API and Platform License Agreement

This API and Platform License Agreement ("API and Platform Agreement") contains the terms and conditions that govern your and if applicable, any Purchaser's (collectively, "Client"), right to use Onbe, Inc. and its affiliates' (collectively, "Company") application programming interfaces and related information and documentation as it currently exists (collectively, the "API") and to use and access one or more of Company's online platforms or portals, including but not limited to ClientZone, Client Portal, Digital Portal, PromoCode Admin, OMSI, MyPaymentVault, and Onbe Enterprise Portal (together with the services available therein, the "Platform"). This API and Platform Agreement is subject to Client's negotiated agreement with Company ("Agreement"). Unless otherwise defined in the Agreement, "Purchaser" means a customer that requests a physical card, virtual card or other payment modalities or program management services from Company (inclusive of clients of Client, clients of Client's clients and so on (e.g., any reseller that may be nested, double-nested, etc.). Client is fully responsible for Purchaser compliance with this API and Platform Agreement. Company shall have no liability to Purchaser resulting from or related to this API and Platform Agreement.

1. License. Subject to Client's continued compliance with the terms of this API and Platform Agreement, including the guidelines set forth in Section 6, Company grants Client a personal, non-exclusive, revocable, non-transferable and non-sublicensable license to use (i) the API and (ii) Company's Platform and all information, data, text, software, music, sound, photographs, graphics, video, messages, or other material or content displayed, used, or otherwise incorporated into the Platform ("Content") for its intended purpose. If applicable, Client must review and accept Company's terms and conditions, as may be updated from time to time prior to accessing and using the API or Platform. Client's personnel that access the API or Platform are referred to herein as "End Users". Client shall be responsible for the acts and omissions of End Users hereunder. Company may change Client's method of accessing the API or Platform at any time, in Company's sole discretion, and Client shall be responsible, at its sole cost, for procuring all connectivity, equipment and software needed to access the API or Platform. Client acknowledges and agrees that Company may limit, update, modify, or cease support of current or prior versions or releases of the API or the Platform at any time, in its sole discretion, without liability.

2. Content. All Content other than Content submitted to the API or Platform by Client ("Client Content") is owned by Company or its third party licensors and vendors and is protected by applicable copyright, trademark, and/or other intellectual property laws. Nothing contained in this API and Platform Agreement or on the API or Platform should be construed as granting any license or right to use any of the Content without Company's written permission other than as set forth herein. Any use of the any name, logo, and registered and common law trademark and service mark (collectively, "Marks") included in the Content will inure to Company's (or its applicable licensor's) benefit.

3. Client Content. Client owns the Client Content. By submitting Client Content, Client (a) represents and warrants that it has all right, title, and interest to do so and (b) grants Company and its Affiliates a non-exclusive, worldwide, transferable and sublicensable license to use, reproduce, display, perform, modify, transmit, distribute and create derivative works of Client Content in connection with Company's provision of services to Client. Company has the right, but no obligation, to monitor or screen Client Content and remove any Client Content in its sole discretion.

4. Accounts. End Users may be required to create a user account to access the API or Platform. Client is responsible for ensuring its End Users provide complete and accurate information, and for any liability or damages arising from fraudulent or inaccurate information. Accounts and login credentials may not be shared between End Users or transferred from one End User to another. Client is responsible for (a) maintaining the security of its accounts and login credentials and (b) any actions taken using its or its End Users' account credentials. Company shall not be liable for any claims arising from the fraudulent or unauthorized use of the API or Platform by End Users.

5. Use; Termination of Access. The API and Platform are provided on an "as is" and "as available" basis. Client shall (a) notify Company of each End User (or any change thereto), (b) educate each End User about the initiation, implementation and maintenance of a Program using materials, procedures and information provided by or approved in advance in writing by Company, (c) notify Company immediately upon termination of an End User's employment or termination of such person's duties as an End User of the API or Platform and (d) maintain commercially reasonable administrative and technical measures designed to protect against any unauthorized access to or use of the API or Platform. Company may (a) modify or discontinue the API or Platform without notice and (b) terminate or suspend any End User account at any time without liability. Termination of an End User account will not relieve either party from any obligations incurred or arising prior to such termination.

6. Guidelines. With respect to the API, Platform and any Content, Client will not, and will ensure its End Users do not (a) reproduce, modify, distribute, license, sell, create derivative works based upon, or in any way commercially exploit the API, Platform or Content; (b) use manual or automated means to trawl, mine, scrape, frame, or mirror; (c) disassemble, decompile or reverse engineer, or otherwise attempt to discern the source code or interface protocols of the API or the Platform; (d) attempt to hack, defeat, or overcome any encryption technology or security measures, or gain any unauthorized access; (e) interfere with or disrupt operations; (f) promote illegal activity or violate applicable law; (g) post or transmit any Content that is discriminatory, defamatory, abusive, harassing, threatening, pornographic or otherwise inappropriate or infringes any intellectual property or privacy or other rights of any person; (h) send unsolicited advertisements; (i) impersonate any person or misrepresent its identity or affiliation; (j) use the API or Platform in a way that is not for its intended purposes, that is in violation of any applicable law or

regulation or that will adversely affect Company; (k) provide any information that it does not have the right to provide; (l) assign, share, pledge, resell, distribute, or sublicense the API or Platform; (m) share identification or password codes with persons other than End Users, or permit Client's account to be accessed by individuals who are not End Users; (n) introduce into the API or Platform any software, virus, worm, "back door," Trojan Horse, or similar malicious, harmful or disabling code; (o) remove or modify any proprietary marking or restrictive legends placed on the API or Platform, including without limitation any Marks or (p) otherwise violate any of Company's published rules, policies, or guidelines. Company will not be responsible for any loss or damage resulting from use of the API, Platform, Content or conduct of any third parties. Company shall be permitted to monitor Client's usage of the API and Platform to verify compliance with the terms of this API and Platform Agreement, and Client shall permit Company, upon request, to conduct an audit to verify the same, and shall reasonably cooperate with Company with respect to any such audit. Notwithstanding anything to the contrary herein, Company may, in its sole discretion, immediately revoke the grant of rights contemplated in Section 1 if Client breaches or threatens to breach the guidelines in this Section or creates other security or legal concerns. Client hereby agrees that Company will be entitled, in addition to any other remedies available to it at law or in equity, to injunctive relief to prevent the breach or threatened breach of Client's obligations under this Section, without any requirement to demonstrate irreparable harm or post a bond.

7. Feedback. If Client provides feedback, suggestions, improvements, or requests for additional functionality related to the API or Platform (collectively, "Feedback"), Client grants Company a perpetual, irrevocable, royalty-free, worldwide license to use, reproduce, display, perform, modify, transmit, distribute, and create derivative works of such Feedback in any way Company deems reasonable, without any attribution or accounting. This paragraph will survive any termination or expiration of this API and Platform Agreement of Client's accounts on the API or Platform.

8. Representations and Warranties; Disclaimer.

a. Mutual Representations and Warranties. Each party represents and warrants to each other that: (i) it has the necessary corporate power and authority to enter into this API and Platform Agreement and to perform its obligations hereunder; (ii) it will comply with all applicable laws, statutes, ordinances, and regulations in connection with this API and Platform Agreement; and (iii) it has all necessary rights, consents and permissions to transfer any data to the other party via the API and Platform and such transfer is not in violation of its privacy policies or any applicable laws, and it will use any data transferred to it from the other party via the API or Platform in accordance with the terms of applicable data protection laws and contractual requirements.

b. Client Representations and Warranties. Client represents and warrants that (i) it has implemented or contractually required and industry-standard security measures to help protect the security and integrity of, and prevent, unauthorized access to the API and Platform; (ii) it will not do anything that will make the API or Platform subject to any open source or similar license; (iii) it will not disrupt, disable, erase, alter, harm, damage, interfere with or otherwise impair in any manner the API or Platform; (iv) subject to Section 13, if Company notifies Client that the API or Platform causes Client to be in receipt of information subject to Payment Card Industry Data Security Standards ("PCI DSS"), Client will obtain and maintain PCI DSS certification for the duration of the Agreement, or will cease use of the relevant API call or Platform functionality causing receipt of such information; (v) in the event of any security breach or unauthorized access to the API or Platform, Client will immediately investigate such breach and notify Company, and, unless otherwise informed by Company, take all corrective action necessary to remedy such breach, and perform such remediation (with all consumer notifications to be undertaken by Company), all at Client's cost; and (v) Client will comply with all applicable laws and not violate or infringe upon any third party intellectual property, privacy or publicity rights.

c. DISCLAIMERS; NO OTHER WARRANTIES. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 8(a), EACH PARTY HEREBY ACKNOWLEDGES AND AGREES THAT THE API, THE PLATFORM, THE MARKS, AND ANY OTHER MATERIALS, DATA OR SERVICES PROVIDED TO THE OTHER HEREUNDER, ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. EXCEPT AS EXPRESSLY SET FORTH IN SECTION 8(a), NEITHER PARTY MAKES ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT THERETO AND SHALL HAVE NO LIABILITY TO THE OTHER PARTY OR ANY OTHER PERSON OR ENTITY WITH RESPECT TO SAME. EACH PARTY SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ERROR-FREE OR UNINTERRUPTED OPERATION, NON-INFRINGEMENT, AND THOSE WARRANTIES ARISING FROM A COURSE OF PERFORMANCE, A COURSE OF DEALING OR TRADE USAGE. TO THE EXTENT THAT A PARTY MAY NOT AS A MATTER OF APPLICABLE LAW DISCLAIM ANY IMPLIED WARRANTY, THE SCOPE AND DURATION OF SUCH WARRANTY WILL BE THE MINIMUM PERMITTED UNDER SUCH LAW.

9. Indemnification.

   a. Indemnification by Company. Subject to Section 9(c), Company shall defend, hold harmless, and indemnify Client and its officers, directors, members, agents, employees, successors, and permitted assigns from and against any and all losses, liabilities, fines, penalties, damages, costs, and expenses, including reasonable outside attorneys' fees ("Losses") incurred by such parties in connection with any third-party claim, action, or proceeding ("Claim") arising from an allegation that the API, Platform or the Company Marks, as used by Client in accordance with this Agreement, infringe, violate, or misappropriate the United States intellectual property rights of any third party.

   b. Indemnification by Client. Client shall defend, hold harmless, and indemnify Company and its officers, directors, members, agents, employees, successors, and permitted assigns from and against any and all Losses incurred by such parties in connection with any Claim arising from: (i) Client's negligence or willful misconduct; (ii) Client's breach of this API and Platform Agreement or violation of law; (iii) the Client Marks or Client Content, including without limitation any allegation that any of the foregoing infringe, violate, or misappropriate the intellectual property rights of any third party or violate any data protection laws; and/or (iv) except to the extent covered by Company's indemnification obligations, Client's use of the API or Platform.

   c. Exclusions; Infringement Remedies. Company shall not be obligated to indemnify, defend, or hold harmless the indemnified party pursuant to Section 9(a) to the extent any such third-party Claim arises from: (i) Client's modification or misuse of the API or Platform; (ii) alteration of the API or Platform by Client without Company's prior, written consent; (iii) Client's use of the API or Platform in combination with apparatus, hardware, software, or services not authorized by Company; (iv) any use by Client of the API or Platform that violates this API and Platform Agreement or any applicable law or regulation of any governmental authority or self-regulatory agency or authority; (v) any Client Content or (vi) any use by Client of the API or Platform in a manner for which they were not designed. In the event that Company reasonably determines that the API or Platform is likely to be the subject of a claim of infringement or misappropriation of third-party rights, Company shall have the right (but not the obligation), at its own expense and option, to: (x) modify or replace the API or Platform to make it non-infringing with the same or similar functionality; (y) procure any rights from the third party necessary to provide the API or Platform; or (z) terminate providing the API or Platform. THIS SECTION 9 STATES CLIENT'S SOLE AND EXCLUSIVE REMEDY, AND COMPANY'S SOLE AND EXCLUSIVE LIABILITY, REGARDING THE API'S OR PLATFORM'S VIOLATION, INFRINGEMENT OR MISAPPROPRIATION OF ANY INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY.

   d. Indemnity Procedures. The indemnified party will give the indemnifying party prompt written notice of any claim as to which these indemnification provisions apply; provided, however, that any delay in notification shall not vitiate the indemnifying party's indemnification obligations unless the indemnifying party is materially prejudiced thereby. The indemnified party will reasonably cooperate with the indemnifying party and assist in the defense of such claim, at the indemnifying party's sole cost. The indemnifying party, at its own expense, will have the right to select competent counsel. Upon request of the indemnified party, the indemnifying party will allow counsel for the indemnified party, to observe (but not participate or control) the defense at the indemnified party's sole cost, and counsel for both parties shall cooperate with each other. The indemnifying party shall have the right to settle any indemnification claim, provided, however, that any settlement which requires an admission of guilt or any equitable remedies shall require the prior written consent of the indemnified party, such consent not to be unreasonably withheld or delayed.

10. Confidentiality. Client may be given access to certain non-public information, software, and specifications relating to the API or Platform ("Confidential Information"), which is confidential and proprietary to Company.

    a. Exceptions. Confidential Information does not include any information that: (a) was publicly known and made generally available in the public domain prior to the time the disclosing party disclosed the information to the receiving party, (b) became publicly known and made generally available, after disclosure to the receiving party by the disclosing party, through no wrongful action or inaction of the receiving party or others who were under confidentiality obligations, (c) was in the receiving party's possession, without confidentiality restrictions, at the time of disclosure by the disclosing party, as shown by the receiving party's files and records; or (d) is required to be disclosed by the receiving party by applicable law, rule, regulation or court order, provided that the receiving party gives the disclosing party prompt written notice of the required disclosure and cooperates with the disclosing party's attempt to limit the disclosure.

b. Nondisclosure and Non-use. The receiving party will not, during and after the term of this API and Platform Agreement, disclose the Confidential Information of the disclosing party to any third party or use such Confidential Information for any purpose other than as permitted under this API and Platform Agreement. The receiving party will take all reasonable precautions to prevent any unauthorized disclosure of the disclosing party's Confidential Information.

c. Permitted Disclosure. The receiving party may disclose the terms of this API and Platform Agreement to a third Party without disclosing party's consent (a) in confidence, to consultants, accountants, banks, investors, and actual or potential financing sources and their advisors; (b) in confidence, in connection with the enforcement of this API and Platform Agreement or rights under this API and Platform Agreement; (c) in confidence, in connection with a merger or acquisition or proposed merger or acquisition, or the like; or (d) in connection with the requirements of a securities filing.

11. Third Parties. The Platform may contain links and references to third-party websites and applications. Company may, from time to time, at its sole discretion, add or remove these links and references. Company is not responsible for, has no control over and does not endorse these third-party websites and applications. The applicable third party, not Company, is responsible for its acts and omissions and the quality of its offerings. Company is not responsible for the accuracy or reliability of any Content provided by third parties and will not be liable for any cause of action relating to such third party Content. Client is solely responsible for its interactions and transactions with any third parties.

12. General. The API and Platform and derivatives thereof may be subject to export laws and regulations of the United States and other jurisdictions. Client represents that it is not named on any U.S. government denied-party list. Client shall not permit End Users to access or use the API or Platform in a U.S. sanctioned country (currently Cuba, Iran, North Korea, Syria, or Crimea) as well as Belarus, Russia and Ukraine or in violation of any U.S. export law or regulation. This API and Platform Agreement may change from time to time. When Company makes changes to this Agreement, Company will update the "Last updated" date at the beginning of this API and Platform License Agreement. All changes will be effective from the date of publication unless otherwise stated. Use of the API or Platform after notice of such modifications constitutes acceptance of the modified terms.

13. Limited Support; PCI DSS. If specified in the applicable Program Agreement, Master Services or Reseller Agreement or other written agreement between the parties, the following terms apply:

a. Limited Support Terms; PCI DSS Compliance.

i. Limited Support. Company has notified Client that it is permitted to access additional API functionality for purposes of providing certain limited support directly to payment recipients. Client represents and warrants that it will comply with the terms of Exhibit A (Limited Support Terms) attached hereto.

ii. PCI DSS Compliance. The API or Platform limited support access will cause Client to be in receipt of information subject to PCI DSS. Therefore, Client must also have appropriate controls in place for its business to comply with PCI DSS. Client represents, warrants and covenants that at all times during this Agreement it has manual or automated controls in place to comply with PCI DSS, which may include but is not limited to (i) evidence of PCI Attestation of Compliance / Report on Compliance (AOC/ROC) performed by a Qualified Security Assessor (QSA) or (ii) ongoing approved scanning vendor (ASV) scans performed by a PCI DSS ASV.

b. Limited Support Terms; No PCI Information.

i. Limited Support. Company has notified Client that it is permitted to access additional API functionality for purposes of providing certain limited support directly to payment recipients. Client represents and warrants that it will comply with the terms of Exhibit A (Limited Support Terms) attached hereto.

ii. No PCI Information. Client has informed Company that it does not have manual or automated controls to comply with PCI DSS. As such, the API or Platform limited support access will **not** cause Client to be in receipt of information subject to PCI DSS. Client will inform Company immediately if Client believes it has access to information subject to PCI DSS. Client understands and agrees that if it desires the API or Platform to permit access to information subject to PCI DSS at any time during this Agreement, Client will ensure it has manual or automated controls in place to comply with PCI

DSS, which may include but is not limited to (i) evidence of PCI Attestation of Compliance / Report on Compliance (AOC/ROC) performed by a Qualified Security Assessor (QSA) or (ii) ongoing approved scanning vendor (ASV) scans performed by a PCI DSS ASV.

c. Use Restriction; No PCI Information. Client will not use the API or Platform to provide any sort of customer service or support directly to payment recipients. Client understands and agrees that if it desires to provide limited support, additional terms will apply. In addition, Client has informed Company that it does not have manual or automated controls to comply with PCI DSS. As such, the API or Platform limited support access will **not** cause Client to be in receipt of information subject to PCI DSS. Client will inform Company immediately if Client believes it has access to information subject to PCI DSS. Client understands and agrees that if it desires the API or Platform to permit access to information subject to PCI DSS at any time during this Agreement, Client will ensure it has manual or automated controls in place to comply with PCI DSS, which may include but is not limited to (i) evidence of PCI Attestation of Compliance / Report on Compliance (AOC/ROC) performed by a Qualified Security Assessor (QSA) or (ii) ongoing approved scanning vendor (ASV) scans performed by a PCI DSS ASV. Exhibit A to this API and Platform Agreement does not apply.

d. Use Restriction; PCI DSS Compliance.

i. Use Restriction. Client will not use the API or Platform to provide any sort of customer service or support directly to payment recipients and Exhibit A to this API and Platform Agreement does not apply.

ii. PCI DSS Compliance. The API or Platform limited support access will cause Client to be in receipt of information subject to PCI DSS. Therefore, Client must also have appropriate controls in place for its business to comply with PCI DSS. Client represents, warrants and covenants that at all times during this Agreement it has manual or automated controls in place to comply with PCI DSS, which may include but is not limited to (i) evidence of PCI Attestation of Compliance / Report on Compliance (AOC/ROC) performed by a Qualified Security Assessor (QSA) or (ii) ongoing approved scanning vendor (ASV) scans performed by a PCI DSS ASV.

Exhibit A

Limited Support Terms

These Limited Support Terms ("Support Terms") govern Client's use of Company's or its affiliates APIs or Platforms to provide support to Client's participating recipients of a payment ("Payment Recipients") regarding the relevant Client Program(s). These Support Terms are incorporated into and made a part of the API and Platform License Agreement which is subject to Client's negotiated agreement with Company ("Agreement").

1. Support Services. Company may permit Client to offer certain support services to Payment Recipients, which may be in the form of a physical card, virtual card or other payment modalities ("Payment Modalities") participating in one or more of Client's Programs (as further set forth below, the "Support Services"). Client understands Company is the primary customer service provider for Client's Program. For the avoidance of doubt, Support Services will not include access to a Payment Modality's full primary account number (PAN) or card verification value (CVV). Support Services specifically refer to the ability to provide one or more of the following services:

   - Activate, reissue, and/or suspend Payment Modalities.
   - View Payment Modality transaction history including merchant, merchant location, transaction date and time and transaction amount, available in limited circumstances as determined by Company in its sole discretion.
   - View Payment Modality real-time balance.
   - Provide Payment Modality balance information directly to Payment Recipients.
   - Resend Clickable Links or emails.
   - View Payment status.
   - View Physical Card shipping information.
   - Reporting of above items.

2. Payment Recipient Account Information. In its provision of services to Client, Company acts as an agent of the relevant issuing bank or non-bank money service business ("Issuing Bank") and may stores, processes and transmits information and materials, in any form or medium, related to a Payment Modality account, which may include, but is not limited to, a name, address, account number (any debit card number or other account number issued by Issuing Bank), account balance, transaction and purchase information, and payment history (collectively, "Payment Recipient Account Information") of a payment recipient (the "Payment Recipient").

   (a) Compliance Applicable Law. As such, Company is required to comply with applicable law, statute, regulation, order or other rule of law of any federal, state, provincial, local or foreign government, or any court of competent jurisdiction, in each case applicable to a party and applicable to the Issuing Bank ("Applicable Law"), including but not limited to regulations promulgated and administered by the Office of Foreign Assets Control of the U.S. Treasury Department (OFAC), including prohibiting its clients form engaging or processing any transaction (financial or otherwise) associated with a sanctioned country, in addition to the operating rules, policies and procedures of any payment network or the Issuing Bank (together with Applicable Law, the "Rules"). In providing the Support Services, Payment Recipient Account Information will be made available to or collected or access by Client. Therefore, Client must also have appropriate controls in place for its business to prevent individuals with IP address, email or phone numbers with country calling codes connected to comprehensively sanctioned countries from engaging in any activity that may directly or indirectly make use of Company's products or services. In addition, Client will comply, and will ensure that its directors, officers, employees, agents, contractors and any other personnel involved (directly or indirectly) in providing Support Services ("Personnel") comply, with the obligations set forth in Attachment A with respect to the Payment Recipient Account Information.

   (b) Computer Security Provisions. If Client maintains or accesses any confidential or proprietary information of Company or Payment Recipient Account Information on or from a website or web accessible system, Client will abide by the computer security provisions attached hereto as Attachment B.

3. Representations and Warranties. Client represents, warrants and covenants that it: (i) has all rights and authority required to provide the Support Services; (ii) has a manual or automated control to prevent customers with IP addresses, email addresses or phone number with country calling codes form comprehensively sanctioned countries from engaging in any activity that may directly or indirectly make use of Company's products or services, and any fourth parties that also contribute to Client's use of Company's products or services also have similar controls in place; (iii) the Support Services will be provided in a professional manner by qualified and skilled individuals with appropriate expertise and training, and in conformity with standards generally accepted in Client's industry and the financial services industry and (iv) will only avail itself of the

information obtained from its provision of the Support Services to actually provide such Support Services, and solely for the use cases and programs as preauthorized by Company in its discretion.

4. DAMAGES. ANY LIMITATIONS OF LIABILITY SET FORTH IN THE AGREEMENT WILL NOT APPLY TO ANY DAMAGES INCURRED BY COMPANY OR ISSUING BANK RELATED TO THE SUPPORT SERVICES TO THE EXTENT ARISING FROM: (A) THE GROSS NEGLIGENCE, BAD FAITH OR WILLFUL MISCONDUCT OF CLIENT OR CLIENT'S PERSONNEL; (B) PERSONAL INJURY, DEATH, OR PROPERTY DAMAGE CAUSED BY CLIENT OR ITS PERSONNEL; OR (C) A SECURITY INCIDENT. ADDITIONALLY, NO LIMITATION OF LIABILITY IN THE AGREEMENT WILL EXCLUDE ANY DAMAGES FOR CLAIMS TO THE EXTENT COVERED BY INSURANCE POLICIES WITH INSURERS WITH A MINIMUM A.M. BEST FINANCIAL STRENGTH RATING OF "A- (EXCELLENT)" OR BETTER, UP TO THE APPLICABLE MINIMUM COVERAGE AMOUNTS.

5. Subcontractors. Client will not use a subcontractor to perform the Support Services without obtaining Company's prior written approval. If Client is approved to utilize a subcontractor to perform the Support Services, Client must (i) enter into agreements with any such subcontractors to ensure that subcontractors are obligated to fully uphold and comply with the same obligations and responsibilities as Client under the Agreement. Client will remain fully responsible for all acts and omissions of its subcontractors. For the avoidance of doubt, the restrictions on subcontractors in this paragraph includes any performance of the Support Services by clients of Client, clients of Client's clients and so on.

6. Compliance. To the extent permitted by Applicable Law, Client agrees to promptly report to Company the commencement of any enforcement or other regulatory actions brought against Client related to its provision of the Support Services. If any change in Rule requires Company to adopt specific standards regarding its service providers which relate to the Support Services, then Client will make all modifications, at no charge, as are required to enable Company to comply with any changes in Rules or will have the option to cease providing the Support Services. Client will comply with all Rules as may be provided by Company from time to time with respect to the Support Services. Client shall not take any action that would cause Company or Issuing Bank to violate the Rules. Client acknowledges that Company and Issuing Bank are subject to regulatory oversight, and Client will promptly and fully cooperate with the requests of any regulator of Company or Issuing Bank.

7. Policies and Procedures.

   (a) General. Client will comply and will ensure that its Personnel comply with the following, as applicable to the Support Services: (i) Company's security and privacy policies (including without limitation its information security standards) and (ii) any Company policies provided to Client in writing which are applicable to the Support Services provided by Client.

   (b) Identity Theft Program. Client shall adopt an Identity Theft Prevention Program ("ITPP") designed to detect, prevent, and mitigate identity theft in connection with the Support Services. The ITPP shall at a minimum comply with the provisions of Applicable Law and the Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation set forth at Appendix J to 12 CFR Part 41.

   (c) Background Checks. Client shall obtain background checks prior to any Personnel accessing any Payment Recipient Account Information, and will not allow such Personnel such access if such background checks reveal any indictments, arrests, or convictions relating to fraud, financial crimes, or breach of trust.

8. Audits; Access to Information. Client will permit Company, the Issuing Bank or any regulatory authorities which have jurisdiction over Company or Issuing Bank, as applicable, to conduct an audit or request for information of Client solely related to the Support Services. Client will promptly provide, at any time requested by Company, any records kept in the ordinary course of business that pertain to the Support Services. Any audit or request must be preceded by reasonable notice to Client of at least 10 days (unless otherwise required by Applicable Law) and conducted during normal business hours. No more than annually, Client will provide Company with such information as Company may reasonably request to perform an annual due diligence review with respect to Client's provision of the Support Services. Client will disclose to Company if it maintains or in any manner stores on a website or web accessible system any Payment Recipient Account Information, and, if requested by Company but no more than annually, will cooperate with Company in the conduct of a vulnerability assessment or "ethical hack" of such website or web accessible system.

9. Customer Complaints; Required Notice. Within 24 hours of any written or oral submission of dissatisfaction or concern (or, for Payment Modalities subject to Regulation E, "errors" as defined by 12 C.F.R. 1005.11(a)) (collectively, "Complaints"), received by Client from any Payment Recipient or from any regulator, network, consumer protection or advocacy agent or other similar party related to Client's performance under these Support Terms or the Support Services, including Client's possession of Payment Recipient information as a result thereof or (b) the privacy rights of any Payment Recipient, Client shall immediately notify its Company-designated customer support team, relationship manager or other designee identified by Company from time to time. Client will promptly and appropriately respond to all Payment Recipient inquiries and complaints, and will promptly resolve the same in accordance with Applicable Law and any applicable policies and instructions provided by Company from time to time. Client agrees to retain all information related to Complaints and provide such information to Company upon request. Client must provide prompt written notice to Company of any regulatory or

enforcement actions taken against Client as a result of or related to the Support Services (to the extent Client is permitted by Applicable Law to disclose the action to Company

10. Survival. The provisions of these Support Terms that, by their nature and content, must survive the termination or expiration of the Agreement in order to achieve the fundamental purposes of these Support Terms will so survive and continue to bind the parties.

11. Issuing Bank as Third Party Beneficiary. Issuing Bank may enforce the provisions of these Support Terms against Client as a third party beneficiary.

Attachment A

Payment Recipient Account Information Requirements

1. Duty of Care. Client will, at a minimum, undertake the following measures with respect to Payment Recipient Account Information received, observed or otherwise accessed by Client:

   (a) appropriately restrict the storage of Payment Recipient Account Information on laptops, portable devices or other portable media and, where Payment Recipient Account Information must be stored on such devices, encrypt all such Payment Recipient Account Information stored on laptops and, where technically feasible, on other portable devices and portable media;

   (b) dispose of Payment Recipient Account Information in such a way so that it may not be decoded, read or decompiled;

   (c) utilize industry standard passwords, firewalls and anti-malware measures to protect Payment Recipient Account Information stored on computer systems; and

   (d) develop, implement, maintain, and monitor a comprehensive, written information security program that contains administrative, technical, and physical safeguards designed to (i) ensure the security and confidentiality of Payment Recipient Account Information, (ii) protect against any unanticipated threats or hazards to the security or integrity of such information, (iii) protect against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to Company or any Payment Recipients, and (iv) guarantee the proper disposal of such information upon termination of the Agreement (the "Information Security Program").

   Client will encrypt all Payment Recipient Account Information that will travel across public networks or that will be transmitted wirelessly. Client will comply, and will ensure that Personnel comply, with all information security requirements that apply to Client, Company and/or Issuing Bank under Applicable Law and prevailing industry information security standards with respect to the protection and treatment of Payment Recipient Account Information. Where Company or Issuing Bank is subject to specific obligations in respect of the processing of Payment Recipient Account Information (such as the requirements set out in the European General Data Protection Regulation), Client will execute such documents and do all such acts as Company or Issuing Bank may reasonably require in order for Client to comply with its or Company's or Issuing Bank's data protection obligations.

2. Use Restrictions**.** Client will access and use Payment Recipient Account Information only: (a) as necessary for Client to provide the Support Services, (b) in accordance with any Applicable Law, and (c) in accordance with the provisions of Company's and Issuing Bank's policies where relevant to the Support Services. In addition, Client will disclose Payment Recipient Account Information only to those Personnel who have a "need to know" such Payment Recipient Account Information (and only to the extent necessary) in order to provide the Support Services. Client will ensure Personnel providing the Support Services are bound to uphold Client's obligations of confidentiality set forth in the Agreement, including without limitation this Attachment.

3. Offshore Access. Client shall not, without Company's express prior written approval, send any Payment Recipient Account Information to or provide access to Payment Recipient Account Information from, any facility or data center outside of the country from which such Payment Recipient Account Information was collected.

4. Legends. Client shall not remove any copyright nor other proprietary notice of confidentiality contained on or included in Payment Recipient Account Information.

5. Notification. If Client becomes aware of any threatened or actual violation of the obligations or restrictions agreed to by Client with respect to Payment Recipient Account Information, Client will immediately notify Company and Client will, and will assist Company with its efforts to, cure or remedy such violation. Client will be liable to Company for any non-compliance by Personnel.

6. Legally Required Disclosures. The obligations of confidentiality hereunder shall not apply to the extent that Client is required to disclose Payment Recipient Account Information under any Applicable Law. Notwithstanding the foregoing, in the event that Client is served with a request from a governmental authority under Applicable Law, Client will:

   a) promptly notify Company of the request or order in order to provide Company an opportunity to seek a protective order;

   b) reasonably cooperate with Company's lawful efforts to resist the disclosure, upon reasonable request by Company; and

   c) disclose only the portion of Payment Recipient Account Information that is required to be disclosed under such Applicable Law.

7. Accounting for Payment Recipient Account Information. Upon termination of the Agreement or at any time upon the request of Company, Client will return, or at Company's election, destroy all Payment Recipient Account Information supplied to, or otherwise obtained by, Client. Client will certify in writing that it has fully complied with such obligations within 7 days following the date it receives a request from Company for such a certification.

8. Information Security Program Compliance. The Information Security Program shall be in compliance with all Rules (including Applicable Laws for Issuing Bank), including, without limitation, the federal banking agencies' Interagency Guidelines Establishing Information Security Standards and Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Client shall ensure that any Subcontractor having access to Payment Recipient Account Information cooperates in the implementation of similar security measures and response programs as may be directed by Company. Client shall internally review and test its Information Security Program at least annually, and more frequently if reasonably requested by Company. The results from each such review shall be promptly provided to Company in writing. If Client offers its own mobile application and/or website, either directly or through an approved third party, Client shall engage a qualified security assessor approved by the PCI Standards Council to conduct an annual vulnerability and penetration test and an assessment of the effectiveness of Client's Information Security Program related to the mobile application and/or website, the results of which shall be provided to Company upon completion.

9. Security Incident Reporting Process. Client shall develop and share with Company an appropriate incident response plan to properly identify, report, investigate, escalate, contain, and recover from any unauthorized use, disclosure, or access to Payment Recipient Account Information ("Security Incident"). Client will provide periodic awareness training to its Personnel on recognizing potential indicators of Security Incidents and reporting the incident through the proper channels as set forth in the Information Security Program. Client will inform need-to-know Personnel about the status of any compromised system involved in a Security Incident that the individual may be using. In the event Client discovers a Security Incident, Client shall take appropriate actions at its own expense to immediately limit, stop, mitigate, or otherwise remedy such Security Incident, including, but not limited to, immediately notifying Company of any such incident and cooperating with the instructions of any regulator. When notifying Company of any Security Incident, Client will include estimates of the scope and impact of the Security Incident and specify the corrective action being taken by Client. In the event of a Security Incident, Company may engage an assessor to determine the extent of the Security Incident. Client shall give the assessor access to Client's facilities, records, systems, and Personnel, as requested by the assessor, and shall be responsible for all costs, expenses, and fees of the assessor. Company shall provide Client, upon receipt, any reports or documents prepared by or received from the assessor relating to the Security Incident. In the event of a Security Incident, Client will be responsible to pay any fines or penalties assessed against Company or Issuing Bank by any applicable debit transaction network or regulator in connection with the breach. Client also agrees to indemnify, defend, and hold harmless the Company Parties and Issuing Bank against any direct losses or expenses arising from any legal action, claim, demand or proceedings brought against any of them by any third party as a result of a Security Incident.

10. Identity Theft Red Flags. Client acknowledges that various United States Federal Agencies have issued rules and guidelines (sometimes referred to as Red Flag Guidelines and Regulations implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003), and require financial institutions and creditors to develop and implement policies and procedures to detect, prevent, and mitigate patterns, practices and specific forms of activity that indicate the possible existence of an actual or attempted theft or misappropriation of Payment Recipient Account Information. Client will comply with such regulations and other Applicable Law and will assist Company and Issuing Bank in every reasonable manner in their efforts to fulfill their respective obligations under such regulations and other Applicable Law.

11. Compliance; Remedies. Client will ensure that its Personnel comply with the Payment Recipient Account Information obligations set forth in these Support Terms. Client acknowledges and agrees that the Payment Recipient Account Information is Company's confidential or proprietary information for purposes of the Agreement. Client further acknowledges and agrees that in the event of any breach of this Attachment, Company will suffer irreparable injury for which it will not have an adequate remedy available at law. Accordingly, in event of any such unauthorized use or disclosure, Company shall be entitled to obtain, without the posting of any bond or security, such injunctive or other equitable relief as may be necessary or appropriate to prevent or curtail any such breach, threatened or actual. The foregoing shall be in addition to and without prejudice to such other rights as Company may have, subject to the express provisions of the Agreement, at law or in equity.

Attachment B

Computer Security Guidelines

Client shall:

1. General

- Appoint one knowledgeable Client employee to respond to Company's inquiries regarding computer security.
- Use commercially reasonable efforts to regularly monitor reputable sources of computer security vulnerability information such as FIRST, CERT/CC, and vendor mailing lists, and implement relevant patches, updates, and upgrades.
- Maintain, for a period of at least 180 days (or such longer period as may be required by law or contract) detailed log files concerning all activity on Client's systems including, without limitation: (i) all sessions established; (ii) information related to the reception of specific information from a user or another system; (iii) failed user authentication attempts; (iv) unauthorized attempts to access resources (software, data, processes, etc.); (v) administrator actions; and (vi) events generated (e.g., commands issued) to make changes in security profiles, permission levels, application security configurations, and/or system resources.
- All log files should be protected against unauthorized access, modification, or deletion.

2. Network and Communications Security

- Deploy multiple layers of defense on Client systems, including but not limited to firewalls, network intrusion detection, and host-based intrusion detection systems. All such systems must be monitored 24 hours/day, 365 days/year.
- Configure firewalls, network routers, switches, load balancers, name servers, mail servers, and other network components in accordance with commercially reasonable industry standards.
- At the request of Company, based on information received by Company about vulnerabilities and threats, restrict access to any Company-specific component of the networks, systems, and applications used to provide the Support Services.

3. Infrastructure Platforms, Services, and Operations Security

- Configure all infrastructure platforms and services (operating systems, web servers, database servers, firewalls, routers, etc.) used to provide the Support Services and authentication mechanisms according to industry best practices.
- Ensure that all remote administrative access to production systems is performed over encrypted connections (i.e., SSH, SCP, SSL-enabled web-management interfaces, and VPN solutions).

4. Application Security

- Permit only authenticated and authorized users to view, create, modify, or delete information managed by applications used in connection with providing the Support Services.
- Ensure that web browser cookies that store confidential data are encrypted (independently of any transport encryption such as SSL) using a public and widely accepted encryption algorithm. All other cookies must be opaque.
- "Time out" and terminate system communication sessions after a mutually agreed upon period of user inactivity.
- Terminate any active sessions interrupted by power failure, system "crash," network problem, or other anomaly, or when the connection is interrupted by the user.
- Validate all input and output prior to use to avoid data-driven attacks such as "cross-site scripting" and "SQL injection."

5. Data Security

- Transmit all highly confidential Company information using a Company-approved encryption algorithm and method.

6. Physical Security

- Maintain all workstations, servers, and network equipment used to provide the Support Services in secure facilities owned, operated, or contracted for by Client.
- Limit access to these secure facilities to authorized Client Personnel with job-related needs.
- Monitor access to these secure facilities through the use of security guards, surveillance cameras, authorized entry systems, or similar methods capable of recording entry and exit information.
- Maintain all backup and archival media containing Company confidential or proprietary information in secure, environmentally-controlled storage areas owned, operated, or contracted for by Client.
- Limit access to backup and archival media storage areas and contents to authorized Personnel with job-related needs.

7. Malicious Code and Virus Protection

- Use the latest, commercially available virus and malicious code detection and protection products on all workstations and servers used to provide the Support Services.
- Report all occurrences of viruses and malicious code, not handled by deployed detection and protection measures, on any workstation or server used to provide the Support Services, to Company within 24 hours of discovery.