PCI Security Standards Council, LLC
Payment Card Industry
Vendor Release Agreement

This Payment Card Industry Vendor Release Agreement (the "Agreement") is entered by and between PCI Security Standards Council, LLC ("PCI SSC") and the undersigned entity ("Vendor"), as of the date of PCI SSC's signature below (the "Effective Date"). For purposes of this Agreement, terms defined in Section 1 below shall have the meanings ascribed therein and capitalized terms used but not otherwise defined in herein shall have the meanings specified in the corresponding Program Documents.

As part of the device, application and solution validation and acceptance programs conducted by PCI SSC (collectively, the "Programs" and each a "Program"), each Product for which Acceptance is sought must undergo Assessment by an Assessor in accordance with applicable Program Requirements. Corresponding Assessment Reports must then be generated in accordance with applicable Program Requirements and, if approved by the relevant vendor, submitted to PCI SSC for review and Acceptance. As part of PCI SSC's quality assurance initiatives, Reviewing QA Team Members may review Assessment Reports for compliance with Program Requirements.

1. Definitions.

(a) "Acceptance" is defined in Section 2(b) below.

(b) "Appropriate Access Privileges" means the right of an Assessor that has been engaged by a vendor to access and use information provided to PCI SSC by that vendor (or its Assessors) for purposes of submitting, accessing and responding to queries from QA Team Members regarding such vendor's Products, Assessment Reports and supporting information.

(c) "Assessment" means either a Contracted Assessment or a Self-Assessment.

(d) "Assessment Report" means, with respect to a given Product, the report of the applicable Assessor attesting to the Assessment thereof and the Assessor's determination as to whether such Product complies with the applicable PCI Standard(s), prepared for purposes of satisfying applicable Program Requirements. The term Assessment Report does not include any Attestation of Validation for any Program.

(e) "Assessor" means, with respect to a given Program and Product, either: (i) an entity (other than the vendor of such Product) that is then qualified by PCI SSC to perform a Contracted Assessment of such Product under such Program, including without limitation: (A) with respect to the PTS Program, a PCI SSC recognized testing laboratory, (B) with respect to the PA-DSS Program, a PA-QSA; and (C) with respect to the P2PE Program, a QSA (P2PE) or PA-QSA (P2PE) (as applicable) or (ii) if and to the extent permitted under such Program, a vendor performing a Self-Assessment of such Product.

(f) "Component" means a service (such as but not necessarily limited to a key injection service, encryption management service or device management service) that (i) is eligible for validation and Acceptance on a standalone basis as part of a Program pursuant to applicable Program Requirements, and (ii) may be incorporated into and/or referenced as part of a Solution pursuant to applicable Program Requirements.

(g) "Contracted Assessment" means the review and evaluation of a Product, performed by an entity other than the vendor of such Product, for purposes of validating the compliance of such Product with an applicable PCI Standard as part of a Program.

(h) “delist” (and similar terms such as “delisting”) mean the removal of a Listed Product from the applicable Validated Product List.

(i) “Listed Product” means a Product appearing on an applicable Validated Product List.

(j) “Participating Payment Brand” means a payment card brand that, as of the time in question, is a PCI SSC Member or affiliate thereof. Participating Payment Brands as of the release of this version of the Agreement were American Express Travel Related Services Company, Inc., DFS Services LLC, JCB Advanced Technologies, Inc., MasterCard International Incorporated, Visa International Service Association (and their affiliates).

(k) “PCI SSC Member” means an entity that, as of the time in question, is then formally admitted as (or an affiliate of) a member of PCI SSC in accordance with its governing documents (status as a PCI SSC “Participating Organization” does not establish that an entity is a PCI SSC Member).

(l) “PCI Standard” means, with respect to a given Program, the then current versions of (or successor documents to) the corresponding security standards, requirements and assessment procedures published by PCI SSC from time to time in connection with such Program and made available on the Website, including but not limited to, any and all appendices, exhibits, schedules and attachments to any of the foregoing and all materials incorporated therein, in each case, as from time to time amended.

(m) “Permitted Purpose” means, with respect to a given Program, use of Vendor Information either (a) to the extent reasonably necessary for purposes of preparing, updating or disseminating PCI SSC Standards and related errata and training materials, or providing related training, in each case, without disclosing details or information regarding the applicable vendor or Listed Product from which the origin of such Vendor Information is reasonably likely to be determined, or (b) on a confidential basis, as reasonably required in connection with applicable QA Team activities, including without limitation, review, evaluation, Acceptance, approval or rejection of Assessment Reports or Products, preparation and delivery of Program acceptance or rejection statements, notices or related electronic communications, PCI SSC quality assurance initiatives, PCI SSC-managed forensics investigations or legal inquiries, and the provision of feedback to vendors and/or the Assessor(s) that initially provided the corresponding Assessment Report or related Vendor Information to PCI SSC, provided that such feedback, to the extent it incorporates any Vendor Information, shall be delivered electronically in encrypted format, and that PCI SSC shall provide Vendor and/or such Assessor(s) (as applicable) with any necessary encryption keys.

(n) “Product” means a device, application, service, Solution or Component with respect to which validation or Acceptance may be sought on a standalone basis as part of a Program pursuant to applicable Program Requirements.

(o) “Program” shall mean any program conducted by PCI SSC under which any Product may be validated and/or Accepted for purposes of demonstrating compliance with the applicable PCI Standard(s), including but not limited to, PCI SSC's PIN Transaction Security (PTS) Device Testing and Approval Program (the "PTS Program"), Payment Application Data Security Standard Program (the "PA-DSS Program"), Point-to-Point Encryption Security Requirements and Assessment Procedures Program (the "P2PE Program"), and any successor, similar or other program conducted by PCI SSC.

(p) "Program Documents” means, with respect to a given Program and vendor or Assessor, the corresponding PCI Standard and Program Guide, all written agreements executed between PCI SSC and such vendor or Assessor in connection with such Program, all other Program-related materials, requirements, obligations, policies and procedures published from time to time by PCI SSC on the Website or elsewhere, and all successor versions of the foregoing, in each case, as amended from time to time.

(q) "Program Guide" means, with respect to a given Program, the then current version of the program guide (if any) published by PCI SSC from time to time in connection with such Program and made available on the Website, and all successor versions thereof, as amended from time to time.

(r) "Program Requirements" means, with respect to a given Program in which Vendor is a participant

and/or otherwise has any of its Products listed on the applicable Validated Product List, all requirements, obligations, policies and procedures applicable to Vendor or otherwise generally applicable to other vendors or participants participating in such Program, as set forth in the corresponding Program Documents, this Agreement or otherwise established by PCI SSC from time to time in connection with such Program, including without limitation, those relating to disclosure and/or PCI SSC's quality assurance initiatives.

(s) "QA Team" means, with respect to a given Program, all QA Team Members collectively.

(t) "QA Team Member" means, with respect to a given Program, an individual employee, representative or contractor of PCI SSC charged by PCI SSC with responsibility for administering, managing or otherwise carrying out any quality assurance-related aspect of the Program (including but not limited to any PCI SSC Member representative serving in such capacity), including without limitation, related Assessor quality management and assurance initiatives.

(u) "Restricted Section" means, with respect to a given Program, a restricted portion of a Restricted Site reserved for (i) QA Team Members who need access in connection with the Permitted Purpose and (ii) Assessors with Appropriate Access Privileges.

(v) "Restricted Site" means, with respect to a given Program, a restricted web site or portal devoted to the activities of the applicable QA Team and Assessors with Appropriate Access Privileges.

(w) "Reviewing QA Team Member" means, with respect to a given Program, the Program Manager and each QA Team Member charged by PCI SSC with responsibility for reviewing the contents of Assessment Reports for purposes of evaluating, Accepting, rejecting and/or Revoking Assessment Reports or Products, carrying out PCI SSC assessor quality management or quality assurance initiatives or PCI SSC-managed forensics investigations, or providing feedback regarding an Assessment Report or other Vendor Information to the vendor or the Assessor(s) for or by which such Assessment Reports or other Vendor Information was provided to PCI SSC.

(x) "Revocation" and "Revoke" refer to the suspension, withdrawal, revocation, cancellation or imposition of conditions upon (including without limitation, by requiring compliance with appropriate remediation requirements determined by PCI SSC) the Acceptance of, and/or the delisting of, any Listed Product.

(y) "Security Issue" means any actual or suspected defect, flaw, weakness or vulnerability of any Listed Product that the applicable vendor in good faith believes has caused or permitted, or could reasonably be expected to cause or permit, unauthorized access to "Account Data" (as defined in the then current version of (or successor document(s) to) the *Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS) Glossary of Terms, Abbreviations, and Acronyms* available on the Website.

(z) "Self-Assessment" means, if, when, and to the extent permitted under a given Program, the review and evaluation of a Product performed by the vendor of that Product for purposes of validating the compliance of that Product with the corresponding PCI Standard as part of such Program.

(aa) "Solution" means a combination of at least two devices, applications, products, Components or services and corresponding configuration information, with respect to which validation or Acceptance may be sought as part of a Program pursuant to applicable Program Requirements.

(bb) "TPS" or "Third Party Service" means a service that (i) is incorporated into and/or referenced by a "P2PE Solution" or "P2PE Component" (as such terms are defined in Appendix B hereto) of Vendor, (ii) is managed by and/or outsourced to a person or entity other than Vendor and (iii) could reasonably be expected to impact the security of such P2PE Solution or P2PE Component.

(cc) "TPS Provider" means a third party (such as but not limited to a key injection facility, certificate authority, payment gateway or data center) that provides a Third Party Service that is incorporated into and/or referenced by a P2PE Solution or P2PE Component of Vendor.

(dd) "Unique Security Issue" means a Security Issue that relies on, is caused by or otherwise exploits

one or more specific vulnerabilities, features or aspects of a Listed Product in a way that is unlikely in Vendor's reasonable opinion to result in the same Security Issue in other Listed Products (as opposed to a Security Issue resulting from an exploit that is being or could reasonably be expected to be directed at a general class of Products without significant modification);

(ee) "Validated Product List" is defined in Appendix A.2(c).

(ff) "vendor" means the vendor or other provider of a Product that is eligible to be considered for Acceptance under a Program.

(gg) "Vendor Customer" means any customer or client of Vendor (or of any TSP Provider, as applicable).

(hh) "Vendor Information" means (subject to Sections 4(b) and 4(e)(ii) hereof) the following, to the extent (i) provided pursuant to applicable Program requirements, (ii) related to Vendor or any Product thereof for which PCI SSC has received a corresponding Assessment Report and (iii) provided to PCI SSC in encrypted format: (A) the contents of each Assessment Report delivered directly by an Assessor to PCI SSC in accordance with this Agreement, (B) any supplemental information delivered directly by an Assessor to PCI SSC regarding a Product for which PCI SSC has received such an Assessment Report (including but not limited to Assessment Reports and Work Papers described in Section 2(a)(ii)), (C) any other information that PCI SSC requires Vendor or its Assessors to provide to PCI SSC in encrypted form, (D) any Vulnerability Handling Policies (defined in Section 2(a)(i)(C) below) provided to PCI SSC pursuant to Section 2(a)(1)(C) and (E) any other information provided to PCI SSC by Vendor pursuant to Section 2(a)(iii) or in connection with any appeal of a Revocation or delisting in connection with a Security Issue.

(ii) "Website" means the PCI SSC web site located at http://www.pcisecuritystandards.org.

2. Procedural Obligations.

(a) Vendor.

i) Required Agreements and Procedures.

(A) Vendor shall execute an appropriate written agreement with each entity that it engages as an Assessor, governing the performance of such Assessor's Contracted Assessments of Vendor's Products and, in connection with such Assessments, the delivery of the corresponding Vendor Products and all necessary information to such Assessors for purposes of enabling such Assessors to both review such Products in accordance with the applicable Program Documents and comply with all applicable Program Requirements and legal requirements (including without limitation, obtaining applicable export licences and permissions and complying with the terms of this Agreement and all applicable Program Requirements generally applicable to Assessors participating in the relevant Program).

(B) To the extent any of Vendor's Products (including but not limited to any of Vendor's Components) incorporates and/or references any TPS other than a Component then appearing on the applicable list of validated Components on the Website, Vendor shall ensure through a rider or other written agreement consistent with the form attached as Appendix B hereto or other means acceptable to Vendor that (i) such TPS Provider has adopted and implemented, and maintains and adheres to Vulnerability Handling Policies in a manner consistent with Section 2(a)(i)(C)) below, (ii) in the event such TPS Provider becomes aware of any Security Issue (which term, solely for purposes of this Section 2(a)(i)(B), shall have the meaning ascribed to it in Appendix B) associated with such TPS, such TPS Provider complies with such Vulnerability Handling Policies, and (iii) such TPS Provider notifies Vendor of such Security Issue in accordance with Appendix B, has authorized Vendor to notify PCI SSC of each Security Issue, and is otherwise required to comply with the obligations set forth in Appendix B.

(C) Vendor shall: (1) on or before the date of submission to PCI SSC of the first Assessment Report regarding a Vendor Product that occurs on or after the Effective Date, adopt and implement documented security vulnerability handling programs and processes consistent with industry best practices ("Vulnerability Handling Policies"), including without limitation, programs and detailed processes regarding detection, receipt, triage, prioritization and repair of (and creation of a corresponding Fix (defined below) or Fixes for) Security Issues, provisions requiring Vendor to provide its Vendor Customers with prompt notification of all identified Security Issues and permitting disclosure of Security Issues and related information to PCI SSC in accordance with this Agreement, and, upon release of associated Product fixes, patches or other mitigations or modifications (each a "Fix"), prompt disclosure and dissemination of such Fixes and information needed to prioritize and implement such Fixes to Vendor Customers and (2) promptly following each reasonable request by PCI SSC, provide (or ensure that its Assessor provides) to PCI SSC a copy of (or access to) Vendor's then current Vulnerability Handling Policies. Access to such Vulnerability Handling Policies (or portions thereof) may be provided to PCI SSC via one or more links to corresponding Vendor web pages, and all Vulnerability Handling Policies (or portions, copies or summaries thereof) that Vendor considers to be and treats as confidential information (a) shall only be provided to PCI SSC in encrypted format and (b) notwithstanding anything to the contrary in this Section, may be provided to PCI SSC in summary or redacted form, but only to the extent reasonably necessary to avoid detailed disclosure of the portions thereof that Vendor considers to be and treats as confidential and proprietary or trade secret information.

(D) While this Agreement is in effect, Vendor shall maintain and comply with all adopted Vulnerability Handling Policies; provided that Vendor may modify such Vulnerability Handling Policies from time to time (as long as the same, as so modified, remain in compliance with the requirements specified in Section 2(a)(i)(C) above), and that promptly following each material modification thereof, Vendor shall notify (or ensure that its Assessor notifies) PCI SSC of such modification and, if reasonably requested by PCI SSC, provide (or ensure that its Assessor provides) to PCI SSC a copy of Vendor's then current Vulnerability Handling Policies as so modified, in accordance with the last sentence of Section 2(a)(i)(C) above.

(E) Vendor shall ensure that, upon completion (and, in the case of a Contracted Assessment, receipt from the Assessor) of each acceptable Assessment Report, the following are submitted to PCI SSC (by Vendor in the case of Self-Assessments, or by the Assessor in the case of Contracted Assessments): (1) a copy of such Assessment Report in accordance with Section 4(a)(i) below, (2) a written attestation executed by an officer of Vendor on or about the date of such submission, attesting that Vendor is and will remain in compliance with its Vulnerability Handling Policies and that Vendor's Vulnerability Handling Policies comply with the requirements of Section 2(a)(i)(C) above, and (3) if reasonably requested by or not previously provided to PCI SSC, copies of all then current Vendor Vulnerability Handling Policies, in accordance with the last sentence of Section 2(a)(i)(C) above.

ii) Assessor Authorization. By signing this Agreement, Vendor hereby grants (and agrees to grant) Appropriate Access Privileges to all Assessors engaged by Vendor and authorizes (and agrees to authorize) all such Assessors to release to (and discuss with) PCI SSC, subject to the terms and conditions set out in this Agreement, the results of and all work papers associated with all Assessments performed by such Assessors with respect to each of Vendor's Products for which an Assessment Report has been provided to PCI SSC (including without limitation, the encrypted and decrypted Assessment Reports themselves) (collectively, "Assessment Reports and Work Papers"), as well as Vendor's executed copy of this Agreement, Vendor's implementation and/or other instruction guides (as described in the applicable Program Documents) for each such Product, and such other information and materials as are required pursuant to this Agreement or that PCI SSC may reasonably request from time to time in accordance with applicable Program Requirements.

iii) Security Issue Procedures:

(A) In the event Vendor becomes aware of a Security Issue with respect to a given Listed Product of Vendor (or TPS or Component incorporated into such Listed Product), Vendor shall comply with its Vulnerability Handling Policies and, promptly (but in any event within 90 days of so becoming aware) provide written notice of such Security Issue to PCI SSC (each a "Security Issue Notice"), including in such notice: (1) the names, PCI SSC approval numbers and any other relevant identifiers of each Listed Product of Vendor that Vendor reasonably believes may be impacted by such Security Issue; (2) a description of the general nature of the Security Issue; (3) Vendor's good faith assessment, to Vendor's knowledge at the time, as to the severity of the vulnerability or vulnerabilities associated with the Security Issue (using CVSS scoring or an alternative industry accepted standard that is reasonably acceptable to PCI SSC) (a "Severity Assessment"); and (4) Vendor's good faith determination, based on Vendor's knowledge at the time, as to whether the Security Issue is a Unique Security Issue (a "Uniqueness Determination").

(B) Upon receipt of any Security Issue Notice, PCI SSC may, in its sole discretion and without any further action: (1) Revoke the Listed Product(s) identified therein and (2) take any or all other action(s) permitted under this Agreement or the Program Documents in connection with a Security Issue.

(C) A Listed Product delisted (and/or with respect to which Acceptance has been Revoked) in connection with a Security Issue will not be reinstated or re-listed until all of the following conditions have been satisfied to PCI SSC's satisfaction: (1) Vendor has released and made available to all users of such Product an appropriate Fix resolving such Security Issue; (2) Vendor has fully executed all of its responsibilities to communicate regarding such Security Issue with all applicable Vendor Customers in accordance with Vendor's Vulnerability Handling Policies; (3) Vendor has engaged an Assessor to perform a Contracted Assessment of such Product as corrected by the Fix (or, if approved by PCI SSC, a Contracted Assessment of the Fix in conjunction with such Product) in accordance with the applicable Program Requirements; (4) Vendor has fully apprised such Assessor of such Security Issue prior to such Assessor commencing such Contracted Assessment; (5) as a result of such Contracted Assessment, such Assessor has delivered to PCI SSC, and PCI SSC has Accepted, a corresponding new Assessment Report for such Product (or Fix, as applicable), along with the materials described in Section 2(a)(iii)(D) below; and (6) Vendor is in compliance with all applicable Program Requirements.

(D) With respect to any Listed Product delisted (and/or with respect to which Acceptance has been Revoked) in connection with a Security Issue and for which Vendor thereafter seeks reinstatement or relisting by PCI SSC and releases a corresponding Fix: (1) the applicable Assessor performing the Contracted Assessment required by Section 2(a)(iii)(C) above shall provide to PCI SSC, prior to such reinstatement or relisting, a joint written attestation signed by an officer of Vendor and the Assessor certifying that Vendor and such Assessor each have complied with their respective obligations pursuant to Section 2(a)(iii)(C) and that the Security Issue has been fully resolved, and setting forth the following: (a) the name, PCI SSC approval number and any other relevant identifiers of the Product; (b) a final joint Severity Assessment by Vendor and such Assessor; (c) a final joint Uniqueness Determination by Vendor and such Assessor; and (d) if such joint Uniqueness Determination is that the Security Issue was not a Unique Security Issue, the following additional information: (i) a detailed description of the Security Issue, and, if applicable, the nature of the data and other information compromised, breached or otherwise put in jeopardy as a result of the Security Issue (as applicable); and (ii) except to the extent prohibited by applicable privacy law, Vendor security personnel names and contact information for purposes of follow-up discussions regarding such Security Issue; and (2) such Assessor and Vendor shall promptly provide to PCI SSC, at no cost or expense to PCI SSC, such additional information and cooperation as PCI SSC may

reasonably request from time to time for purpose of understanding in all material respects the nature, scope, severity, and cause(s) of such Security Issue, the nature of the data and other information compromised, breached or otherwise made vulnerable to unauthorized access as a result thereof, and any corresponding impact on applicable PCI Standards, the PCI Standards development process and/or other products or solutions in the market (in each case, redacted to the extent permitted pursuant to Section 2(a)(iv) below).

iv) Notwithstanding anything to the contrary in Section 2(a)(iii) or elsewhere in this Agreement, Vendor may redact (as described below) from the information otherwise required to be provided to PCI SSC pursuant to Section 2(a)(iii) any (A) Confidential Customer Information (defined below) with respect to a given Vendor Customer that is the subject of the corresponding Security Issue, unless and until such time as such Vendor Customer has authorized Vendor to release such Confidential Customer Information to PCI SSC, which authorization may, at the election of such Vendor Customer, be conditioned upon the execution of a separate non-disclosure agreement mutually acceptable to such Vendor Customer and PCI SSC and (B) information that, under the circumstances, Vendor is prohibited from disclosing to PCI SSC pursuant to applicable privacy law (e.g. laws concerning the protection of personal and/or personally identifiable information, including (if applicable to Vendor and such information under the circumstances) but not limited to, laws promulgated pursuant to the European Commission's Directive on Data Protection, Directive 95/46/EC). For purposes of the foregoing, "Confidential Customer Information" means, with respect to a given Security Issue and Vendor Customer, any of the following information to the extent Vendor is prohibited from disclosing or transferring the same to PCI SSC pursuant to a valid written agreement between Vendor and such Vendor Customer: (1) the name of the applicable Vendor Customer and any other information the disclosure of which to PCI SSC is reasonably likely to enable PCI SSC to determine the identity of such Vendor Customer, (2) information regarding the specific impact of such Security Issue on such Vendor Customer and (3) any valuable trade secret information of such Vendor Customer.

v) Vendor shall comply with all applicable Program Requirements, including without limitation, the terms of this Agreement, requirements regarding payment to PCI SSC of all applicable vendor fees for each Program in which Vendor is a participant ("Program Fees") as and in the manner provided for in the applicable vendor fee schedule provided on the Website or elsewhere in the Program Documents, and requirements relating to Self-Assessments performed by Vendor.

(b) PCI SSC. Following Acceptance of a Product by PCI SSC, PCI SSC will communicate such Acceptance to the Assessor in accordance with the Program Documents, and post applicable details regarding the Product and Vendor on the Validated Product List. A Product is deemed to have been "Accepted" (and "Acceptance" is deemed to have occurred) when all of the following conditions have been met: (i) PCI SSC has received the corresponding Assessment Report regarding the Contracted Assessment of the Product from the Assessor in which the Assessor determines that the Product satisfies all applicable Program Requirements; (ii) PCI SSC has confirmed that the Assessment Report is correct as to form, that the Assessor adequately reported the compliance of the Product in accordance with applicable Program Requirements and that the detail provided in the Assessment Report meets Program Requirements; (iii) PCI SSC has received all applicable Program Fees and all other documentation required with respect to the Product; and (iv) PCI SSC has listed the Product on the Validated Product List (provided that PCI SSC may suspend, withdraw, revoke, cancel or place conditions upon (including without limitation, complying with remediation requirements) Acceptance of any Listed Product in accordance applicable with Program Requirements).

3. Vendor Warranties. Vendor represents and warrants to PCI SSC that, subject to the restrictions on use set forth in this Agreement, it has the right to disclose to the Reviewing QA Team Members all Vendor Information, including without limitation, the contents of each Assessment Report.

4. Confidentiality.

(a) The parties agree that, except as otherwise expressly provided herein or approved by Vendor and PCI SSC in writing:

i) Vendor will ensure that each Assessor (and Vendor, in the case of Self-Assessments) (A) encrypts, using such industry recognized commercial encryption program (e.g., PGP) or processes as may be designated by PCI SSC from time to time ("Required Encryption"), all Assessment Reports and other Vendor Information delivered by the Assessor (or Vendor) to PCI SSC and (B) delivers all such encrypted Vendor Information to PCI SSC in the manner designated by PCI SSC (which may include e-mail, posting directly to a PCI SSC designated web site or portal, or other means, as determined by PCI SSC). With respect to the PTS Program, Required Encryption shall include commercial encryption software capable of generating pairs of mathematically related cryptographic keys and each Reviewing QA Team Member will be required to install such software on his or her own computer and generate one pair of keys, a "Private Key" and a "Public Key." The Private Key will reside on the Reviewing QA Team Member's computer, be accessible only by using a password specified by the Reviewing QA Team Member, and be required in order to decrypt encrypted Vendor Information. The Public Key will be posted on a Restricted Site, sent to each applicable Assessor, and be required in order for the applicable Assessor to encrypt Assessment Reports and other Vendor Information for decryption by Reviewing QA Team Members (the "Public Key"). In the event that a Reviewing QA Team Member loses use of his or her Private Key (if applicable), such Reviewing QA Team Member will be required to install the required encryption software on a replacement computer and generate new Public and Private Keys, and PCI SSC will instruct the Assessors to cease using the original Public Key. Where Public Keys and Private Keys are used, PCI SSC will promptly notify applicable Assessors in the event of any change in the applicable list of then-current Reviewing QA Team Members and instruct such Assessors not to use the Public Key of any person who has ceased to be a Reviewing QA Team Member. Vendor Information delivered to PCI SSC will be maintained in a Restricted Section of the Restricted Site, and PCI SSC will use commercially reasonable efforts to ensure that (except as otherwise permitted under Sections 4(a)(iv) or 4(b)(ii) below) access to the Restricted Section is available only to QA Team Members who need access in connection with the Permitted Purpose and Assessors with Appropriate Access Privileges, and only active Reviewing QA Team Members (including but not limited to PCI SSC Member representatives serving in such capacity) and Assessors with Appropriate Access Privileges are entitled to access, download, decrypt or review such encrypted Vendor Information; provided that, at a minimum, PCI SSC shall require use of an authorized user name and password in order to gain access to the Restricted Section except with respect to staff and contractors of PCI SSC who need access to information other than Vendor Information in connection with standard site operations and maintenance.

ii) Prior to accessing Vendor Information, each Reviewing QA Team Member shall be required to acknowledge and agree in writing or electronically that by accessing Vendor Information, such Reviewing QA Team Member agrees, during the applicable Restricted Period (defined below) (a) not to disclose such Vendor Information to any third party or PCI SSC Related Entity (defined in Section 4(c) below) other than Reviewing QA Team Members who have a need to know, as required by law or as otherwise permitted with respect to "Permitted Advisors" pursuant to Section 4(a)(iv) below, (b) to use such Vendor Information only for the Permitted Purpose, and (c) to take commercially reasonable precautions to keep all Vendor Information, his or her password(s) for the Restricted Section and his or her Private Keys (if applicable) confidential and, at a minimum, safeguard the foregoing with the same degree of control and care as a reasonably prudent person would exercise with respect to his or her own confidential and proprietary information under similar circumstances.

iii) During the applicable Restricted Period (defined below), PCI SSC will use commercially reasonable efforts to: ensure that Reviewing QA Team Members comply with the foregoing restrictions, treat Vendor Information as confidential, take commercially reasonable precautions to prevent any unauthorized use or disclosure thereof, and in any event, at a

minimum, safeguard Vendor Information with the same degree of control and care as a reasonably prudent person would exercise with respect to its own similar confidential and proprietary information under similar circumstances. For purposes of the foregoing: (A) the "Restricted Period" shall be ten (10) years after the date of disclosure of the applicable Vendor Information to PCI SSC; provided, however, that the "Restricted Period" with respect to Product Information (defined below) shall be the period beginning upon disclosure thereof to PCI SSC and ending upon the later of (i) ten (10) years after the date of disclosure thereof to PCI SSC or (ii) ten (10) years after the expiration of the most recent PCI SSC approval of any Vendor Product that Vendor has informed PCI SSC incorporates or utilizes such Product Information (including without limitation successor versions of earlier approved Listed Products); and (B) "Product Information" means all Vendor Information directly relating to the technical or security aspects of any Product for which PCI SSC has received an Assessment Report in connection with the PTS Program, including without limitation, hardware and software design and content, technical processes, formulae and source and object code of such product.

iv) Subject to the foregoing (including without limitation, the specific restrictions set forth in this Agreement with respect to access to decrypted Vendor Information), Vendor Information will only be used in connection with the Permitted Purpose, and access to decrypted Vendor Information will be restricted to those Reviewing QA Team Members (including but not limited to PCI SSC Member representatives serving in such capacity) who have a need to know the same in connection with such Permitted Purpose, Assessors with Appropriate Access Privileges, and professional advisers on a need-to-know basis who are obligated to maintain the confidentiality of such Vendor Information ("Permitted Advisors"). PCI SSC shall notify each Permitted Advisor given access to Vendor Information by PCI SSC that it is obligated to maintain the confidentiality of such Vendor Information.

(b) Vendor acknowledges and agrees that:

i) Notwithstanding anything to the contrary in this Agreement, the restrictions set forth in Section 4(a) above shall not apply to, and the term "Vendor Information" expressly shall not include, any information that:

(A) At the time of disclosure to PCI SSC or any QA Team Member hereunder was, or subsequently becomes, part of the public domain, without breach (or deemed breach) of this Agreement;

(B) Is lawfully obtained by PCI SSC or any QA Team Member from a third party that was not under and did not impose any known obligation of confidentiality with respect to such information;

(C) Is independently developed by PCI SSC or any QA Team Member without reference to any Vendor Information and can be demonstrated as such;

(D) Was known to PCI SSC or any QA Team Member prior to receipt of such Vendor Information, free of any known nondisclosure obligations; or

(E) PCI SSC is otherwise permitted to disclose pursuant to the terms of this Agreement.

ii) Notwithstanding the foregoing, Vendor acknowledges and agrees that PCI SSC may disclose Vendor Information as required by law or in response to any request, subpoena, order or demand issued by any court, government authority or agency of competent jurisdiction. To the extent legally permitted, PCI SSC shall give Vendor timely notice of such disclosure, prior to such disclosure if practicable under the circumstances, in order to provide Vendor an opportunity to intervene to preserve the confidentiality of the Vendor Information; and PCI SSC shall provide Vendor reasonable assistance in its efforts to seek such confidential treatment, at Vendor's request and sole cost and expense.

(c) Vendor acknowledges that in the course of the activities contemplated by this Agreement it may receive information from PCI SSC, any QA Team Member, any PCI SSC Member, any employee, officer, agent or other affiliate of any of the foregoing, or any Permitted Advisor (each of foregoing,

including without limitation, a PCI SSC Member, is referred to as a "PCI SSC Related Entity"), including without limitation, details of security requirements and testing specifications, and information relating to particular attack methods and techniques (collectively, "PCI SSC Information"; and together with the Vendor Information, "Confidential Information"). Vendor agrees that for a period of ten (10) years from receipt of PCI SSC Information:

i) It will treat such PCI SSC Information as confidential, take commercially reasonable precautions to prevent any unauthorized use or disclosure thereof, and in any event, at a minimum, safeguard such PCI SSC Information with the same degree of control and care as a reasonably prudent person would exercise with respect to its own similar confidential and proprietary information under similar circumstances;

ii) It will restrict access to such PCI SSC Information to those of its employees, affiliates, contractors and professional advisors who (A) have a need to know the same for the purposes of performing Vendor's obligations under this Agreement and (B) are obligated to maintain the confidentiality and restrict the use of such PCI SSC Information in a manner that is at least as protective of the PCI SSC Information and PCI SSC's rights therein as the restrictions on use and disclosure set forth in this Agreement, as they apply to Vendor; and

iii) It will only use such PCI SSC Information for the purpose of the activities contemplated by this Agreement.

(d) PCI SSC acknowledges and agrees that:

i) Notwithstanding anything to the contrary in this Agreement, the restrictions set forth in Section 4(c) above shall not apply to, and the term "PCI SSC Information" expressly shall not include, any information that:

(A) At the time of disclosure to Vendor hereunder was, or subsequently becomes, part of the public domain (through a source other than Vendor) without breach of this Agreement;

(B) Is lawfully obtained by Vendor from a third party that was not under and did not impose any known obligation of confidentiality with respect to such information;

(C) Is independently developed by Vendor without reference to any PCI SSC Information and can be demonstrated as such;

(D) Was known to Vendor prior to receipt from the disclosing PCI SSC Related Entity, free of any known nondisclosure obligations; or

(E) Vendor is otherwise permitted to disclose pursuant to the terms of this Agreement.

ii) Notwithstanding the foregoing, PCI SSC acknowledges and agrees that Vendor may disclose PCI SSC Information as required by law or in response to a request, subpoena, order or demand issued by any court, government authority or agency of competent jurisdiction. To the extent legally permitted, Vendor shall give the owner of such PCI SSC Information timely notice of such disclosure, prior to such disclosure if practicable under the circumstances, in order to provide such owner an opportunity to intervene to preserve the confidentiality of the PCI SSC Information; and Vendor shall provide PCI SSC reasonable assistance in its efforts to seek such confidential treatment, at PCI SSC's request and sole cost and expense.

(e) Vendor acknowledges and agrees that:

i) Any PCI SSC Related Entity may become aware of information regarding a Security Issue, Vendor or Product from a variety of sources, that not all such information necessarily constitutes Vendor Information, and that information is only subject to the terms of this Agreement if and to the extent it also constitutes Vendor Information. Nothing in this Agreement shall prevent PCI SSC (or any other PCI SSC Related Entity) from using or disclosing any information that does not constitute Vendor Information, regardless of the nature of such information.

ii) In the event any PCI SSC Related Entity other than PCI SSC becomes aware of information regarding a Security Issue other than from (directly or indirectly) PCI SSC, then notwithstanding anything to the contrary in this Agreement or whether such information may otherwise constitute Vendor Information, and without limiting any other rights of any PCI SSC Related Entity, if such PCI SSC Related Entity discloses such information to PCI SSC, then such information shall no longer be considered Vendor Information for purposes of this Agreement.

iii) In the event PCI SSC becomes aware of a Security Issue with respect to a Vendor Product, then notwithstanding anything to the contrary in this Agreement or the fact that any of the information relating to that Security Issue may constitute Vendor Information, and without limiting any other rights of PCI SSC, PCI SSC will be entitled to use such information for the Permitted Purpose and disclose to each PCI SSC Member (without restriction) that a Security Issue has occurred with respect to the Product in question (without otherwise revealing any other Vendor Information).

(f) The parties agree that any breach of Section 4 of this Agreement would cause irreparable injury to the disclosing party for which no adequate remedy at law exists; therefore, the parties agree that in addition to all other remedies available to the parties, equitable remedies, including without limitation injunctive relief and specific performance, are appropriate remedies to redress any breach or threatened breach of the confidentiality provisions relating to Confidential Information in Section 4 of this Agreement by the receiving party, or any other persons acting for or on behalf of or with the receiving party.

(g) Upon written request, unless otherwise required by law or any request, order or demand issued by any court, government authority or agency of competent jurisdiction, each party (the "Recipient") shall promptly return to the other party (the "Discloser") all Confidential Information of the Discloser in the Recipient's possession or under its control, or (at the election of the Discloser) destroy the same and provide to the Discloser written confirmation of such destruction.

5. Applicability. The provisions of the applicable Program Documents (as modified by PCI SSC from time to time in its sole discretion) and all appendices hereto are hereby incorporated into, and shall apply to all of the activities contemplated by, this Agreement, to the exclusion of any terms and conditions provided by Vendor. In the event of any express conflict between this Agreement and the Program Documents, the terms of this Agreement shall control. PCI SSC agrees that, without Vendor's prior written consent, it shall not impose any warranty, indemnity or confidentiality obligations upon Vendor by way of modification of the Program Documents that are in addition to or inconsistent with Vendor's obligations as set forth in this Agreement.

[Remainder of page intentionally left blank]

IN WITNESS WHEREOF, each of the parties has caused this Agreement to be executed on behalf of such party by its duly authorized officer, to be effective as of the Effective Date.

PCI Security Standards Council, LLC

By:	
Name:	
	(duly authorized signatory)
Title:	
Date:	

Vendor:

By:	
Name:	
	(duly authorized signatory)
Title:	
Date:	
E-mail:	
E-mail Alias:	*(for Section A.2 of Appendix A only)*
Address:	

Appendix A – Additional Legal Terms and Conditions

Vendor hereby agrees to the following additional terms and conditions as a condition to its participation in any Program and listing of any Vendor Product on the Validated Product List:

A.1. No act or omission of PCI SSC, any PCI SSC Member or any affiliate, agent, employee or contractor of any of the foregoing in relation to any Program, or Acceptance of any Product thereunder, constitutes or shall be construed to constitute any:

a. guarantee, warranty or endorsement of Vendor or any Product, whether express or implied, including without limitation, any implied warranty of merchantability, fitness for purpose, or non-infringement, each of which is hereby expressly disclaimed by PCI SSC;

b. guarantee of freedom from security vulnerabilities; or

c. forward-looking statement, and is instead to be limited to the circumstances prevailing at the time of such act or omission or Acceptance.

A.2. PCI SSC:

a. May amend, remove, add to or suspend any provision of any Program, and/or cease to operate any Program, whether with or without replacing it with any other program, in its sole discretion, and without notice.

b. Does not guarantee, warrant or endorse any Product.

c. May, at its discretion, with respect to each Program, publish a list or lists of Products Accepted by PCI SSC thereunder, identifying the applicable validating Assessors and related Program participant information, together with corresponding Product status information (including without limitation, Acceptance, approval, suspension, remediation, and/or Revocation status) and other information identifying such Products, including without limitation, Vendor name and contact information, Product descriptions, version numbers, types, Components, TPSs and TPSPs, target markets and reference numbers, information as to whether or not such Products and/or components thereof have satisfied applicable Program requirements, applicable Acceptance, validation, revalidation and expiry dates, reference, approval or acceptance numbers, deployment notes, PCI Standard version numbers, device types, hardware, firmware and application version numbers, and other information as identified or described in the Program Guide (the applicable list of Products Accepted by PCI SSC for a given Program, the "Validated Product List").

d. May Revoke (i) a given Listed Product in the event Vendor fails to timely pay applicable Program Fees for such Product or PCI SSC reasonably determines that Revocation of such Product is necessary as a result of (A) a Security Issue with respect to, or any other defect, flaw, weakness or vulnerability of such Product that compromises the security of such Product; (B) the failure of such Product to comply with requirements applicable to other Products of the same type or applicable Program Requirements; or (C) PCI SSC's determination that such Product is of a type that is not within the scope of the applicable Program (each of the circumstances described in preceding clause (i) a "Product Default") and/or (ii) all of Vendor's Listed Products, if Vendor fails to comply with any applicable material Program Requirement (each such failure, a "Program Default"), which shall be deemed to include, without limitation, any failure to provide any required notice in accordance with Section 2(a)(iii) of the Agreement or to protect PCI SSC Confidential Information in accordance with Section 4 of the Agreement; provided, however, that for purposes of the foregoing, a Product Default, without more, shall not be considered a Program Default (each of the circumstances described in preceding clause (i) or (ii) above, a "Revocation Event"). PCI SSC shall provide Vendor with written notice of any such Revocation (a "Revocation Notice"), detailing the reasons therefor and providing Vendor an opportunity to request an appeal by providing written notice to PCI SSC within thirty (30) days of the date of the Revocation Notice (the "Initial Appeal Period"). The parties shall negotiate in good faith with respect to any such timely requested appeal until the earlier of (X)

such time as the Revocation Event has been cured to the satisfaction of PCI SSC or (Y) the end of the period consisting of (1) the Initial Appeal Period, (2) except with respect to Vendor's failure to pay applicable Program Fees or any Program Default, a period of sixty (60) days after the end of the Initial Appeal Period and (3) such additional period (if any) as PCI SSC may deem to be reasonable under the circumstances (the entire period described in the preceding clauses (1), (2) (if applicable) and (3) (if applicable), the "Appeal Period"). In the event that, despite good faith negotiations, by the end of the applicable Appeal Period, the Revocation Event has not been cured to PCI SSC's reasonable satisfaction or the parties are unable to otherwise resolve PCI SSC's concerns to PCI SSC's reasonable satisfaction, PCI SSC may permanently revoke its Acceptance of (and accordingly, may permanently delist) the applicable Listed Product(s) immediately upon written notice to Vendor. Notwithstanding the foregoing, PCI SSC may immediately suspend and/or place conditions upon its Acceptance of (and accordingly, may delist) any Listed Product in the event that PCI SSC determines, in its sole but reasonable discretion, either that such Product does not provide sufficient protection against current threats and conform to the requirements of the applicable Program, or that the continued listing and/or Acceptance of such Product by PCI SSC in light of the Revocation Event represents a significant and imminent security threat to users thereof, which suspension, delisting or conditions shall be subject to reinstatement, relisting, withdrawal, revocation, cancellation or imposition of additional conditions pending the outcome of a corresponding appeal (if any) requested by Vendor in accordance with this Section A.2(d). PCI SSC shall notify Vendor in writing of any suspension, delisting or condition imposed pursuant to the preceding sentence in accordance with Section A.11 of this Appendix A and, to the extent Vendor has provided PCI SSC with an "alias" e-mail address (an "E-mail Alias") for purposes of this Section A.2(d) (by including such E-mail Alias on the signature page hereto or notifying PCI SSC of such E-mail Alias in accordance with Section A.11 of this Appendix A), shall also promptly notify Vendor of such suspension, delisting or condition by e-mail sent to such E-mail Alias.

e. For the avoidance of doubt, and without limiting any of PCI SSC's other rights or remedies hereunder, upon any Program Default, subject to compliance with applicable notice and appeal requirements under Section A.2(d) above, PCI SSC's rights under Section A.2(d) of this Appendix A include, and accordingly, as a result of any Program Default PCI SSC shall have, the right to: (i) suspend, withdraw, revoke, cancel or place conditions upon its Acceptance of (and accordingly delist) any or all of Vendor's Listed Products, (ii) suspend processing and/or evaluation of Assessor Reports and/or "deltas" relating to any or all of Vendor's Products, and/or (iii) terminate this Agreement pursuant to Section A.10 of this Appendix A.

A.3. Vendor:

a. Does not obtain any rights, including intellectual property rights, in any Program.

b. May, while this Agreement is in full force and effect, publicize its compliance with applicable Programs and/or, solely with respect to the particular version(s) of a Listed Product that was reviewed by an appropriate Assessor qualified to do so by PCI SSC and subsequently Accepted and listed by PCI SSC on the Validated Product List (the "Accepted Version") (and only while such Acceptance and listing are in effect and have not been suspended, withdrawn, revoked or cancelled), state that such version of such Listed Product has been accepted by PCI SSC, including without limitation, by stating that such version of such Listed Product is "PCI Accepted".

c. Shall not state or imply (or permit any third party to state or imply) that any Product (or version thereof) that has not been Accepted by PCI SSC (or with respect to which such Acceptance or the applicable listing on the Validated Product List has been suspended, withdrawn, revoked or cancelled) has been Accepted (or qualified, certified, validated or otherwise approved by PCI SSSC), or that any such Acceptance, listing, compliance or the passing of any Program testing or requirement is a warranty, endorsement, guarantee or recommendation of Vendor or any Product of Vendor by PCI SSC.

d. To the extent Vendor markets or promotes, or permits any third party to market or promote any Listed Product under a name other than the name of that Product as it then appears on the applicable Validated Product List, Vendor shall ensure that the corresponding marketing and/or promotional materials for such Product (including but not limited to electronic and/or hard copy documentation, materials and press releases, but excluding the Product hardware (if applicable) on which such different name appears) also include the name of that Product as it appears on the applicable Validated Product List.

e. Shall have no authority to make, and accordingly shall not make any statement to any third party or to the public that would constitute any implied or express endorsement or warranty regarding the functionality, quality or performance of any Vendor product or service or any aspect thereof by PCI SSC.

f. Shall have no "right of access" to, and PCI SSC shall be under no obligation to provide to Vendor, any Program data; provided that in the event a Product of Vendor has been rejected, PCI SSC shall notify Vendor and provide an explanation for such rejection.

g. Shall remain, as between PCI SSC and Vendor, the sole owner of all right, title and interest in and to each Vendor Product and all other materials and information of Vendor provided to PCI SSC in connection with this Agreement, including without limitation, all related software and all copyrights, trademarks, patents, trade secrets and other proprietary rights therein.

h. Hereby grants to PCI SSC a limited, non-transferable, fully paid up, irrevocable, worldwide license to use (and permit each QA Team Member to use on behalf of PCI SSC) the Vendor Information as provided for and in accordance with this Agreement, subject to all applicable restrictions and confidentiality requirements set forth in this Agreement.

i. Hereby grants to PCI SSC a limited, non-transferable, fully paid up, irrevocable, worldwide license to (i) use (and permit any Participating Payment Brand to use on behalf of PCI SSC) each Vendor Product provided by Vendor to PCI SSC or any Participating Payment Brand for the purposes (if any) specified in the applicable Program Guide and (ii) post images of Accepted Vendor Products on the applicable Validated Product List and otherwise use and display such images for legitimate PCI SSC purposes. Except as otherwise permitted or contemplated by this Agreement, nothing in this Agreement shall be construed to grant to PCI SSC any other right, license or interest in any Vendor Product or related intellectual property rights.

A.4. Vendor acknowledges and agrees, and shall take reasonable steps to inform all purchasers, licensees and other users of Vendor Products that have been Accepted under any of the Programs, that:

a. Acceptance and/or listing of a given Product by PCI SSC only applies to the Accepted Version of that Product, and only while such Acceptance and listing are in effect. If any aspect of a product or version thereof is different from that which was reviewed by such Assessor and Accepted and listed by PCI SSC – even if the different product or version (the "Alternate Version") conforms to the basic product description of the Accepted Version – then the Alternate Version is not Accepted by PCI SSC and Vendor shall not (and shall not permit any third party to) market or promote the Alternate Version as such. The authoritative lists of Products then Accepted by PCI SSC will appear on the Website.

b. Vendor shall not (and shall not permit any third party to) refer to any product as having been approved, accepted, qualified, certified or validated (using the foregoing or similar terms) by PCI SSC, or otherwise state or imply that PCI SSC has, in whole or part, approved, accepted, qualified, certified or validated (using the foregoing or similar terms) any aspect of Vendor or its services or products, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a corresponding letter of acceptance provided by PCI SSC. All other references to PCI SSC's approval, acceptance, qualification, certification or validation (using the foregoing or similar terms) of any product, service or version thereof are strictly and actively prohibited by PCI SSC, should be reported to PCI SSC, and

constitute a breach of applicable Program requirements.

c. When granted, Acceptance is provided to signify the Assessor's determination that the Product has demonstrated achievement of certain security and operational characteristics important to the security of payment card data, but such Acceptance does not under any circumstances include or imply any endorsement or warranty by PCI SSC regarding applicable vendor, the Product, or the functionality, quality, or performance of the Product or any other product or service. PCI SSC does not warrant any products or services provided by third parties. Acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or noninfringement, all of which are expressly disclaimed by PCI SSC. To the extent any rights or remedies regarding products or services that have received acceptance from PCI SSC are provided, those rights and remedies shall be provided by the party providing such products or services, and not by PCI SSC or any of its payment brand members.

d. When granted, Acceptance of a given Product applies solely to the Accepted Version of that Product, and does not, under any circumstances, include or imply that the vendor of that Product, or any of its facilities, operations, services or other products in any way complies with any PCI Standard.

A.5. To the extent permitted by applicable law, in no event will PCI SSC be liable to Vendor, any other participant in any Program or any third party (including without limitation, Vendor's and such participants' customers) for any loss, damages (including without limitation, direct, special, punitive, exemplary, incidental or consequential damages) or costs (including without limitation, attorneys' fees) (each of the foregoing, collectively, "Claims") arising out of or relating to this Agreement or the performance or non-performance of any aspect of any Program or any obligation hereunder or thereunder; provided, however, that such limitation shall not apply to Claims by Vendor to the extent such Claims (a) arise from any breach or deemed breach of the confidentiality obligations in Section 4(a) of this Agreement; (b) arise from any withdrawal, revocation, cancellation or conditions placed by PCI SSC on Acceptance in violation of Section A.2 of this Appendix A, but only to the extent such Claims are caused directly by PCI SSC's gross negligence or willful misconduct; or (c) are for direct damages resulting from any breach or deemed breach of any other terms of this Agreement by PCI SSC which, in the aggregate, do not exceed the total amount Vendor has paid to PCI SSC or any approved Assessor performing Contracted Assessments for Vendor during the twelve months prior to such Claim in respect of activities that Vendor has undertaken as part of the applicable Program.

A.6. To the extent permitted by applicable law, in no event will Vendor be liable to PCI SSC, any other PCI SSC Related Entity or any other third party for any Claims arising out of or relating to this Agreement or the performance or non-performance of any obligation of Vendor hereunder; provided, however, that such limitation shall not apply to (a) Claims arising from any breach by Vendor of its obligations under Sections 2(a)(iii), 3 or 4(c) of this Agreement; (b) Vendor's indemnification obligations under this Agreement (including without limitation, this Appendix A); or (c) Claims for direct damages resulting from any breach of any other terms of this Agreement by Vendor which, in the aggregate, do not exceed the total amount Vendor has paid to PCI SSC or any approved Assessor performing Contracted Assessments for Vendor during the twelve months prior to such Claim in respect of activities that Vendor has undertaken as part of the applicable Program.

A.7. To the extent permitted by applicable law, under no circumstances will any PCI SSC Related Entity (other than PCI SSC in accordance with the limitations set forth in Sections A.5 and A.8 of this Appendix A) be liable to Vendor, any participant in any Program or any other third party (including without limitation, Vendor's and such participant's customers) for any Claim whatsoever, arising out of or in connection with this Agreement or the performance or non-performance of any aspect of any Program; provided that the parties acknowledge and agree that the breach by any PCI SSC Related Entity of any provision of this Agreement, including disclosure of Vendor Information to or by any PCI SSC Member in breach of the terms of this Agreement, will be deemed to be a breach

of such provisions by PCI SSC for purposes of this Agreement, and that, accordingly, subject to the limitations set forth in Sections A.5 and A.8 of this Appendix A, PCI SSC shall be solely responsible to Vendor for any such breach, and Vendor's sole remedy with respect to any Claims arising from such breach shall be to seek recovery directly against PCI SSC in accordance with and subject to the limitations set forth in this Agreement.

A.8. The limitations of liability set forth above in Sections A.5, A.6 and A.7 of this Appendix A shall apply to any and all Claims or causes of action under law or equity whatsoever, including contract, warranty, strict liability, or negligence, even if PCI SSC, Vendor or the applicable PCI SSC Related Entity has been notified of the possibility of such Claims or causes of action.

A.9. Notwithstanding anything to the contrary in Sections A.6 or A.8 of this Appendix A, Vendor will defend, indemnify and hold harmless each PCI SSC Related Entity from and against any and all losses, third-party claims, damages, injuries, expenses (including reasonable attorneys' fees and court costs) and liabilities arising out of or in connection with any (i) breach of Vendor's representations or warranties under Section 3 of this Agreement; (ii) third-party claim regarding any Vendor Product, the use thereof, or the fact that such Product suffers from any defect, flaw, security weakness or vulnerability (provided that the indemnity provided for in the foregoing language of this clause (ii) shall not apply to any Participating Payment Brand or any affiliate, employee, officer or agent of such Participating Payment Brand, other than (a) PCI SSC, PCI SSC's employees, officers or Permitted Advisors and those individuals who comprise PCI SSC's governing boards and (b) individuals who are QA Team Members), or does not comply with any express or implied warranties or commitments made by Vendor to its customers or clients; or (iii) third-party claim that any Vendor Product infringes, misappropriates or violates any patent, trademark, copyright, trade secret, or other intellectual property right. Upon becoming aware of any claim for which indemnification may be sought hereunder, PCI SSC shall reasonably promptly notify Vendor thereof and shall reasonably cooperate with Vendor (at Vendor's request and sole cost and expense) in connection therewith (provided that the failure or delay in providing such notice or cooperation shall not relieve Vendor from any obligation to indemnify as provided for hereunder except to the extent such delay or failure materially prejudices Vendor's ability to defend against such claim). Vendor shall be entitled to control the handling of any such claim against PCI SSC and to defend or settle any such claim, in its sole discretion, with counsel of its own choosing; provided, however, that, in the case of any such settlement, Vendor shall obtain written release of all liability of PCI SSC, in form and substance reasonably acceptable to PCI SSC; and provided, further, that PCI SSC shall have the right, but not the obligation, to participate in the handling, defense or settlement of any such claim with counsel of its own choosing, at PCI SSC's request and sole cost and expense.

A.10. This Agreement shall commence as of the Effective Date and shall remain in full force and effect for a period ending upon the effective date of termination in accordance with this Section (the "Term"). Vendor may terminate this Agreement at any time upon thirty (30) days written notice to PCI SSC. PCI SSC may terminate this Agreement (a) effective as of the end of any calendar year during the Term upon at least one hundred twenty (120) days prior written notice to Vendor; (b) subject to prior compliance with applicable notice and appeal requirements under Section A.2(d) above, upon thirty (30) days prior written notice to vendor in the event of any Program Default that is not resolved to PCI SSC's satisfaction within the applicable Appeal Period; or (c) immediately upon written notice to Vendor in the event (1) no Vendor Product is listed on any Validated Product List, (2) PCI SSC discontinues all Programs in which Vendor is a participant, or (3) Vendor is subject to voluntary or involuntary bankruptcy, receivership, reorganization, dissolution or liquidation under state or federal law and the same is not dismissed within thirty (30) days. Upon any termination of this Agreement: (i) all Vendor Products will be removed from the Validated Product List; (ii) Vendor shall immediately cease all advertising and promotion of its Products as listed on the Validated Product List or otherwise Accepted or approved by PCI SSC; (iii) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify any of its PCI SSC Members and any acquirers, Vendor Customers or others of such termination and the reason(s) therefore (without disclosing Vendor Information); and (iv) the confidentiality provisions and Sections 1 and 4 of this Agreement,

and the provisions set forth in Sections A.1, A.3 and A.5 through A.12 of this Appendix A shall survive such termination in accordance with their respective terms.

A.11. This Agreement shall be governed by the internal laws of the State of Delaware, without regard to its choice of law provisions, as such laws are applied to agreements entered into and fully performed in the State of Delaware. The parties hereby consent to the non-exclusive jurisdiction of the Federal and State courts located in Wilmington, Delaware, U.S.A., for purposes of resolving disputes that may arise under this Agreement. Any notice required or permitted under this Agreement shall be in writing and sent to the intended recipient at the applicable address on the signature page of this Agreement (in the case of Vendor) or PCI Security Standards Council, LLC, 401 Edgewater Place, Suite 600, Wakefield, MA 01880, Attention: General Manager (as applicable). Either party may modify its address and contact for notice purposes by notice in accordance with the preceding requirements and all notices will be deemed effective upon delivery by hand, five (5) days after being deposited in the US mails, postage prepaid, certified or registered, return receipt requested, or on the next business day after being sent by overnight courier, charges prepaid.

A.12. Except as otherwise expressly provided herein, no modification or amendment to this Agreement shall be effective unless made in a writing executed by both parties. No waiver under this Agreement in one instance shall effect a waiver in any other instance. This Agreement, all Appendices hereto and the provisions of the Program Documents together constitute the entire agreement of the parties with respect to the subject matter hereof, and amend, restate and supersede in all respects all prior agreements or understandings between the parties hereto with respect to such subject matter.

[remainder of page intentionally left blank]

Appendix B – PCI Security Standards Council Third Party Service Provider Rider

This PCI Security Standards Council Third Party Service Provider Rider (the "Rider") is entered into by and between [INSERT VENDOR NAME] ("Vendor") and [INSERT THIRD PARTY SERVICE PROVIDER NAME] ("TPSP") as of [INSERT RIDER EXECUTION DATE] in connection with the [INSERT NAME OF APPLICABLE AGREEMENT BETWEEN VENDOR AND TPSP] between Vendor and TPSP dated [INSERT DATE OF APPLICABLE AGREEMENT BETWEEN VENDOR AND TPSP] (the "Agreement"). Capitalized terms used herein shall have the meanings set forth in Section D below or elsewhere in this Rider.

As a P2PE Solution Provider or vendor of a P2PE Component approved by PCI Security Standards Council, LLC ("PCI SSC"), pursuant to the terms of the Payment Card Industry Vendor Release Agreement between Vendor and PCI SSC (the "VRA"), Vendor may be required to disclose to PCI SSC certain TPSP Information under the circumstances described herein.

In order to ensure that Vendor has all necessary rights and permissions to make such disclosures if and when requested by PCI SSC in accordance with the VRA and applicable P2PE Program policies and procedures, for good and valuable consideration, the receipt and sufficiency of which are acknowledged, TPSP and Vendor hereby agree as follows:

A. Notwithstanding anything to the contrary in the Agreement or any other agreement between Vendor and TPSP, TPSP hereby (i) agrees to adopt, implement, maintain and adhere to Vulnerability Handling Policies in a manner consistent with the terms of the VRA, (ii) agrees that upon becoming aware of any Security Issue involving any service or product provided by TPSP that is incorporated into and/or referenced by any P2PE Solution or P2PE Component then identified on the list of P2PE Solutions or P2PE Components on the PCI SSC Website (each a "TPS"), TPSP shall (a) comply with such Vulnerability Handling Policies and (b) promptly (and in any event within 30 days of so becoming aware) notify Vendor of such Security Issue, including in such notice the information specified in Section B below and (iii) authorizes Vendor (without any additional consent, authorization, approval or permission of TPSP or otherwise required) to disclose to PCI SSC the information described in Sections B(i), B(ii) and B(iii) below and the good faith assessments described in Section B(iv) below (all of the foregoing information, collectively, "TPSP Information").

B. Each notice required pursuant to Section A(ii)(b) above shall include the following information: (i) the name and PCI SSC approval number of each P2PE Solution and/or P2PE Component subject to such Security Issue; (ii) the name and a description of the applicable TPS; (iii) a description of the general nature of such Security Issue and the status thereof; and (iv) any additional information reasonably requested by Vendor in order for Vendor to make a good faith assessment as to the impact or potential impact of such Security Issue on Vendor's P2PE Solution(s), P2PE Component(s) and customers and as to whether the Security Issue in question is the result of an exploit that is being or could reasonably be expected to be directed at a general class of P2PE Solutions, P2PE Components or other products or services without significant modification.

C. The parties acknowledge that to the extent any TPSP Information disclosed to PCI SSC pursuant to this Rider constitutes "Confidential Information" for purposes of the VRA, the use and disclosure thereof by PCI SSC shall be governed by the terms and conditions of the VRA.

D. For purposes of this Rider, the following capitalized terms shall be defined as follows:

1. "P2PE Component," "P2PE Solution" and "P2PE Solution Provider" shall have the respective meanings ascribed to them in the then current version of (or successor document to) the *Payment Card Industry (PCI) Point-to-Point Encryption (P2PE)™ Glossary of Terms, Abbreviations, and Acronyms* then available on the PCI SSC Website.

2. "P2PE Program" means the Point-to-Point Encryption Security Requirements and Assessment Procedures Program conducted by PCI SSC.

3. “PCI SSC Website” means means the PCI SSC web site located at http://www.pcisecuritystandards.org.

4. "Security Issue" means any actual or suspected defect, flaw, weakness or vulnerability of any P2PE Solution, P2PE Component or component of any of the foregoing that TPSP in good faith believes has caused or permitted, or could reasonably be expected to cause or permit, unauthorized access to Account Data (as defined in the then current version of (or successor document(s) to) the *Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS) Glossary of Terms, Abbreviations, and Acronyms* available on the PCI SSC Website.

E. This Rider is hereby incorporated into and deemed a part of the Agreement, and the Agreement is hereby amended to the extent necessary to enable Vendor to make the disclosures provided for herein in accordance with the terms hereof. This Rider shall survive any termination or expiration of the Agreement.

IN WITNESS WHEREOF, the parties hereto have caused this Rider to be executed as of the date first above written.

[VENDOR COMPANY NAME]		**[TPSP COMPANY NAME]**	
By:	_____	By:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____