features, and functionality in this **Exhibit B** are required to be supported as part of the Program. The Parties will work together in good faith to determine any additional required Program-related features and functionality and project timelines. All features will be implemented in line with mutually agreed timelines to support the Program and all requisite testing activities. Apple will have sole final discretion on the required Program-related features and functionality.

<b>In-app Provisioning &amp; Multi-factor Authentication</b>
<p>Access Partner and Participating Provider must support in-app provisioning to provide a secure, seamless provisioning User experience from the Participating Provider's iOS mobile app or watchOS app (if applicable).</p> <ul style="list-style-type: none"><li>• Access Partner's mobile app(s) must support in-app provisioning and adhere to all Apple written guidelines and best practices pertaining to in-app provisioning as set forth in <b>Program Guidelines</b>.</li><li>• Access Partner will expose capabilities to third parties (Participating Providers or their selected developers) to support in-app provisioning within the Participating Provider-branded software application made available on an Enabled Device that is used to manage, administer, and/or use Credentials or an associated Account from an Enabled Device.</li><li>• iOS Mobile apps (including Access Partner and third party) performing in-app provisioning must support multi-factor authentication.</li></ul> <p>Access Partner will offer mobile key/credential as a default option in-app to all eligible Participating Providers and their Users.</p>
<b>Pass Attributes</b>
<p>A digital representation that reflects the physical pass art of the Participating Provider card must be provided (per Apple specifications) as set forth in <b>Program Guidelines</b> as updated in accordance with specification changes.</p>
<b>Real-Time Push Notifications</b>
<p>Access Partner, on behalf of Participating Providers, must support real-time transaction notifications via Apple Push Notification service (APNs) as set forth in <b>Program Guidelines</b>.</p>
<b>Card Lifecycle Management ("CLM")</b>
<p>Access Partner, on behalf of Participating Providers, must support fully automated CLM for real-time deletion, suspension, resumption, and updating of provisioned passes on Enabled Devices, including CLM initiated by the User (via iCloud, Credential Manager mobile app and/or Participating Provider's third party mobile app which includes Credential Manager iOS SDK) and by the Participating Provider as set forth in <b>Program Guidelines</b>.</p>



### **Customer Service**

Access Partner will support and require Participating Providers to support Users to provision passes on Enabled Devices via existing customer support channels (e.g., website, iOS mobile app, call center, in-person, etc.).

Access Partner will provide all relevant tools or APIs to support Participating Providers to enable such customer service and support the provisioning of Credentials to Enabled Devices.

### **Testing**

Access Partner will provide non-production and production test data for integration as well as automation testing as set forth in **Exhibit G (Credential Asset Management Program) and Exhibit J (Terminal/Reader Procurement)**. Test accounts will remain valid until they have been used by Apple.

Access Partner will, for each reader, make non-production and production connectivity to a representative back office management system available to allow for full Credential management testing with compatible NFC devices.

Access Partner must self-test (prior to launch of each Participating Provider and on an ongoing basis thereafter) in a certification environment (in accordance with the Apple provided Self-Test Plan) and report the percentage pass rate for review and approval by Apple.

### **Provisioning & Credential Support**

#### ***Credential Technology***

Access Partner will support the provisioning of the following credential technologies:

- Apple Unified Air Protocol, and
- MIFARE DESFire

***Provisioning***

Access Partner will support the provisioning of the above-referenced credential technologies utilizing the Specifications.

Access Partner will adhere to SLAs and performance requirements as outlined within this Exhibit.

***Key Management***

Access Partner readers will support requirements as set forth in **Access Security Guidelines**.

**SLAs**

**§ Server Connectivity**

- Set up a QA, Load Test, and Production environment.
- A highly-available disaster recovery configuration, such that traffic may be served out of an alternative datacenter in the event the primary datacenter is unavailable or otherwise cannot serve traffic. Alternatively, maintain an active/active architecture where multiple datacenter can serve traffic simultaneously, in at least different physical locations, that provides for automatic failover within 5 minutes. Two countries may be required to support expansion outside of the US.
- Prior to launch, a 2.2 seconds for 90th percentile of API calls, which will be required upfront, agreed upon defaults should the Participating Provider's other systems or the Issuer's systems respond slowly for any reason
- 99.99% uptime for production environments, including planned and unplanned outages. A minimum seven day notice prior to planned outages/maintenance.
- 98% uptime for all non-production environments (and accountability for issuer connection), including planned and unplanned outages.
- 95% for automated testing QA environments including planned outages
- 95% for functional testing QA (and accountability for issuer connection) including planned outages
- Projections for scale volume transaction per second /capacity to be mutually agreed upon.
- Delayed response times from one Issuer should not have an adverse impact on the response times for other Issuers utilizing the Participating Provider services.

**§ Disaster Recovery**

- Services should be hosted from multiple, geographically-distributed data centers / cloud regions
- Individual data centers / cloud regions should have a fault tolerant, highly available architecture
- Data centers/cloud regions should be configured in active/active or active/passive architecture. At a minimum, passive sites should be configured as a "hot standby".
- Access Partner should operate a fault detection system that is configured to automatically shift traffic away from an unhealthy region, to a healthy one.
- Access Partner should be able to failover / perform DR preferably without any downtime OR not exceeding any more than 30 minutes of interruption
- Projections for scale volume transactions per second/ capacity to be mutually agreed
- Disaster Recovery Plan should be shared
- Joint Disaster Recovery exercises must be conducted prior to launch

## Exhibit C

### Credential Provider Integration Approach, Features, and Functionality

When Access Partner is acting as the Credential Provider for the Program, the following integration approach, features, and functionality in this **Exhibit C** are required to be supported as part of the Program. The Parties will work together in good faith to determine any additional required Program-related features and functionality and project timelines. All features will be implemented in line with mutually agreed timelines to support the Program and all requisite testing activities. Apple will have sole final discretion on the required Program-related features and functionality

<b>Provisioning &amp; Credential Support</b>
<i>Credential Technology</i>
Access Partner will support the provisioning of the following credential technologies: <ul style="list-style-type: none"><li>• Apple Unified Air Protocol, and</li><li>• MIFARE DESFire</li></ul>
<i>Provisioning</i>
Access Partner will support the provisioning of the above-referenced credential technologies utilizing the Specifications.  Access Partner will adhere to SLAs and performance requirements as outlined within this Exhibit B, <i>Guidelines for Contactless Access Pass in Apple Wallet</i> (the “ <u>Program Guidelines</u> ”).
<i>Key Management</i>
Access Partner readers will support requirements as set forth in <i>Access Partner Security Requirements</i> (the “ <u>Access Security Guidelines</u> ”).
<b>Customer Service</b>
Access Partner will provide support to Participating Providers and, if applicable, to Access Service Partners that are acting as credential managers, to and for Provisioned Credentials on Enabled Devices.  Access Partner will provide all relevant tools or APIs to support Participating Providers and, if applicable, Access Service Partners that are acting as credential managers, to enable such customer service and support the provisioning of Credentials to Enabled Devices.

## Testing

Access Partner will provide non-production and production test data for integration as well as automation testing as set forth in **Exhibits G (Credential Asset Management Program) and J (Terminal/Reader Procurement)**. Test accounts will remain valid until they have been used by Apple.

Access Partner will procure and set up a minimum of three (3) non-production keyed and three (3) production keyed readers representative of Licensed Products and provide updated readers to Apple from time to time upon request.

Access Partner will, for each reader, make non-production and production connectivity to a representative back office management system available to allow for full Credential management testing with compatible NFC devices.

Access Partner must self-test (prior to launch of each Participating Provider and on an ongoing basis thereafter) in a certification environment (in accordance with the Apple provided Self-Test Plan) and report the percentage pass rate for review and approval by Apple.

## Reader Support

### Adherence to Specifications

Any reader configured under the Apple Specification to operate within the Program will comply with such Specifications.

### Reader Security

Apple will have the right to review Access Partner (or its Affiliates) reader implementations to assess any security vulnerabilities and suggest mitigation for use within the Program. Specifically, Apple will have the ability to review security evaluation test reports based on tests completed by Access Partner or external labs.

### Express Mode Support

As a base configuration, Access Partner readers will support the Apple Enhanced Contactless Polling (ECP2.x) specification to enable Express Mode with auto presentment.

Access Partner will support configuration associated with Terminal Requested Authentication in line with Program Guidelines.

## SLAs

### § Server Connectivity

- Set up a QA, Load Test, and Production environment.
- A highly-available disaster recovery configuration, such that traffic may be served out of an alternative datacenter in the event the primary datacenter is unavailable or otherwise cannot serve traffic. Alternatively, maintain an active/active architecture where multiple datacenter can serve traffic simultaneously, in at least different physical locations, that provides for automatic failover within 5 minutes. Two countries may be required to support expansion outside of the US.
- Prior to launch, a 2.2 seconds for 90th percentile of API calls, which will be required upfront, agreed upon defaults should the Provider's other systems or the Issuer's systems respond slowly for any reason
- 99.99% uptime for production environments, including planned and unplanned outages. A minimum seven day notice prior to planned outages/maintenance.
- 98% uptime for all non-production environments (and accountability for issuer connection), including planned and unplanned outages.
- 95% for automated testing QA environments including planned outages
- 95% for functional testing QA (and accountability for issuer connection) including planned outages
- Projections for scale volume transaction per second /capacity to be mutually agreed upon.
- Delayed response times from one Issuer should not have an adverse impact on the response times for other Issuers utilizing the Participating Provider services.

### § Disaster Recovery

- Services should be hosted from multiple, geographically-distributed data centers / cloud regions
- Individual data centers/cloud regions should have a fault tolerant, highly available architecture
- Data centers/cloud regions should be configured in active/active or active/passive architecture. At a minimum, passive sites should be configured as a "hot standby".
- Access Partner should operate a fault detection system that is configured to automatically shift traffic away from an unhealthy region, to a healthy one.
- Access Partner should be able to failover/perform DR preferably without any downtime OR not exceeding any more than 30 minutes of interruption
- Projections for scale volume transactions per second/ capacity to be mutually agreed
- Disaster Recovery Plan should be shared

**Exhibit D**  
**Apple Marks**

Apple
Apple logo
Apple Pay
Apple Pay logo
Apple Watch (including rights to display images of the Apple Watch)
iPhone (including rights to display images of the iPhone device, but only those models that are technologically capable of being an Enabled Device)
Touch ID
Face ID
App Store
iCloud
Wallet
Apple Wallet

## **Exhibit E**

### **Billing Reports**

Billing will be provided as prescribed specifically for each use case under this agreement, and as amended from time to time by Apple. Each new use case will be included in a relevant sub-exhibit and numbered E-1 and E-2, etc.

Access Partner (when acting as Credential Manager) must create Billing Reports and submit them to Apple by the 10th Business Day of each calendar month. Billing Reports must be provided in the below format. All Billing Reports must be submitted by Access Partner within the given timeframe through PartnerConnect; a web-portal hosted by Apple. Detailed monthly processes are outlined below:

#### **Monthly Upload Process**

Access Partner generates Billing Report.

Access Partner submits Billing Report to PartnerConnect by the 15th Calendar Day of each month.

Access Partner receives an Invoice from Apple by the last Friday of each month.

Access Partner has N30 days of the invoice date to remit payment via Bank Transfer.

#### **Method of Payment**

Payments must be sent via Bank transfer to an account provided by Apple at a later date.

Payments must reference the Invoice number, SAP ID number, and PO number displayed on the invoice.

#### **Billing Report Details**

Access Partner Name: The business name for Access Partner.

Posting Cycle: The calendar month cycle for the reported fees.

Currency: The currency which Access Partner will be billed. This should be US Dollars].

Reported Month: The calendar month of the posting cycle.

Fee Type: The description of the fee type being reported. The fee type descriptions will be provided at a later date.

Calculated Total Fees: The total amount of each fee type.

PO Number: Access Partner PO number for each fee type.

Notes: Optional text field. Notes should be the same for each Fee Type.

#### **Incorrect Reports and/or Invoices**

Any incorrect invoice or report is subject to review. If both parties agree there is an error, a credit note will be issued by Apple to 'clear' the original invoice.

A new invoice will be sent with the appropriate totals and a new payment term of 30 days will be set.

<b>HDRC</b>	<b>Partner Name</b>	<b>Posting Cycle</b>	<b>Currency</b>	<b>Reported Month</b>
<b>HDR</b>				
<b>DTLC</b>	<b>Fee Type</b>	<b>Calculated Total Fees</b>	<b>PO Number</b>	<b>Notes</b>
<b>DTL</b>	None			
<b>DTL</b>	None			
<b>DTL</b>	None			
<b>DTL</b>	None			
<b>DTL</b>	None			
<b>DTL</b>	None			

All reports to be delivered monthly, as indicated in the table above, will be delivered on the 15th Calendar Day of each month, in conjunction with any fee reports due in accordance with section 8(a). If reports cannot be delivered on time, both parties will discuss and decide on a new deadline.

Apple has the right to update billing processes from time to time. Apple will inform the Access Partner (in its role as Program Manager) 90 days before the changes need to be implemented and live.



## **Exhibit F**

### **Data to be included in Reports**

The following reporting data must be collected by Access Partner (when acting as Credential Manager) and provided to Apple over an SFTP that is hosted by such Access Partner. A report must contain aggregated data at the institution/university level.

All reporting metrics must be sent on a Daily, Weekly, and Monthly cadence. The specific daily timelines and SFTP configuration are outlined in the associated “D-2 SFTP Reporting Requirements” document which should be referenced with this exhibit.

#### **The following will be provided by Access Partner:**

- A. Ever Provisioned - Apple Access
  - 1) By Enabled Device type (i.e. iPhone and Apple Watch)
  - 2) By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)
- B. Live Credential - Apple Access
  - 1) By Enabled Device type (i.e. iPhone and Apple Watch)
  - 2) By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)

**Access Partner will provide the following data to Apple upon request, on a monthly or quarterly basis:**

- A. Transaction - Apple Access
  - 1) By Enabled Device type (i.e. iPhone and Apple Watch)
  - 2) Optional, if available: By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)
  - 3) By Transaction type (i.e. Door Access, Event)
- B. Ever Provisioned – Other
  - 1) Other Mobile Wallets
  - 2) Physical/Plastic Cards
- C. Live Credential – Other
  - 1) Other Mobile Wallets
  - 2) Physical/Plastic Cards
- D. Transaction – Other
  - 1) Other Mobile Wallets
    - i. By Transaction type (i.e. Door Access, Event,)
    - ii. By Transaction Status (i.e. Successful/Declines)
  - 2) Physical Cards
    - i. By Transaction type (i.e. Door Access, Event,)
    - ii. By Transaction Status (i.e. Successful/Declines)
- E. Total Enabled Users
  - 1) By Device type (i.e. iPhone and Apple Watch)
  - 2) By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)

Access Partner will provide the following data to Apple at the time of Participating Provider launch:

- A. Total Eligible Users
  - 1) By OS type (i.e. iOS, Android)

*\*“Live Credentials” means Credentials that have been provisioned and are “live” on a device*

*\*\* “Enabled User” means individuals using an iPhone or Apple watch within a Participating Provider Property*

## Exhibit G

### Commercial Addendum

Commercial terms are as agreed specifically for each use case under this agreement, and as amended from time to time by Apple.

#### Currency

Fees are denominated in US Dollars

#### Fees

When acting as credential manager, Access Partner will set a rate for Provisioned Credentials as part of the launch Program in an amount which may change from time to time based on Access Partner's sole discretion.

Access Partner will not impose any Program-specific fees or other commercial terms on Participating Providers for such Participating Providers use of, or participation in the Program, where such fees or terms would reasonably be expected to discriminate against Apple as compared to other fees or commercial terms imposed by Access Partner on Participating with respect to a Competing Platform.

The initial rate for Provisioned Credentials will be the following and are subject to change as stated herein:

#### **CORPORATE:**

**Employees/Contractors/Long-term User Fee** – For Users expected to utilize a Provisioned Credential for long-term use, a non-prorated annual Fee of \$3 per iCloud Account under which a Provisioned Credential has been issued. For avoidance of doubt, (i) no new fee will be assessed on life cycle management events; and (ii) users may provision Credentials to multiple devices (i.e., iPhone and Watch) connected to the same iCloud account for a single annual Fee. The annual Fee period begins when the User provisions the Credential to an Enabled Device. The Provisioned Credential automatically renews, and another Fee will be incurred until the initiation of revocation of the Provisioned Credential in accordance with the Specification.

**Visitors/Temporary guest Users** – For Users expected to utilize a Provisioned Credential for short-term use (including, but not limited, to use for one day or a month), a non-prorated daily fee of \$0.15 per iCloud Account under which a Provisioned Credential has been issued for a 24-hour period. For avoidance of doubt, (i) no new fee will be assessed on life cycle management events; and (ii) users may provision Credentials to multiple devices (i.e., iPhone and Watch) connected to the same iCloud account, subject to applicable device limits, for the daily fee. The 24-hour period begins when the User provisions the Credential to an Enabled Device and becomes a Provisioned Credential. Another 24-hour period will automatically begin, and another Visitor Fee will be incurred until the initiation of revocation of the Provisioned Credential in accordance with the Specification.

#### **HOSPITALITY:**

A non-prorated Fee of \$0.40 per iCloud Account under which a Provisioned Credential has been issued to a User per stay and every 30 days at any given property. For avoidance of doubt, (i) no new fee will be assessed on life cycle management events; and (ii) users may provision Credentials to multiple devices (i.e., iPhone and Watch) connected to the same iCloud account for a single per stay fee. This Fee will include any sharing of temporary keys to iCloud accounts other than the User. The per stay fee period begins when the User provisions the Credential to an Enabled Device such that the Enabled Device may be used to make Transactions as authorized by the Access Partner

and/or Participating Provider.

**MULTI-FAMILY HOME:**

A non-prorated annual Fee of \$5.50 per iCloud Account. For avoidance of doubt, no new fee will be assessed on life cycle management events, including when a credential is transferred to another device. This Fee will include any sharing of temporary keys to iCloud accounts other than the User. The annual Fee period begins when the User provisions the Credential to an Enabled Device such that the Enabled Device may be used to make Transactions as authorized by the Access Partner and/or Participating Provider. The Provisioned Credential automatically renews, and another Fee will be incurred until the initiation of revocation of the Provisioned Credential in accordance with the Specification.

**UNIVERSITY:**

A non-prorated annual Fee of \$0.83 per iCloud Account. For avoidance of doubt, no new fee will be assessed on life cycle management events, including when a credential is transferred to another device. This Fee will include any sharing of temporary keys to iCloud accounts other than the User. The annual Fee period begins when the User provisions the Credential to an Enabled Device such that the Enabled Device may be used to make Transactions as authorized by the Access Partner and/or Participating Provider. The Provisioned Credential automatically renews, and another Fee will be incurred until the initiation of revocation of the Provisioned Credential in accordance with the Specification.

## **Exhibit H**

### **Supported Reader Models**

The following is a list of all reader models that have a base configuration that will support the requirements of the Program. This list will be updated on a quarterly basis.

## **Exhibit I**

### **Credential Asset Management Program**

The requirements for production will be provided by URL. Until such documentation is available online, the following will apply.

This document will outline the requirements for production credentials and how they will be managed. Credentials will be provided as requested by Apple to validate new credential technologies, integration approaches, Access Partner, or Participating Providers.

The Credential Asset Management Program will be agreed with any Participating Providers where Apple deems it is necessary to conduct end-to-end testing. In cases where testing is conducted, an approach will be agreed and a joint program will be initiated.

#### **Account Attributes**

Apple requires multiple accounts for each pass type offered by the partner.

Apple requires each account type to be offered in QA and Production.

Each account must include a login and password provided by an Access Partner.

Each account (in both environments) must be reconfigurable on balances, access, images, and user information by a Credential Manager with support of the Access Partner.

Reconfigurations must be complete within a 24-hour timeframe.

#### **Number of Accounts/Credentials**

Access Partner must be able to provide 25 accounts per environment (QA and Production) for a total of 50 accounts.

Accounts may not be requested until after go-live. These accounts will be used for validation testing or marketing campaigns hosted by Apple.

More accounts may be requested for testing purposes which will be negotiated and agreed by both parties.

#### **Account and Credential Use**

Accounts and Credentials used by the E2E testing team will be used in a lab.

Provisioning will be completed using green flow.

Accounts and Credentials will also be used to test future hardware/software before Access Partner, when acting as the credential manager, or Participating Providers can be disclosed.

Accounts and Credentials used by the field testing team will be used in a lab and at Participating Provider sites in coordination with the Participating Providers.

Prior to launch, Accounts and Credentials will be provisioned to disguised devices.

Testing will take place at multiple locations.

After launch, testers will continue to test at campus locations that are Apple Access enabled and at any future locations that are soon to be Apple Access enabled.

The Accounts and Credentials used by marketing for promotions or executive demos will be used in a studio or in a Participating Provider setting.

Marketing will use Accounts and Credentials to prepare marketing images and videos for the website, commercials and demos.

Executives will use the Accounts and Credentials for internal leadership demonstrations/discussions as well as “in the field” demonstrations at promotional events.

Accounts and Credentials used by various other Apple teams (including in-app review) will be used in a lab.

Access Partners may be required to provide credentials to third-party test lab to run additional testing on behalf of Apple. The lab will be agreed upon prior to the creation of new accounts.

Quantities, configurations, SLAs, and setup for test labs must match the requirements from Apple as outlined in sections A, B, and C.

### **Re-Issue of Accounts and Credentials**

If the Accounts and Credentials issued become unusable, Access Partner and/or Participating Provider must provide a new batch of all Account and Credential types.

### **Account Owners**

All Accounts and Credentials will be issued to Apple. Apple will be fully liable for all changes made by Apple employees and testers.

All Accounts and Credentials will be tracked and assigned to testers by Apple’s Business Operations team.

Apple is responsible for guaranteeing all balances are paid at the end of every billing cycle.

### **Participating Provider Support**

For ongoing support, a servicing email group should be set up so that any issues with the Accounts and Credentials can be resolved within one (1) Business Day.

### **Governance Process**

A yearly review will be established to review use, process, and reporting for all Accounts and Credentials.

### **Risks and Mitigations**

If an Account or Credential is lost or stolen, the tester is responsible for notifying Global Lead or any subsequent personnel designated by Apple who will work Access Partner, when acting as credential manager, and/or the Participating Provider to blacklist and reissue credential.

If any issues with the credentials or balances are discovered, Access Partner, when acting the credential manager, and/or Participating Provider should contact Global Lead who will resolve the issue.

## **Exhibit J**

### **Participating Provider Pass-Through Terms**

The Participating Provider Agreement between Access Partner and Participating Providers will contain the following terms passed through exactly as provided in **Exhibit J-1**. These terms will apply only so long as Credentials offered by a Participating Provider are included in the Program. Apple will define an approval process and any necessary forms to enable this approach. The form will ensure that each Participating Provider acknowledges and agrees to the program terms, and Apple will make the ultimate decision on any exceptions. Apple will be notified as each party requests to participate in the platform and will provide approval prior to the Participating Provider launching the Program.



## Exhibit J-1

### Participating Provider Pass-Through Terms for the Apple Access Platform

These Terms and Conditions (“Terms and Conditions”) are in addition to the Alert Enterprises Agreement and Related Services (“Terms of Service”). These additional terms apply if You use Apple Access Technology to securely execute instructions given by Users via Apple Access Technology and for the purpose of enabling Users to securely use Provisioned Credentials to make Transactions (the “Program”). All foregoing terms shall have the meaning set forth below.

**In the event of a conflict between these Terms and Conditions and the Terms of Service, these Terms and Conditions shall govern with respect to Your use of the Apple Access Technology.**

#### Definitions.

“Access Partner” shall mean Alert Enterprises Agreement or an affiliated entity of Alert Enterprises.

“Access Partner Data” means any data supplied by Access Partner to Apple or Participating Provider for the purpose of facilitating Participating Provider’s provisioning path decision process.

“Access Partner Technology” means Technology owned, controlled or licensable by Access Partner or any of its Affiliates (other than Apple Technology).

“Access Services” means the provisioning of Apple Access Technology to Participating Providers to enable Users to virtually authenticate to and/or to gain access to a physical space or service to utilize such physical space or service controlled or provided by a Participating Provider.

“Account” means any account under which a User may initiate any Access Service through Participating Provider pursuant to a User Agreement.

“Affiliate” means, with respect to a party, any Person that controls, is controlled by, or is under common control with such party. As used in this definition, the term “control” means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract, or otherwise. For the avoidance of doubt, but not by way of limitation, the direct and indirect ownership of more than fifty percent (50%) of (i) the voting securities or (ii) an interest in the assets, profits, or earnings of a Person will be deemed to constitute “control” of the Person.

“Apple Access Guidelines” means documentation outlining the minimum program requirements and best practice guidelines that are required to support Access Services and/or the Program. Such Apple Access Guidelines may be updated from time to time will and be provided by Access Partner as a .pdf upon request until a hyperlink becomes available.

“Apple Access Platform” means Apple’s platform that utilizes Apple Technology, and may utilize Access Partner Technology pursuant to Apple’s agreement with Access Partner, to enable Users to gain access to or authenticate virtually to use a physical space or controlled service using physical, digital or virtual access cards, credentials or account access devices and to access other related services using Apple Products designated by Apple or any of its Affiliates.

“Apple Product” means any Technology, product, or service distributed under an Apple Mark, or used internally and under development for distribution under an Apple Mark or an Apple Affiliate.

“Apple Access Technology” means the Apple Technology that enables Users to gain access to a physical space or controlled service, or authenticate virtually to use (physically, virtually, or otherwise) Participating Provider services, using Apple Products designated by Apple or any of its Affiliates.

“Apple Brand Guidelines” means the guidelines set forth at <http://www.apple.com/legal/trademark/guidelinesfor3rdparties.html> (“Apple Trademark and Copyright Guidelines”) and <https://developer.apple.com/apple-pay/marketing> (“Apple Pay Marketing Guidelines”).

“Apple Marks” means all Marks set forth in Exhibit C (Apple Marks), as may be amended by Apple from time to time. “Apple Technology” means Technology owned, controlled or licensable by Apple or any of its Affiliates.

“Credential” means any digital or virtual card, account access device, or other device capable of accessing an Account issued by Access Partner at the request of Participating Provider for the purposes of initiating an Access Service.

“Effective Date” means the Effective Date of your Terms of Service applicable to Your use of Alert Enterprises agreement and Related Services.

“Enabled Device” means any Apple Product that has been enabled to store and/or transmit Provisioned Credentials.

“Governmental Authority” means any domestic or foreign, federal, state, provincial, municipal or local government, any political subdivision thereof and any entity exercising executive, legislative, judicial, regulatory, or administrative functions of or pertaining to government, regardless of form, including any agency, bureau, court, tribunal, or other instrumentality.

“Intellectual Property Rights” means the rights in and to all (i) patents and patent applications in any jurisdiction or under any international convention claiming any inventions or discoveries made, developed, conceived, or reduced to practice, including all divisions, divisionals, substitutions, continuations, continuations-in-part, reissues, re-examinations, renewals and extensions thereof; (ii) copyrights; (iii) confidential information and other proprietary information or data that qualifies for trade secret protection; (iv) semiconductor chip or mask work rights; (v) design patents or industrial designs, and (vi) other similar intellectual or other proprietary rights (excluding all Marks) now known or hereafter recognized in any jurisdiction.

“Law” means any federal, state, local or foreign law (including common law), code, statute, ordinance, rule, regulation, published standard, permit, judgment, writ, injunction, rulings or other legal requirement.

“Marks” means all trademarks, service marks, trade dress, trade names, brand names, product names, business marks, logos, taglines, slogans, and similar designations that distinguish the source of goods or services, whether registered or unregistered, along with all registrations and pending applications for any of the foregoing.

“Non-Apple Access Service” means any software, other than the Apple Pay Technology, that enables the use of a digital or virtual card for the purposes of gaining access to a physical space or authenticating to utilize a controlled service on personal electronic devices.

“Participating Provider” shall mean You as the End Customer.

“Participating Provider Data” means all information related specifically to an Account, Credential, Participating Provider, and/or User that is obtained, generated or created by or on behalf of such Participating

Provider in connection with Account establishment, processing and maintenance activities, customer service, and transaction data (as enumerated in the Apple Access Guidelines).

“Participating Provider Properties” means properties owned, leased, or controlled by Participating Provider that are participating in the Program.

“Participating Provider Technology” means Technology owned, controlled or licensable by Participating Provider or any of its Affiliates.

“Person” means any individual, corporation, limited liability company, partnership, firm, joint venture, association, trust, unincorporated organization, Governmental Authority or other entity.

“Provisioned Credential” means a Credential that has been provisioned to an Enabled Device so that the Enabled Device may be used to make Access Services available using such Provisioned Credential.

“Service Provider” means any subcontractor, independent contractor, or third party service provider engaged by a party to provide a service on behalf of such party.

“Technology” means any information, ideas, know-how, designs, drawings, specifications, schematics, software (including source and object codes), manuals and other documentation, data, databases, processes (including technical processes and business processes), or methods (including methods of operation or methods of production).

“Transaction” means using an Enabled Device to gain access to a physical space, or utilize a service controlled or provided by an entity that controls access to physical spaces, in locations agreed to by Access Partner, Participating Provider and Apple.

“User” means a Person that has entered into a User Agreement establishing an Account with a Participating Provider.

“User Agreement” means the agreement between Participating Provider and a User (and any replacement of such agreement), establishing a User Account and governing the use of a Credential, together with any amendments, modifications or supplements that may be made to such User Agreement (and any replacement of such agreement).

## **Terms.**

All aspects of the Participating Provider implementation will meet the Apple Access Guidelines.

Participating Provider will ensure that Provisioned Credentials can be used everywhere physical access credentials can be used in Participating Provider Properties, unless an exception is pre-approved in writing by Access Partner and based on guidelines provided by Apple.

To support the end-to-end user mobile contactless experience, if Participating Provider Properties are enabled for the hospitality use case, all Participating Provider’s payment systems accepting payment cards (credit/debit) at such properties will accept Apple Pay (including Apple Pay Cash, as described in the Apple Access Guidelines), unless an exception is pre-approved in writing by Apple.

For provisioning of Credentials, Participating Provider will authorize Access Partner to send data, including Access Partner Data in its possession or control, and any other necessary identifiers for Credentials issued by Participating Provider to Apple necessary to provision credentials.

Participating Provider will support Users by ensuring that the level of service (both in quality and the types

of transactions that can be supported) provided for Provisioned Credentials is at least on parity with the level of service provided to physical credentials and credentials offered by Non-Apple Access Services.

Participating Provider will be responsible for the management of the relationship with Users, including being responsible for: (i) the decision to approve or deny provisioning of Credentials to an Enabled Device; (ii) the right to decline the use of a Provisioned Credential to make Transactions (where technically possible to do so); (iii) the on-going management and operation of Accounts, including whether any Provisioned Credential, should be suspended or deactivated; and (iv) providing all access services to Users in connection with Provisioned Credentials.

Apple (on behalf of itself and each of its Affiliates) hereby grants Participating Provider and each of its Affiliates, during the term, a non-exclusive, non-assignable, non-transferable, non-sublicensable, royalty-free, fully paid-up, worldwide right and license to use, reproduce, have reproduced, display, and have displayed any of the Apple Marks solely for the purposes of announcing and promoting the provisioning of Credentials on Enabled Devices at Participating Provider Properties, subject in all cases to Apple's prior written consent. Use of the Apple Marks by Participating Provider, its Affiliates or Service Providers will be pursuant to, and in accordance with, the Apple Brand Guidelines, unless otherwise agreed in writing by Apple and Participating Provider. For the avoidance of doubt, in the event Participating Provider wishes to use any of the Apple Marks in any paid advertising, Participating Provider must first obtain Apple's written consent for such advertising. Apple represents and warrants that, as of the Effective Date, Apple has the right to grant all of the licenses and other rights granted to Participating Provider and each of its Affiliates and Service Providers in these Terms and Conditions. For clarity, the foregoing license shall terminate immediately upon termination of Participating Provider's participation in the Program for any reason.

Participating Provider will ensure that the level of user awareness (both in quality and the types of use cases featured) provided by Participating Provider for Provisioned Credentials is at least on parity with the user awareness provided for physical credentials and/or credentials on Non-Apple Access Services.

Participating Provider will market and describe the Program to potential users in accordance with the Apple Access Marketing Guidelines unless an exception is pre-approved by in writing Apple.

In no event will Participating Provider promote or advertise the launch of credential services for Non-Apple Access Service using the Apple Access Guidelines or the Apple Access Marketing Guidelines provided by Apple.

**System Changes.** Absent prior written notice to Access Partner, Participating Provider may not implement changes to its systems, procedures, processes or functionality, which, as the case may be, may have a material impact on: (a) the Apple Access Technology; (b) the manner in which Credentials are provisioned on an Enabled Device, or (c) the manner in which Credentials provisioned to an Enabled Device function or are processed on the Apple Access Technology (such changes to systems, procedures, processes or functionality are referred as to "System Changes"). In addition, and not by way of limitation, Participating Provider will (i) notify Access Partner not less than ninety (90) days prior to any System Change that Participating Provider reasonably believes will disable any core functionality of the Apple Access Technology, or introduce any material additional security exposure to Apple or consumers and (ii) provide support to Access Partner to work in good faith with Apple to address any bona fide concerns of Apple with regard to such proposed System Change. If Apple objects to any System Change, the System Change may not go forward until the objection is resolved.

#### **Intellectual Property.**

1. Participating Provider and its Affiliates own or have the right to use all Participating Provider Technology (and all Intellectual Property Rights therein or thereto). Apple and its Affiliates own or have the right to use all Apple Technology (and all Intellectual Property Rights therein or thereto).
2. Except as agreed in writing by Apple and Participating Provider, no other rights or licenses to exploit (in whole or in part), in any manner, form or media, any of the Technology, Intellectual Property Rights or Marks of the other party are granted. Nothing contained in these Terms and Conditions

will be construed as constituting a transfer or an assignment to a party by the other party of any of the Technology, Intellectual Property Rights or Marks of such other party or any of its Affiliates.

**Governmental Authority.** Participating Provider shall promptly notify Access Partner if it is notified by any domestic or foreign, federal, state, provincial, municipal or local government, any political subdivision thereof or any entity exercising executive, legislative, judicial, regulatory, or administrative functions of or pertaining to government, regardless of form, including any agency, bureau, court, tribunal, or other instrumentality (“Governmental Authority”), or otherwise reasonably believes, upon advice of counsel, that it is not complying with any law applicable to Participating Provider due to the processes used by Apple, Access Partner or Participating Provider, for use and provisioning of Credentials using the Apple Access Platform.

**Confidentiality.** Participating Provider will protect Apple Confidential Information obtained pursuant to these Terms and Conditions from unauthorized dissemination and use with the same degree of care that it uses to protect its own like information. Apple will protect Participating Provider Confidential Information obtained pursuant to the Program from unauthorized dissemination and use with the same degree of care that it uses to protect its own like information. Except as expressly set forth herein, Participating Provider will not use the Apple Confidential Information for purposes other than those necessary to directly further the purposes of these Terms and Conditions. Except as expressly permitted under these Terms and Conditions, Participating Provider will not disclose to third parties the Apple Confidential Information without the prior written consent of Apple, including (i) the public disclosure of any metrics related to the Program and (ii) Participating Provider’s planned participation in the Program prior to the public launch of Participating Provider’s participation in the Program.

**Termination.** Apple may suspend or terminate Participating Provider’s participation in the Program in the event of Participating Provider’s breach of any of these terms and such breach is not remedied within thirty (30) days of receiving written notice of such breach by Apple. Participating Provider also acknowledges and agrees that any violation of the requirements set forth in these terms will be grounds for Apple to suspend the provisioning of Credentials to Enabled Devices.

#### **Data Privacy and Security.**

1. Participating Provider and Apple acknowledge that any information which directly or indirectly identifies individuals (“Personal Data”) collected, accessed, processed, maintained, stored, transferred, disclosed, or used in relation to these terms, shall be done for each party’s own benefit and not on behalf of the other party, and each party shall be independently and separately responsible for its own relevant activities. Participating Provider and Apple further acknowledge that Apple does not determine the purpose and means of the processing of Personal Data subject to these Terms and Conditions by Participating Provider, which is determined by Participating Provider solely in its own independent capacity. Participating Provider and Apple acknowledge and agree that the Access Partner is processing Personal Data in relation to the Program for the benefit of the Participating Provider as its data processor.
2. Solely in its own independent capacity and commitment to the protection of Personal Data, Participating Provider shall comply with **Exhibit B (“Apple Data Privacy and Information Security Terms”)** and all applicable data protection laws (altogether, “Data Protection Laws”), including entering into data processing agreements as may be required with Access Partner and, where necessary, ensuring that international data transfers take place only in compliance with the conditions laid down in Data Protection Laws (for example, by executing approved standard contractual clauses). Participating Provider must also ensure that its Service Providers are bound by the same privacy and security obligations as Participating Provider under these Terms and Conditions and will comply with the Data Protection Laws which shall continue to apply regardless of the location of processing of the data for which Participating Provider acts as data controller. Apple will comply with all Data Protection Laws with respect to the handling and use of Personal Data.
3. Participating Provider will promptly notify Access Partner and Apple if it (i) discovers that any person or entity has breached security measures relating to the Program, or gained unauthorized access to any

data related to the Program, including Participating Provider Data, Access Partner Data, or Access Partner Provisioning Data, (in each such case an “**Information Security Breach**”) or (ii) receives a written supervisory communication, written guidance or written direction from a Governmental Authority that requires a modification to or suspension of the provisioning of Credentials on Enabled Devices. Upon discovery of an Information Security Breach for which Participating Provider is responsible, the Participating Provider will, at its cost, (A) appropriately investigate, remediate, and mitigate the effects of the Information Security Breach and (B) provide Access Partner and Apple with assurances reasonably satisfactory to such parties that appropriate measures have been taken to prevent such Information Security Breach from recurring.

**Unauthorized Transactions.** Participating Provider acknowledges and agrees that Apple will not be liable to any party for any Transaction initiated by a person or party who is not authorized to make a Transaction on an Account, including without limitation any fraudulent Transaction.

**Parity with Physical Access Credential and other Access Services.** Participating Provider may not process or decline Transactions, or activate, suspend or cancel Credentials or Accounts, in a manner that discriminates against the Program compared to physical access credentials and Non-Apple Access Services.

**Reporting Data.** Participating Provider agrees to provide Apple (via Access Partner) the data and statistics identified in **Exhibit A (Reporting)** and in accordance with the Apple Access Guidelines (the “**Reports**”). Apple may use the data and statistics provided by Participating Provider for purposes of (1) performing its obligations and exercising its rights under these Terms and Conditions, or (2) improving the Apple Pay Technology and other Apple Products or technology used internally by Apple in connection with Apple Products.

**Pass Data.** Participating Provider expressly agrees to provide User Personal Data directly to Enabled Devices to support in the creation of representations of Credentials in accordance with Apple Access Guidelines and according to the User’s preferences to the extent such provision is allowed under applicable Law.

**Third Party Beneficiaries.** Apple shall be entitled to rely upon, shall be an express third party beneficiary of, and shall be entitled to enforce, the provisions of these Terms and Conditions. The parties hereto agree that Apple shall be an express third-party beneficiary of these Terms and Conditions as provided herein.

## **Exhibit A**

### **Data to be included in Reports**

The following reporting data must be collected by Access Partner (when acting as Credential Manager) and provided to Apple over an STFP that is hosted by such Access Partner. A report must contain aggregated data at the Participating Provider level.

All reporting metrics must be sent on a Daily, Weekly, and Monthly cadence.

#### **The following will be provided by Access Partner:**

##### **C. Ever Provisioned - Apple Access**

- 1) By Enabled Device type (i.e. iPhone and Apple Watch)
- 2) By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)

##### **D. Live Credential - Apple Access**

- 1) By Enabled Device type (i.e. iPhone and Apple Watch)
- 2) By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)

**Access Partner will provide the following data to Apple upon request, on a monthly or quarterly basis:**

F. Transaction - Apple Access

- 1) By Enabled Device type (i.e. iPhone and Apple Watch)
- 2) Optional, if available: By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)
- 3) By Transaction type (i.e. Door Access, Event)

G. Ever Provisioned – Other

- 1) Other Mobile Wallets
- 2) Physical/Plastic Cards

H. Live Credential – Other

- 1) Other Mobile Wallets
- 2) Physical/Plastic Cards

I. Transaction – Other

- 1) Other Mobile Wallets
  - i. By Transaction type (i.e. Door Access, Event,)
  - ii. By Transaction Status (i.e. Successful/Declines)
- 2) Physical Cards
  - i. By Transaction type (i.e. Door Access, Event,)
  - ii. By Transaction Status (i.e. Successful/Declines)

J. Total Enabled Users

- 1) By Device type (i.e. iPhone and Apple Watch)
- 2) By Credential type (i.e. full-time employee, contractor, part-time employee, intern, etc.)

Access Partner will provide the following data to Apple at the time of Participating Provider launch:

B. Total Eligible Users

- 1) By OS type (i.e. iOS, Android)

*\*“Live Credentials” means Credentials that have been provisioned and are “live” on a device*

*\*\* “Enabled User” means individuals using an iPhone or Apple watch within a Participating Provider Property*



## Exhibit B

### Apple Data Privacy and Information Security Terms

Unless otherwise defined, capitalized terms will have the same meaning as such terms in the Terms and Conditions. In the event of a conflict between this Exhibit B and the Terms and Conditions, this Exhibit B will control only with regard to the subject matter addressed in this Exhibit B.

Depending on the location of the use of the Provisioned Credential, “Apple” means Apple Inc., located at One Apple Park Way, Cupertino, California, for users in the United States, including Puerto Rico; Apple Canada Inc., located at 120 Bremner Blvd., Suite 1600, Toronto ON M5J 0A8, Canada for users in Canada; Apple Services LATAM LLC, located at 1 Alhambra Plaza, Ste 700 Coral Gables, Florida, for users in Mexico, Central or South America, or any Caribbean country or territory (excluding Puerto Rico); iTunes K.K., located at Roppongi Hills, 6-10-1 Roppongi, Minato-ku, Tokyo 106-6140, Tokyo for users in Japan; Apple Pty Limited, located at Level 3, 20 Martin Place, Sydney NSW 2000, Australia, for users in Australia or New Zealand, including in any of their territories or affiliated jurisdictions; and Apple Distribution International Ltd., located at Hollyhill Industrial Estate, Hollyhill, Cork, Republic of Ireland, for all other users.

Participating Provider confirms that this Exhibit B sets out its information security commitments regarding the handling of Personal Data by Participating Provider.

#### 1. Protection of Personal Data.

To the extent that the Participating Provider (and Participating Provider’s personnel, affiliates, employees, agents, contractors or subcontractors (“Provider Personnel”)) may process certain information that identifies, relates to, is linked to or is capable of being linked to individuals (“Personal Data”) in relation to the operation of the Terms and Conditions, the Participating Provider, undertakes in its own independent capacity, that such Personal Data will be collected, accessed, processed, maintained, stored, transferred, disclosed or used by it and its Provider Personnel for the Participating Provider’s own benefit in connection with the performance of its obligations under the Terms and Conditions and not on behalf of Apple.

Participating Provider undertakes solely in its own independent capacity to (and will procure that all Provider Personnel): (i) comply with all applicable Laws, regulations and international accords or treaties pertaining to Personal Data; and (ii) take all appropriate legal, organizational and technical measures to protect against unlawful and unauthorized processing of Personal Data.

Participating Provider shall be liable for the damage caused to any Data Subject as a result of Participating Provider’s or Provider Personnel’s handling of Personal Data in connection with the Terms and Conditions, including (without limitation) where Participating Provider or Provider Personnel has not complied with its commitments under this Exhibit B or any applicable Laws, regulations and international accords or treaties pertaining to Personal Data.

#### 2. Data Security Procedures.

Participating Provider undertakes solely in its own independent capacity to (and will procure that all Provider Personnel will) maintain reasonable operating standards and security procedures, and shall use their best efforts to secure Personal Data and Confidential Information (collectively, “Confidential Data”) through the use of reasonable and appropriate administrative, physical, and technical safeguards including, but not limited to, appropriate network security and encryption technologies governed by an established set of policies and procedures (an “Information Security Management System”). Participating Provider shall maintain and regularly update the Information Security Management System based upon a formal change control process that governs how security controls are adjusted over time ensuring at all times that it maintains a comparable or better level of security than that defined in this Exhibit B. Such Information Security Management System shall: (A) ensure the ongoing confidentiality, integrity, availability, and resilience of Participating Provider

systems and services processing Confidential Data and those of subcontractors that have been authorized by Apple to process Confidential Data; (B) enable Participating Provider to restore the availability and access to Confidential Data in a timely manner in the event of a physical or technical incident; (C) maintain a process for regularly testing, assessing, and evaluating the effectiveness of all technical and organizational measures for ensuring the security of Confidential Data at all times; and (D) shall also include the following:

- (i) Implementation of controls to manage access to Confidential Data, including:
  - (a) Preventing access to Confidential Data other than by those Provider Personnel that must access Confidential Data to perform Participating Provider's obligations under the Terms and Conditions (hereinafter, the "Services");
  - (b) Immediately terminating access privileges to Confidential Data for any Provider Personnel that no longer need such access, and conducting regular reviews of access lists in accordance with high industry standards to ensure that access privileges have been appropriately provisioned and terminated;
  - (c) Requiring Provider Personnel the use of multi-factor authentication to access Confidential Data; and
  - (d) Providing regular training on data security to all Provider Personnel that may have access to Confidential Data;
- (ii) Maintenance of firewalls to segregate Participating Provider's internal networks from the Internet, implementation of reasonable and appropriate network segmentation, and employing appropriate intrusion detection, prevention, monitoring, and logging capabilities to enable detecting and responding to potential security breach attempts as well as data loss resulting from malicious acts;
- (iii) Conducting regular vulnerability assessments encompassing every system or network in which Confidential Data is collected, stored, transited, or otherwise processed, or from which it may be accessed;
- (iv) To the extent that Participating Provider develops or uses applications in connection with Services, Participating Provider undertakes solely in its own independent capacity to perform security testing in accordance with industry standards for secure software development, including, in the case of web-based applications, to ensure that the application or application code is secure against the vulnerabilities described in (i) the version of the OWASP Top Ten List available as of the Effective Date of the Terms and Conditions and (ii) any changes to the OWASP Top Ten List after the Effective Date of the Terms and Conditions (within a reasonable time after such changes are initially published). The term "OWASP Top Ten List" shall mean the Open Web Application Security Project's Top Ten list (currently available at <https://www.owasp.org/www-project-top-ten/>);
- (v) Application of all manufacturer-recommended security updates to, and the use of manufacturer-supported versions (and, for the avoidance of doubt, no software that is past its "end of life") of all software on, all systems, devices, or applications collecting, storing, processing, or transiting Confidential Data in a timely manner. In the case of security patches or updates that are classified by their manufacturer or otherwise as "critical," or are associated with a vulnerability with a CVSS score of 9.0 or higher in the National Institute of Standards and Technology's National Vulnerability Database, such patches or updates shall be applied as soon as practical, but no later than thirty (30) days after release for systems that are not exposed to the public Internet, or seventy-two (72) hours for systems that are exposed to the public Internet. Provider shall apply those security patches or updates that are associated with a CVSS score of 7.0 or higher, or that are classified as "high" risk, promptly and no later than ninety (90) days from date of release;
- (vi) Maintenance and enforcement of policies and procedures to ensure that all of the following requirements are met:
  - (a) up-to-date virus protection software shall be installed on all computer systems attached to Participating Provider's networks and/or the networks of any subcontractor Provider Personnel;

- (b) access to Participating Provider’s computer resources and networks (including wireless networking and remote access) and those of any subcontractor Provider Personnel shall be limited to configurations approved by the Participating Provider utilizing appropriate authentication and authorization methods, including reasonable minimum password requirements, of sufficient length and complexity in accordance with industry standards, which shall be automatically enforced by the operating system used by Participating Provider;
- (c) the operating system shall enable a dictionary check to reject commonly used passwords, or Participating Provider shall regularly conduct password audits using tools designed to identify guessable or crackable passwords, and shall lock out the user account after failed authentication attempts, in accordance with industry standards;
- (d) Participating Provider shall prevent the use of shared credentials (any credentials that are shared between multiple users) to access Confidential Data except for a limited set of system admin account credentials (the “SysAdmin Accounts”) that are regularly changed in accordance with high industry standards and any use of the SysAdmin Accounts to access Confidential Data shall be irrevocably logged with the ability to identify Provider Personnel using any such SysAdmin Account;
- (e) Participating Provider shall remain current with industry standards pertaining to digital identity guidelines implementing new measures, as appropriate, from time to time, such as the National Institute of Standards and Technology (NIST) Digital Identity Guidelines (SP 800-63-3), or the successor thereto;
- (f) Confidential Data, other than traditional contact information of Apple personnel that is shared with Participating Provider for day-to-day business operations such as name, email address, phone number, and other similar contact information, shall at all times be encrypted in accordance with the Encryption Standards described below, regardless of whether such Confidential Data is at rest or in transit;
- (g) all encryption shall be accomplished with strong, modern cryptographic algorithms and ciphers employing robust integrity protection mechanisms and in accordance with industry standards for secure key and protocol negotiation and key management (collectively, the “Encryption Standards”);
- (h) without limitation to the terms of this Section 2, Participating Provider shall manage in a secure manner in accordance with high industry standards any mobile devices that are used to collect, transmit, store, or otherwise process Confidential Data, including by ensuring that: (i) Confidential Data stored on any such devices can be remotely wiped by Participating Provider; (ii) Confidential Data stored on any such devices is encrypted in accordance with the terms of subsection (g); (iii) the location of each such device can be remotely determined by Participating Provider; and (iv) Participating Provider maintains an up-to-date inventory of all such devices (devices meeting such requirements “Secure Mobile Devices”).
- (i) Confidential Data shall only be stored on any portable storage device or media, not Secure Mobile Devices, including but not limited to flash drives or other removable media (collectively, “Portable Storage Devices”), solely if authorized by Apple as necessary for the purposes of performing Participating Provider’s obligations under the Terms and Conditions, and shall be encrypted at all times in accordance with the terms of subsection (g) with a record of all such Portable Storage Devices including, to the extent possible, a detailed summary of the Confidential Data on any such Portable Storage Device maintained in an up-to-date inventory subject to regular review in accordance with ISO/IEC 27001:2013 or any successors thereto;
- (j) to the extent that Participating Provider provides hosted applications or services to Apple, whether single-tenant or multi-tenant, including software-as-a-service, platform-as-a-service, infrastructure-as-a-service, and similar offerings, (collectively, “Cloud-based Services”) to collect, transmit, store, or otherwise process Confidential Data, Participating Provider shall provide Apple the ability: (i) to isolate such Confidential Data logically from the data of Participating Provider’s other customers; (ii) to restrict, log, and monitor access to such Confidential Data at any time including access by Provider Personnel; (iii) to create, enable, disable, and delete the uppermost encryption key (the “Customer Managed Key”) used to encrypt and decrypt subsequent keys including the lowermost data encryption key; and (iv) to restrict, log, and monitor

access to the Customer Managed Key at any time; and at no time shall any subsequent encryption key, an encryption key in a key hierarchy lower than the Customer Managed Key, be stored in the same system as Confidential Data unless encrypted by the Customer Managed Key, also known as being wrapped by the Customer Managed Key;

(k) all documents and electronic media containing Confidential Data shall at all times be protected in accordance with Participating Provider's obligations of confidentiality of the Terms and Conditions, and if disposal is permitted by the Terms and Conditions, shall be disposed of in a secure and final manner in accordance with the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization (SP 800-88 rev. 1) or ISO/IEC 27040:2015 Information technology — Security techniques — Storage security, or any successors thereto ("Deletion Requirements");

(l) without limitation to Participating Provider's obligation to transmit Confidential Data only in encrypted form, Participating Provider shall ensure that any identities used for electronic communication (e.g. email addresses) are wholly owned by Participating Provider. Participating Provider shall ensure that any domains that it uses to identify itself are adequately protected to prevent impersonation. Provider Personnel shall not use personal email addresses or public email services (e.g. Gmail, Yahoo, Hotmail) to transmit Confidential Data or to communicate with Apple; and

(m) if reasonably requested by Apple at any time during Participating Provider's participation in the Program, Participating Provider shall provide Apple with a copy of the then-current Information Security Management System policies and procedures maintained by Participating Provider.

#### 1. Information Security Breach.

Participating Provider shall promptly (or in any case within 48 hours) notify Apple if Participating Provider knows or has reason to believe there has been any misuse, compromise, loss, or unauthorized disclosure or acquisition of, or access to, Confidential Data (an "Information Security Breach"). Upon any discovery of an Information Security Breach, Participating Provider will investigate, remediate, and mitigate the effects of the Information Security Breach. To the extent the Information Security Breach relates to Apple's Confidential Information, Participating Provider will reasonably cooperate with Apple in connection with each of the foregoing and will comply with any reasonable instructions provided by Apple in connection therewith. Without limitation to the foregoing sentence, in the event that Apple reasonably determines that a third-party security assessment is recommended in connection with an Information Security Breach, Participating Provider will engage a third-party security assessor to conduct such an assessment. Participating Provider shall provide any information related to any such Information Security Breach requested by Apple, including but not limited to, vulnerabilities or flaws, start or end date, date of discovery, and specific actions taken to contain and/or mitigate. If any Information Security Breach occurs as a result of an act or omission of Participating Provider or Participating Provider's Personnel, Participating Provider will, at Participating Provider's sole expense, undertake remedial measures (including notice, credit monitoring services, fraud insurance and the establishment of a call center to respond to customer inquiries).

#### 4. Assistance.

Participating Provider shall provide Apple with reasonable assistance and support where there is a question in relation to a matter that is the responsibility of Apple in its capacity as a separate party, in (i) responding to an investigation or cooperation request by a data protection regulator or similar authority; (ii) providing notice of an Information Security Breach to any third party where required or requested by Apple; (iii) conducting legally required privacy, security, or data protection impact assessments; and (iv) consulting with the relevant authorities when required in relation to such impact assessments.

#### 5. Return or Destruction of Apple Confidential Information.

Upon termination of Participating Provider's participation in the Program for any reason, Participating Provider shall promptly contact Apple for instructions regarding the return, destruction, or other appropriate

action with regard to Apple Confidential Information. Unless otherwise instructed by Apple upon termination Participating Provider's participation in the Program for any reason, or at any time at the request of Apple, Participating Provider: (i) return all Apple Confidential Information to Apple including but not limited to all paper and electronic files, materials, documentation, notes, plans, drawings, and all copies thereof, and ensure that all electronic copies of such Apple Confidential Information are deleted from Participating Provider (and where applicable, its subcontractors') systems; or (ii) if requested by Apple in writing, or remaining on Participating Provider systems following the return of Apple Confidential Information set forth above, promptly destroy all instances of Apple Confidential Information; and for the avoidance of doubt, Apple Confidential Information shall be destroyed in accordance with the Deletion Requirements including Apple Confidential Information on any media used for backup, disaster recovery, and/or business continuity purposes. If requested by Apple, Participating Provider shall provide Apple with written confirmation of its compliance with the requirements of this section.

6. Third Parties including Subcontractors and Provider Personnel.

Participating Provider may only disclose Confidential Data to third parties (including Provider Personnel) who have a need to know that Confidential Data in order to perform the Services and have signed agreements that require them to protect Confidential Data in the same manner as detailed herein. Participating Provider shall not engage any third party to perform any portion of the Services if such party may obtain or otherwise process Apple's Confidential Information, without Apple's prior written consent. Notwithstanding such consent, Participating Provider any shall not be relieved of any obligations under this Exhibit B and shall remain solely liable if any Provider Personnel or other third party fails to fulfil its obligations with respect to Confidential Data.

7. Notification of Non-Compliance.

Without limitation to Participating Provider's obligations under this Exhibit B, and without prejudice to any other rights or remedies available to Apple, if Participating Provider is unable to comply with its commitments stated in this Exhibit B, Participating Provider shall promptly notify Apple, and Apple may immediately terminate Participating Provider's participation in the Program.

## Exhibit C

### Apple Marks

The following is a non-exhaustive list of Apple Marks for use in the Program:

Apple
Apple logo
Apple Pay
Apple Pay logo
Apple Watch (including rights to display images of the Apple Watch)
iPhone (including rights to display images of the iPhone device, but only those models that are technologically capable of being an Enabled Device)
Touch ID
Face ID
App Store
iCloud
Wallet
Apple Wallet

Complete list of Apple Marks and guidelines set out at <https://www.apple.com/legal/intellectual-property/trademark/appletmlist.html>

**Exhibit K**

**Participating Providers**

Any Participating Providers to be activated after the Program Launch Date will be added to this Exhibit H.

<u>Participating Provider</u>	<u>Territory</u>	<u>Company Registration Number</u>	<u>Registered Address</u>	<u>Contact Person</u>

This Exhibit K may be amended by the mutual consent of the Parties in writing (including email) from time to time.

## **Exhibit L**

### **Access Partner Marks**

The following is a non-exhaustive list of Access Partner Marks:



## Exhibit M

### Terminal/Reader Procurement

Apple requires six (6) readers (or fewer, at Apple's sole discretion) for every reader model used in the Program with Participating Provider. Readers will be provided at a zero-dollar cost and may continue to be used throughout the scope of the project.

#### Reader Attributes

Readers must be set up with appropriate mode, system, and configuration by Access Partner prior to shipping.

A comprehensive list of in-scope readers for each system must be provided to Apple for managing test cases and ensuring accurate terminal tracking/management.

For the avoidance of doubt, a terminal is the reader that processes the credentials and any minimal processing capability required to drive it.

#### Number of Readers

Six (6) readers per system as it pertains to the project must be provided to Apple for Testing.

Three (3) readers must be configured in QA and three (3) must be configured in Production.

#### Reader Cost

Readers must be provided at no-cost.

A zero-dollar quote must be provided to Apple for any hardware shipped at a given time.

#### Maintenance & Support

Ongoing terminal support will be required. There should be no cost for reasonable support and Access Partner must identify a contact who can support engineering with setup, troubleshooting, and updating terminals throughout the scope of the project.

Access Partner must acknowledge an engineering support request within 2 hours. Monday through Friday from 08:00PST to 18:00PST. Special arrangements may be made by mutual agreement.

#### Reader Ownership Term

Terminals will remain with Apple for the duration of the project. After the project is executed, terminals may be returned.

#### Reader Security

Terminals will be stored in a secure lock-down environment on Apple's campus.

#### Reader Shipping

The Business Operations Team will manage distribution across Apple Engineering teams. Shipping address should be as follows, unless another address is provided prior to shipping by Apple:

Apple Inc.  
Attn: IOT Team  
C/O: Vignesh Muralidharan  
9779 Towne Center Drive  
San Diego, California, 92121  
United States

## Exhibit N

### Marketing Commitment

Access Partner marketing commitments are described in this **Exhibit N**.

Within 90 days of the Effective Date, Access Partner and Apple will use reasonable efforts to agree to a marketing plan for promotion of the Program and the onboarding of Participating Providers and, if applicable, additional Access Service Partners. The marketing plan will be focused on driving user adoption and usage of Provisioned Credentials.

All promotions must receive prior approval from Apple before being counted against the marketing commitment and Apple will communicate to Access Partner, within a commercially reasonable period of time, Apple's decision of whether it provides such approval.

The Parties intend to work together on a variety of marketing and sales initiatives to demonstrate Apple Access Technology, to build a business pipeline, all with the goal of driving adoption and sales for Apple Access Technology and Access Partner's NFC solution including:

#### Sales Personnel

Access Partner will hire and deploy its sales personnel to execute on the implementation, and sale or licensing of the Apple Access Technology ("Apple Wallet Pass Sales Specialists"). Access Partner will provide training support for its Apple Wallet Pass Sales Specialists throughout each of its approved territories. Access Partner's sales team will include end-user representatives, electronics sales representatives, and architectural and engineering specification writers to educate multiple customer stakeholders of the value and benefits of the Apple Access Technology. Each electronics sales representative and integrator sales representative will be trained in the sale and licensing of the Apple Access Technology at each of Access Partner's sales offices within approved territories and will benefit from Access Partner's sales incentives.

#### Client Briefings

Access Partner will conduct client briefings on an agreed schedule at Access Partner's facilities and at other agreed physical and virtual locations.

#### Company Events and Conferences

Access Partner will provide Apple with mutually agreed space for Apple to exhibit at all mutually agreed conferences where Apple and Access Partner have agreed to go-to-market as identified in the Business Plan. At each such identified Access Partner conferences, (i) Access Partner will provide space to Apple at no cost to Apple, and (ii) Apple's space will be of similar square footage and location as other like companies, if Apple provides Access Partner notice of its intent to attend at least three months prior to the date of the event.

#### Demand Generation Initiatives

Access Partner will promote and present webinars and run email, social media, and call campaigns regarding the Apple Access Technology. Access Partner will execute four (4) campaigns per year (i.e.: one (1) per calendar quarter).

#### Apple Access Technology Offers

Access Partner will work with Apple to develop and launch mutually agreed special offerings directed toward users of the Apple Access Technology targeting a mutually-identified business market (the “Offering”). Access Partner at its own cost will execute the Offering 2 (two) times per calendar year.

#### Thought Leadership

In support of the Apple Access Technology, Access Partner will create and produce mutually agreed “thoughtware” (for example, such thoughtware may include infographics, white papers, slide decks, and presentations), that describes how to implement Apple Access Technology. Including thoughtware featuring an analysis of the business outcomes for Participating Providers and methods to optimize the total return on investment of Apple Access Technology with Access Partner’s NFC solution.

#### Customer Marketing Support

Access Partner will work directly with customers to support marketing programs. All marketing materials must comply with the app unless Apple provides prior written approval to use with 90 days of execution of this agreement.