Payment Card Industry (PCI)
Data Security Standard
Validation Requirements

For Approved Scanning Vendors (ASV)

Version 1.2
October 2008

Document Changes

Date	Version	Description
October 1, 2008	1.2	To align version number with PCI DSS v1.2; no other changes made.

Table of Contents

1 Introduction

In response to requests from merchants for a unified set of payment account data security requirements, members of the payment card industry (PCI) have adopted a single set of requirements for cardholder data protection across the entire industry. This PCI Data Security Standard (PCI DSS) is maintained by the PCI Security Standards Council, LLC (PCI SSC).

Key to the success of the PCI DSS is merchant and service provider compliance. PCI DSS requirements, when implemented appropriately, provide a well-aimed defense against data exposure and compromise.

The PCI SSC will provide the tools needed for compliance with the standard.

Organizations that validate adherence by performing vulnerability scans of internet facing environments of merchants and service providers are known as Approved Scanning Vendors (ASVs).

The compliance tools applicable to Internet-facing systems include specific requirements for scans of merchants and service providers (the PCI Scanning Procedures), and periodic remote PCI Scanning Services of these organizations by recognized scanning vendors.

Validation of these requirements by independent and qualified security companies is important to ensure the effectiveness of PCI DSS. The quality, reliability, and consistency of an ASV's work are essential to ensure the protection of cardholder data.

This document describes the necessary qualifications for an ASV company (and staff) to be recognized by the PCI SSC to perform remote PCI Scanning Services.

To achieve (and maintain) approval status, ASVs must comply with requirements in this document.

1.1 Goal

To be recognized as an ASV by PCI SSC, the ASV, ASV employees, and the ASV's scanning solution must meet or exceed the requirements described in this document and execute the "PCI ASV Compliance Test Agreement" attached as Appendix A (the "Agreement") with PCI SSC. The companies that qualify are identified on PCI SSC's ASV list on PCI SSC's web site in accordance with the Agreement.

The requirements defined in this document serve as a **validation baseline** for PCI SSC and provide a transparent process for ASV admittance and re-qualification across the payment industry. The ASV must adhere to all requirements in these *Validation Requirements for Approved Scanning Vendors (ASV)* (the "ASV Requirements") and must provide all of the required provisions described.

1.2 Qualification Process Overview

The ASV qualification process consists of three parts: the first involves the qualification of the security company itself. The second relates to the qualification of the company's employee(s) responsible for the remote PCI Scanning Services. The third consists of the security testing of the company's remote scanning solution(s).

All ASVs appear on the PCI SSC ASV list. If a security company is not on this list, its work product is not recognized by PCI SSC. ASVs appearing on this list must re-qualify annually.

The ASV requirements are incorporated into the Agreement. To initiate the qualification process, the security company must sign the Agreement in unmodified form and submit it to PCI SSC. One provision of the Agreement requires the company to warrant that – to the best of its ability – the information provided to PCI SSC to support the ASV application process is accurate and complete as of the date of its submission.

1.3 Document Structure

This document defines the requirements a security company must meet to become an ASV. The document is structured in five sections as follows.

Section 1: Introduction offers a high level overview of the ASV applications process.

Section 2: ASV Business Requirements covers minimum business requirements that must be demonstrated to PCI SSC by the security company. This section outlines information and items that must be provided to prove business stability, independence, and insurance coverage.

Section 3: ASV Capability Requirements reviews the information and documentation necessary to demonstrate the security company's service expertise, as well as that of at least one of its employees (the scanning operation technical manager).

Section 4: ASV Administrative Requirements focuses on the standards to meet regarding the logistics of doing business as a PCI ASV, including background checks, adherence to PCI procedures, quality assurance, and protection of confidential and sensitive information.

Section 5: ASV Qualification Maintenance briefly outlines the yearly re-qualification process, as well as revocation procedures if there is a breach of the Agreement.

1.4 Related Publications

This document should be used in conjunction with other PCI SSC publications: the *PCI Data Security Standard*, the *PCI Technical and Operational Scanning Requirements*, and the *PCI Scanning Procedure*s, available through the PCI SSC web site.

1.5 ASV Application Process

I In addition to explaining the requirements that a PCI ASV must meet to perform remote PCI Scanning Services, this document describes the information that must be provided to PCI SSC as part of the application process. Each outlined requirement is followed by the information that must be submitted to document that the security company meets or exceeds the stated requirements. To facilitate preparation of the application package, refer to Appendix B: "ASV Application Process Checklist."

All application packages must include a signed Agreement and the required documentation. Applicants should send the completed packages by mail to the following address:

PCI SSC
401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone number: 1-781-876-8855

E-mail submissions will not be accepted.

2 ASV Business Requirements

This section describes the minimum business requirements and related information that must be provided to PCI SSC. The provisions requested include information about the company's business legitimacy, independence, and required insurance coverage.

2.1 Business Legitimacy

2.1.1 Requirement

The ASV must be recognized as a legal entity. Provisions

2.1.2 Provisions

The following information must be provided to PCI SSC:

- Copy of Business license or equivalent, including year of incorporation, and location(s) of offices
- Written statements describing any past or present allegations or convictions of any fraudulent or criminal activity involving the ASV (and ASV principals), and the status and resolution

2.2 Independence

2.2.1 Requirement

The ASV must adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing PCI Scanning Services.

The ASV must have a code of conduct policy, and provide this code of conduct policy to PCI SSC upon request.

The ASV must adhere to all independence requirements as established by PCI SSC, including without limitation, the following:

- The ASV must not undertake to perform PCI Scanning Services of entities that it controls or with which it is under common control or in which it holds any investment.
- The ASV must not have been offered or provided (and will not offer or provide) any gift, gratuity, service, or other inducement to any employee of PCI SSC or any ASV subject or agency involved in retaining the ASV to enter into the Agreement or to provide ASV-related services.
- The ASV must fully disclose in the Scan Report if they perform PCI Scanning Services to customers who use any security-related devices or security-related applications that have been developed or manufactured by the ASV, or to which the ASV owns the rights, or that the ASV has configured or manages, including the following:
  - Application or network firewalls
  - Intrusion detection/prevention systems
  - Database or other encryption solutions

  - Security audit log solutions
  - File integrity monitoring solutions
  - Anti-virus solutions
- The ASV agrees that when the ASV recommends remediation actions which include one of its own solutions or products, the ASV will also recommend other market options that exist.
- The ASV agrees that it will not use its status as a "listed ASV" to market services unnecessary to bring ASV subjects into compliance with the PCI DSS.
- The ASV must not, and agrees that it will not, misrepresent requirements of the PCI DSS in connection with its promotion or sales of services to ASV clients, or state or imply that the PCI DSS requires use of the ASV's products or services.

2.2.2 Provisions

The ASV must describe company practices to maintain scanning independence, including but not limited to practices, organizational structure/separation, and employee education in place to prevent conflicts of interest in a variety of scenarios, such as the following:

- ASV customer uses products or applications developed or manufactured by the ASV company.
- ASV customer uses products or applications managed or configured by the ASV company.

2.3 Insurance Coverage

2.3.1 Requirement

At all times while its Agreement is in effect, the ASV shall maintain sufficient insurance, insurers, coverages, exclusions, and deductibles that PCI SSC reasonably requests to adequately insure the Vendor for its obligations and liabilities under the Agreement, including without limitation, the ASV's indemnification obligations.

The ASV must adhere to all requirements for insurance coverage required by PCI SSC, including without limitation, the requirements in Appendix D – Insurance Coverage, which includes details of required insurance coverage.

2.3.2 Provisions

The ASV must sign the Agreement, which states that the ASV meets locally applicable PCI SSC insurance coverage requirements.

The ASV must provide a proof of coverage statement to PCI SSC to show that insurance coverage matches locally-mandated insurance coverage requirements.

3 ASV Capability Requirements

This section describes the minimum ASV capability requirements and related documentation the ASV must provide to PCI SSC. The provisions requested include information to demonstrate necessary information security vulnerability assessment expertise, work history, and industry experience.

3.1 ASV Company – Services and Experience

3.1.1 Requirement

The ASV must possess security scanning assessment experience similar or related to the PCI Scanning Services.

The ASV must have a dedicated security practice that includes staff with specific job functions that support the security practice.

3.1.2 Provisions

The following information must be provided to PCI SSC:

- ASV's experience and knowledge with information security vulnerability assessment engagements and penetration testing, preferably related to payment systems
- Description of the ASV's relevant areas of specialization within information security (for example, network security, database and application security, and incident response)
- Evidence of a dedicated security practice, such as the number of employees performing security scanning assessments and the percentage of time dedicated to such PCI Scanning Services
- Brief description of core business offerings
- Description of size and types of market segments in which the ASV tends to focus, such as Fortune 500, financial industry, insurance industry, or small-medium sized businesses
- List of languages supported by the ASV
- Two client references from security engagements within the last 12 months

3.2 ASV Staff – Skills and Experience

At least one ASV employee performing or managing PCI scanning Services must be qualified by PCI SSC. ASV employees are responsible for performance of the PCI Scanning Services in accordance with the PCI Technical and Operation Scanning Requirements.

3.2.1 Requirement

The ASV employee(s) performing or managing PCI Scanning Services should possess sufficient information security knowledge and experience to conduct technically complex scanning assessments, and should possess industry-recognized security certification(s) or equivalent work experience.

The ASV employee(s) performing or managing the PCI Scanning Services must be knowledgeable about the PCI DSS and the PCI Technical and Operation Scanning Requirements. ASV employee(s) may be required to attend annual training provided by PCI SSC, and pass the examination conducted at training.

3.2.2 Provisions

The following information should be provided to PCI SSC for each individual that conducts PCI Scanning Services to be qualified:

- Area(s) of Expertise (network security, application security and consultancy, system integration, auditing, special skills) with at least 1 year (total) in three separate areas
- Years of working experience and responsibilities
- Years of experience related to payment industry and responsibilities
- Résumé
- ASV's are requested to provide PCI SSC documentation of the following certifications for employees performing PCI Scanning Services:
- Copy of Certified Information System Security Professional (CISSP) certificate and ID number
- Copy of Certified Information Systems Auditor (CISA) certificate and ID number
- Copy of Certified Information Security Manager (CISM) certificate and ID number
- If the managing employee does not have any of the above experience, criteria, or certificates, he or she must provide a description of a **minimum of five (5) years** of relevant information security experience or proof of other recognized security certifications.

4 ASV Administrative Requirements

This section describes the administrative requirements for ASVs, including company contacts, background checks, adherence to PCI procedures, quality assurance, and protection of confidential and sensitive information

4.1 Contact Person

4.1.1 Requirement

The ASV must provide PCI SSC with a primary and secondary contact.

4.1.2 Provisions

The following contact information must be provided to PCI SSC, for both primary and secondary contacts:

- Name
- Title
- Address
- Phone number
- Fax number
- E-mail address

4.2 Background Checks

4.2.1 Requirements

The ASV must perform a background check (as described in this subsection) when hiring ASV employees, if legally permitted within the applicable jurisdiction.

The ASV must adhere to all background check requirements as required by PCI SSC.

Upon request, the ASV must provide to PCI SSC the background check history for each ASV employee, when legally permitted within the applicable jurisdiction.

4.2.2 Provisions

The ASV must provide the following to PCI SSC:

- For each employee to be qualified, a written statement that the ASV employee successfully completed the background check in accordance with the ASV's policies and procedures (where legally permitted)
- The ASV must sign the Agreement, which includes a statement that the ASV will perform background checks for each ASV employee, in accordance with applicable ASV procedures
- A summary description of current ASV personnel background check policies and procedures, to confirm the procedures include at least (to the extent legally permissible in the applicable jurisdiction):
- Gathering of current photographs

- Verification of aliases (when applicable)
- Review of records of any criminal activity, arrests, or convictions, updated annually
- Comparison of fingerprints with national and regional criminal records

  Note: *Misdemeanors are allowed, but felonies automatically disqualify an employee from consideration as an ASV employee.*

4.3 Adherence to PCI Procedures

4.3.1 Requirements

The ASV report must follow the procedures documented in the PCI Technical and Operational Scanning Requirements Provisions

The ASV must sign the Agreement, which includes a statement that the ASV will adhere to the requirements.

4.4 Quality Assurance

4.4.1 Requirements

- The ASV must have an implemented quality assurance process.
- The ASV must adhere to all PCI SSC quality assurance requirements.
- The ASV must provide an ASV Feedback Form to their client at the completion of the PCI Scanning Service. See Appendix C – "Sample ASV Feedback Form".
- PCI SSC reserves the right to conduct site-visits and audit the ASV at the discretion of the PCI SSC.
- Upon request, the ASV must provide the quality assurance manual to PCI SSC.

4.4.2 Provisions

The ASV must provide the following to PCI SSC:

- The ASV's executed Agreement, which includes a statement that the ASV has developed and implemented, and will adhere to, a quality assurance process and manual
- A description of the contents of the ASV quality assurance process, to confirm the procedures fully document the PCI Scanning Services and the review process for generation of the report requirements contained in the PCI Technical and Operational Scanning Requirements, including at least the following:
  - Reviews of scanning procedures, supporting documentation, and information documented in the *PCI Technical and Operational Scanning Requirements* related to the appropriate selection of system components
  - Requirement that ASV employees must adhere to the PCI Technical and Operational Scanning Requirements

4.5 Protection of Confidential and Sensitive Information

4.5.1 Requirements

The ASV must maintain adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect sensitive and confidential information against any threats or unauthorized access during storage, processing, and/or communicating of this information.

The ASV must adhere to all requirements to protect sensitive and confidential information, as required by PCI SSC.

The ASV must maintain the privacy and confidentiality of information obtained in the course of performing duties under the Agreement, unless (and to the extent) disclosure is required by legal authority.

4.5.2 Provisions

The ASV must provide the following:

- Description of the ASV's confidential and sensitive data protection handling practices, including physical, electronic, and procedural safeguards, including at least the following:
- Systems storing customer data do not reside on Internet accessible systems
- Protection of systems storing customer data by adequate network and application layer controls including a firewall and IDS/IPS
- The following physical and logical access controls:
- Restricting access (for example, via locks) to the physical office space
- Restricting access (for example, via locked file cabinets) to paper files
- Restricting logical access to electronic files by role-based access control
- Encryption of sensitive customer information when transmitted over the Internet either by e-mail or other means
- Secure transport and storage of backup media
- Encryption of customer data on consultants' laptops
- Description of requirements and processes used to ensure employee confidentiality of customer data, including a (blank) copy of confidentiality agreements required to be signed by employees
- ASV must sign the Agreement, which includes a statement that the ASV will adhere to the requirements.

4.6 Evidence Retention

4.6.1 Requirements

The ASV must securely maintain digital and/or hard copies of case logs, scanning results and work papers, notes, and any technical information that was

created and/or obtained during the PCI Scanning Services for a minimum of two (2) years.

The ASV must adhere to all requirements to protect sensitive and confidential information, as required by PCI SSC.

This information must be available upon request by PCI SSC and its Affiliates for a minimum of two (2) years.

The ASV must provide a copy of evidence retention policy and procedures to PCI SSC upon request.

4.6.2 Provisions

A description of the ASV's evidence retention policy and procedures that covers the requirements must be provided to PCI SSC.

5 ASV Initial Qualification and Annual Re-qualification

This section describes the process after initial qualification and activities related to the annual ASV re-qualification. This section includes 1) the ASV list, 2) annual maintenance of ASV qualification, and 3) revocation, if necessary, of an ASV's qualification.

5.1 ASV List

Once a company has met all requirements specified in this document, PCI SSC will add the ASV to the Approved Scanning Vendor List. Only those ASVs on this list are authorized by PCI SSC to perform remote PCI Scanning Services. This list is posted on the PCI SSC web site.

PCI SSC reserves the right to perform random site audits of the ASV.

In the event a company does not meet the requirements in this document, PCI SSC will notify the company.

The company will have 30 days from the date of notification to appeal the decision. Appeals must be addressed to PCI SSC General Manager and follow the procedures outlined on https://pcisecuritystandards.org.

If a company's appeal is denied, its name will not be placed on the approved PCI Approved Scanning Vendor List.

5.2 ASV Re-qualification

5.2.1 Requirements

All ASVs and employees must be re-qualified by PCI SSC on an annual basis, based on the ASV's original qualification date. Re-qualification by PCI SSC is based on payment of annual fees, proof of training attended, and satisfactory feedback from the ASV clients (the merchants or service providers that received PCI Scanning Services) to PCI SSC

PCI SSC reserves the right to perform random on-site audits of the ASV.

5.2.2 Provisions

The following must be provided to PCI SSC and/or will be considered by PCI SSC during the re-qualification process:

- Feedback from ASV clients (entities that received PCI Scanning Services), requested by PCI SSC (see Appendix C – "Sample ASV Client Feedback Form"). Significant or excessive unsatisfactory feedback may be cause for revocation.
- Proof of information systems vulnerability assessment training within the last 12 months to support professional certifications (even if the employee does not have professional certifications), of a minimum 20 hours per year and 120 hours over the rolling three year period. This is in addition to training provided by PCI SSC.

5.3 ASV Revocation Process

The following examples highlight some of the revocation conditions covered by the Agreement, provided here for clarity purposes only.

An ASV may have its qualification revoked if it is found to be in breach of the Agreement, including for the following reasons:

- The ASV fails to validate compliance in accordance with the PCI Technical and Operational Scanning Requirements.
- The ASV violates any provision regarding non-disclosure of confidential materials.
- The ASV fails to maintain physical, electronic, and procedural safeguards to protect confidential and sensitive information and/or fails to report unauthorized access to systems storing confidential and sensitive information.
- The ASV engages in unprofessional or unethical business conduct.
- The ASV fails to provide quality services, based on customer feedback or evaluation by PCI SSC or its Affiliates.

When an ASV qualification is revoked, the ASV will have 30 days from the date of notification to appeal the revocation. Appeals must be addressed to the PCI SSC General Manager and must follow procedures outlined on https:/www.pcissecuritystandards.org.

If an ASV's appeal is denied, the following will result:

- The ASV name will be removed from the approved PCI Approved Scanning Vendor List.
- PCI SSC will notify the participating payment brands.

Appendix A. PCI ASV Compliance Test Agreement

THIS AGREEMENT (the "Agreement") is entered into between PCI Security Standards Council, LLC, a Delaware limited liability company, having its principal place of business at 401 Edgewater Place, Suite 600, Wakefield, Massachusetts 01880 ("PCICo") and the entity identified on the signature page below ("Vendor"), effective as of the date executed by PCICo as set forth on the signature page hereto (the "Effective Date").

PCICo and Vendor are hereinafter collectively referred to as the "Parties".

RECITALS

A. PCICo is an international consortium of payment systems companies, established by its founding Members to maintain, develop and support the implementation of standards relating to payment account security.

B. PCICo offers a cost-effective, global security solution called the PCI Approved Scanning Vendor Compliance Test Program ("ASV Program"), which provides security compliance solution vendors with the ability to deploy security compliance programs to assist their Vendor Clients to better protect against illegitimate network intrusions and account data compromises (collectively, "Vendor Services").

C. As part of the ASV Program, PCICo publishes the PCI Standard.

D. Vendor is the provider of a Security Solution or Security Solutions that it believes are compliant with the PCI Standard.

E. PCICo is willing to assist and to check whether such Security Solutions are compliant with the PCI Standard and Vendor meets the requirements for PCICo-approved scanning vendors ("ASVs"). In case a Security Solution is deemed compliant with the PCI Standard and Vendor meets such requirements, Vendor will be entitled to present itself to Vendor Clients as an ASV with respect to such Security Solution in the framework of the ASV Program, as provided in this Agreement.

F. Vendor has submitted an online application form requesting participation in the ASV Program and PCICo has considered Vendor as eligible to move to the initial approval Testing phase of the ASV Program.

NOW THEREFORE, in consideration of the mutual promises herein, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1 Definitions

1.1 In addition to the definitions established elsewhere in this Agreement, the following terms, when capitalized in this Agreement, shall have the following meanings ascribed to them:

"**Compliance Notification**" shall mean the letter in the form attached as Schedule 2, which is hereby incorporated into this Agreement;

"Confidential Information" shall mean (i) all terms of this Agreement; (ii) any and all information designated in this Agreement as Confidential Information; (iii) any and all originals or copies of, any information that either Party has identified in writing as confidential at the time of disclosure; and (iv) any and all Personal Information, proprietary information, merchant information, technical information or data, scan reports, trade secrets or know-how, information concerning either Party's past, current, or planned products, services, fees, finances, member institutions, Issuers, Acquirers, concepts, methodologies, research, experiments, inventions, processes, formulas, designs, drawings, business activities, markets, plans, customers, equipment, card plastics or plates, software, source code, hardware configurations or other information disclosed by either Party or any Member, or their respective directors, officers, employees, agents, representatives, independent contractors or attorneys, in each case, in whatever form embodied (e.g., oral, written, electronic, on tape or disk, or by drawings or inspection of parts or equipment or otherwise), including without limitation, any and all other information that reasonably should be understood to be confidential. "Personal Information" means any and all Member payment card account numbers, Member transaction information, IP addresses or other PCICo, Member or third party information relating to a natural person, where the natural person could be identified from such information. Without limiting the foregoing, Personal Information further includes any information related to any Member accountholder that is associated with or organized or retrievable by an identifier unique to that accountholder, including accountholder names, addresses, or account numbers.

"**Intellectual Property Rights**" shall mean all present and future patents, trade marks, service marks, design rights, database rights (whether registrable or unregistrable, and whether registered or not), applications for any of the foregoing, copyright, know-how, trade secrets, and all other industrial or intellectual property rights or obligations whether registrable or unregistrable and whether registered or not in any country;

"**Member**" means a then current member of PCI Security Standards Council, LLC.

"**PCI Standard**" means the then current version of the PCI Data Security Standard, the current version of which is accessible on the PCICo web site at http://www.pcisecuritystandards.org (the "Website");

"**Related Company**" shall mean each entity that directly or indirectly, controls, is controlled by, or is under common control with Vendor, and any entity in which Vendor holds any investment in excess of 5%.

"**Security Solution**" means a solution (consisting of the applicable administration process, scanning tools and reporting system for such solution) that Vendor believes is compliant with the PCI Standard and which is to be assessed during the Testing phase of the ASV Program. Each Security Solution is identified and referred to in the applicable Compliance Notification (as further described in clause 5.1(b)).

"**Testing**" means evaluating a Security Solution to determine whether or not it complies with the PCI Standard; "Test" and "Tested" will be interpreted accordingly;

"**Vendor Client**" means any member financial institution of a Member (each a "Financial Institution"),issuer of Member payment cards (each an "Issuer"), merchant authorized to accept any Member payment cards (each a "Merchant"), acquirer of Merchant accounts ("Acquirer") or data processing entity performing services for any Financial Institution, Issuer, Merchant or Acquirer ("Processor").

1.2 In this Agreement and unless the context otherwise requires, words importing the singular include the plural and vice versa, words importing the masculine gender include the feminine and neuter and vice versa. References to clauses and schedules are, unless otherwise stated, references to clauses of, and schedules to this Agreement. Headings are for convenience only and are not to affect the interpretation of this Agreement.

1.3 This Agreement is comprised of the following:

Clauses 1 to 14

Schedule 1: Fees

Schedule 2: Compliance Notification (sample)

2 Vendor obligations

2.1 Vendor shall provide all reasonable assistance as well as accurate information and documentation to PCICo and its agents as may be needed for the purpose of Testing.

2.2 Vendor shall disclose the result of the Test or any other technical information exchanged in the scope of Testing only in accordance with the provisions of clause 6.

2.3 Vendor acknowledges and agrees that it may only advertise, offer or use a Security Solution as Tested and deemed compliant by PCICo, and in accordance with clause 5.1(b). Consequently, Vendor shall immediately inform PCICo of any significant change in any Security Solution as provided in clause 3.1.

2.4 Vendor acknowledges that even though a Security Solution receives a Compliance Notification, such Security Solution shall be subject to an annual Testing maintenance process. Such annual Testing maintenance process shall ensure that such Security Solution remains capable of identifying newly reported public domain vulnerabilities. Consequently, Vendor shall submit each Security Solution for annual maintenance Testing within three (3) months upon request from PCICo.

2.5 Vendor shall make nonrefundable payment to PCICo of the applicable fees in accordance with the payment terms set forth in Schedule 1, which is hereby incorporated into this Agreement. Vendor acknowledges that PCICo may review and modify the fees specified in Schedule 1 at any time and from time to time. Whenever a change in such fees occurs, PCICo shall notify Vendor in accordance with the terms of clause 12. Such change(s) will be effective for any new Testing submission and annual Testing maintenance after the date of PCICo's notification of such changes. However, should Vendor not agree with such change(s), Vendor shall have the right to terminate this Agreement in accordance with the provisions of clause 6.2(iii) (A) at any time within thirty days of delivery of the aforementioned notice.

2.6 Vendor shall comply with all requirements as set forth in the then current versions of the "Technical and Operational Requirements for Approved Scanning Vendors" and the "Validation Requirements for Approved Scanning Vendors" (collectively, the "ASV Requirements") as each is set forth on the Website. Additionally, Vendor agrees to monitor the Website at least weekly for changes to the ASV Requirements and to comply with all such changes within 15 days of the effective dates thereof.

3 Terms and conditions of Testing

3.1 In accordance with the terms of clause 2.3 where Vendor shall inform PCICo of any significant change in each Security Solution, PCICo may decide in its sole discretion (i) that such Security Solution is deemed to remain compliant by sending a new Compliance Notification or (ii) to request Vendor to resubmit a modified Security Solution for a new Testing within one (1) month upon receipt by PCICo of said information given pursuant to clause 2.3 and subject to payment of the related new Testing fee (and Additional Testing fee if applicable) as specified in Schedule 1.

3.2 Notwithstanding clause 3.1, if at any time PCICo believes that a Security Solution is no longer compliant with the PCI Standard, PCICo shall be entitled to require Vendor to resubmit such Security Solution for a new Testing within three (3) months of such request from PCICo and subject to payment of the related new Testing fee (and Additional Testing fee) as specified in Schedule 1.

3.3 Vendor shall have no "right of access" to any data associated with the ASV Program or Testing, except as allowed by PCICo under this Agreement.

3.4 PCICo shall have no obligation with respect to Vendor having not successfully completed Testing other than informing Vendor that Vendor is not compliant with the PCI Standard by sending a non-compliance notification to Vendor.

3.5 PCICo may amend, remove, add to or suspend any provision of the ASV Program, or cease to operate the ASV Program, whether with or without replacing it with any other program, in its discretion. Additionally, PCICo may from time to time require Vendor to provide a representative to attend any mandatory training programs in connection with the ASV Program, which may require the payment of attendance and other fees.

3.6 In order to assist in ensuring the reliability and accuracy of Vendor's testing and assessment procedures for Vendor Clients, Vendor hereby agrees to provide to any Member, within 15 days of written request by such Member, such Vendor Client testing and assessment results as such Member (as applicable) may reasonably request with respect to any Vendor Client that is a Financial Institution of such Member, Issuer of such Member, Merchant authorized to accept such Member's payment cards, Acquirer of accounts of Merchants authorized to accept such Member's payment cards or Processor performing services for such Member's Financial Institutions, Issuers, Merchants or Acquirers. Each agreement between Vendor and its Vendor Clients shall include such provisions as may be required to ensure that Vendor has all necessary rights, licenses and other permissions necessary for Vendor to comply with its obligations and requirements pursuant to this Agreement. Any failure of Vendor to comply with this clause 3.6 shall be deemed a material breach of this Agreement for purposes of clause 7.3(b) (i), and upon any such breach, PCICo may remove Vendor's name from the ASV List and/or terminate this Agreement in its sole discretion.

3.7 Vendor shall allow PCICo or its designated agents access during normal business hours during the Term (as defined in clause 7.1) and for a period of six (6) months thereafter to perform audits of Vendor's facilities, operations and records on Vendor Services to determine whether Vendor has complied with this Agreement. Vendor shall provide PCICo or its designated agents during normal business hours with books, records and supporting documentation adequate to evaluate Vendor's performance. Upon request, Vendor shall provide PCICo or its designated agents with a copy of its most recent audited financial statements, a letter from Vendor's certified public accountant or other documentation acceptable to PCICo setting out Vendor's current financial status and warranted by Vendor to be complete and accurate. Any failure of Vendor to comply with this clause 3.7 shall be deemed a material breach of this Agreement for purposes of clause 7.3(b) (i), and upon

any such breach, PCICo may remove Vendor's name from the ASV List and/or terminate this Agreement in its sole discretion.

4 Intellectual Property Rights

4.1 All Intellectual Property Rights, title and interest in the ASV Program and the PCI Standard, including future versions or revisions, extensions, and improvements thereof, are and at all times shall remain solely and exclusively the property of PCICo or its licensors, as applicable. All Intellectual Property Rights, title and interest in all materials Vendor receives from PCICo are and shall remain vested in PCICo or its licensors, as applicable. Vendor may use and disclose, subject to the provisions of clause 6, such materials only for the purposes of this Agreement.

4.2 All Intellectual Property Rights, title and interest in all assessment results performed by PCICo are and at all times shall remain the property of PCICo. Vendor may use and disclose, subject to the provisions of clause 6, the assessment results only for the purposes of this Agreement. Vendor shall not revise, abridge, modify or alter such assessment results. Vendor shall not assert or imply that assessment results other than those upon which a Compliance Notification was issued by PCICo are connected or related to such Compliance Notification. Vendor shall have the right to make copies of a given Compliance Notification to inform PCICo and its Members' members that the Security Solution described therein is in compliance with the PCI Standard and that Vendor has been approved as an ASV.

4.3 Vendor shall not during or at any time after the completion, expiry or termination of this Agreement in any way question or dispute PCICo's or its licensors' (as applicable) Intellectual Property Rights in the ASV Program.

4.4 All Intellectual Property Rights, title and interest in material submitted by Vendor to PCICo for assessment and Testing purposes are and at all times shall remain vested in Vendor.

5 Advertising and Promotion

5.1 ASV List and Use of ASV Marks.

(a) As long as Vendor is in Good Standing (as defined below) as an ASV, PCICo may, at its sole discretion, display the identification of Vendor and each Security Solution that complies with the PCI Standard, together with information as to such compliance, in such publicly available list of ASVs as PCICo may maintain and/or distribute from time to time, whether on the Website or otherwise (the "ASV List"). Vendor shall provide all requested information necessary to ensure to PCICo's satisfaction that the identification and information provided on the ASV List are accurate. Vendor shall be deemed to be in "Good Standing" as an ASV as long as this Agreement is in force, Vendor has been approved as an ASV and such approval has not been revoked, a Vendor Security Solution has successfully completed the Testing phase of the ASV Program and is in compliance with the PCI Standard, and Vendor is not in breach of any of the terms and conditions of this Agreement (including without limitation, all provisions regarding compliance with the ASV Requirements and payment).

(b) If Vendor is in Good Standing and PCICo issues a Compliance Notification (in the form set out in Schedule 2) confirming that a given Security Solution is deemed compliant with the PCI Standard and that PCICo has approved Vendor as an ASV, Vendor may disclose and advertise the same and the existence of such Compliance Notification, in accordance with the terms of such Compliance Notification. In the event that Vendor is no longer in Good Standing as an ASV, Vendor's rights pursuant to the preceding

sentence shall immediately cease and the Security Solution and related Vendor's information shall be removed from the ASV List. In the event that Vendor is otherwise in Good Standing as an ASV, but a given Security Solution of Vendor's is no longer deemed compliant with the PCI Standard, Vendor's rights pursuant to the first sentence of this clause 5.1(b) with respect to such noncompliant Security Solution shall immediately cease and such noncompliant Security Solution shall be removed from the ASV List. While Vendor is in good standing as an ASV and Vendor is listed in the ASV List, Vendor may also make reference to the fact that it is so listed in its advertising materials.

(c) Vendor shall make no use of PCICo or Member marks without the prior written consent of PCICo or the applicable Member that owns such marks, as the case may be. Without limitation of the foregoing, Vendor shall have no authority and consequently shall not make any statement that would constitute any implied or express endorsement, recommendation or warranty by PCICo regarding Vendor, the Vendor Services or products (including but not limited to Vendor's Security Solution(s)) or the functionality, quality or performance of any aspect of any of the foregoing. All materials referring to the PCI Standard, Vendor's listing on the ASV List or any PCICo or Member mark must be reviewed and approved in writing by PCICo and, to the extent applicable, such Member, prior to publication or other dissemination in each instance. Prior review of such materials by PCICo and any applicable Member does not relieve Vendor of any responsibility for the accuracy and completeness of such materials or for Vendor's compliance with this Agreement or any applicable law. Any dissemination of promotional materials or publicity in violation of this Agreement shall be deemed a material breach of this Agreement and upon any such violation, PCICo may remove Vendor's name from the ASV List and/or terminate this Agreement in its sole discretion.

5.2 Uses of ASV Name and Designated Marks. ASV grants PCICo and each Member the right to use ASV's name and trademarks, as designated in writing by ASV, to list ASV on the ASV List and to include reference to ASV in publications to Financial Institutions, Issuers, Merchants, Acquirers, Processors, and the public regarding the ASV Program. Neither PCICo nor any Member shall be required to include any such reference in any materials or publicity regarding the ASV Program. ASV warrants and represents that it has authority to grant to PCICo and its Members the right to use its name and designated marks as contemplated herein.

5.3 No Other Rights Granted. Except as expressly stated in this clause 6, no rights to use any Party's marks or other intellectual property are granted and each Party respectively reserves all rights therein. Without limitation of the foregoing, no rights are granted to ASV to any intellectual property in the PCI Standard or otherwise.

6 Confidentiality

6.1 General Restrictions

(a) Each Party (the "Receiving Party") agrees that all Confidential Information received from the other Party (the "Disclosing Party") shall: (i) be treated as confidential; (ii) be disclosed only to those Members, officers, employees, legal advisers and accountants of the Receiving Party who have a need to know and be used thereby solely as required in connection with (A) the performance of this Agreement and (B) the operation of such Party's respective payment card data security compliance programs and (iii) not be disclosed to any third party except as expressly permitted in this Agreement or in writing by the Disclosing Party, and only if such third party is bound by confidentiality obligations in form and substance similar to the provisions of this clause 6.

(b) Except with regard to Personal Information, such confidentiality obligation shall not apply to information which: (i) is in the public domain or is publicly available or becomes publicly available otherwise than through a breach of this Agreement; (ii) has been lawfully obtained by the Receiving Party from a third party; (iii) is known to the Receiving Party prior to disclosure by the Disclosing Party without confidentiality restriction; or (iv) is independently developed by a member of the Receiving Party's staff to whom no Confidential Information was disclosed or communicated. If the Receiving Party is required to disclose Confidential Information of the Disclosing Party in order to comply with any applicable law, regulation, court order or other legal, regulatory or administrative requirement, the Receiving Party shall promptly notify the Disclosing Party of the requirement for such disclosure and co-operate through all reasonable and legal means, at the Disclosing Party's expense, in any attempts by the Disclosing Party to prevent or otherwise restrict disclosure of such information.

6.2 Vendor Client Data

To the extent any data or other information obtained by Vendor from any Vendor Client in the course of providing Vendor Services is subject to any confidentiality restriction between Vendor and such Vendor Client, the applicable agreement containing such restriction must permit (a) Vendor to disclose such information to PCICo and/or its Members, as requested by the Vendor Client, and (b) each Member to disclose such information on an as needed basis to its respective member Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies. Confidentiality of information provided to Members by Vendor or any Vendor Client shall be subject to confidentiality arrangements between such Member, on the one hand, and Vendor or such Vendor Client (as applicable), on the other hand. Accordingly, notwithstanding anything to the contrary in clause 6.1(a), PCICo may disclose Confidential Information obtained by PCICo in connection with this Agreement to Members in accordance with this clause 6.2, who in turn may disclose such information to their respective member Financial Institutions and other Members. Vendor hereby consents to such disclosure by PCICo and its Members.

6.3 Personal Information

In the event that Vendor receives Personal Information from PCICo or any Member or Vendor Client in the course of providing Vendor Services or otherwise in connection with this Agreement, in addition to the obligations set forth elsewhere in this Agreement, Vendor will at all times during the Term maintain such data protection handling practices as may be required by PCICo from time to time, including without limitation, as a minimum, physical, electronic and procedural safeguards designed: (a) to maintain the security and confidentiality of such Personal Information (including, without limitation, encrypting such Personal Information in accordance with applicable Member guidelines); (b) to protect against any anticipated threats or hazards to the security or integrity of such information; and (c) to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to such cardholders. Vendor will make available to PCICo and its Members, and will require in its agreements with Vendor Clients that Vendor Clients will make so available, such appropriate reviews and reports to monitor Vendor's compliance with the foregoing commitments as PCICo or its Members may reasonably request from time to time. Without limitation of the foregoing, Vendor acknowledges and agrees that if it performs certain services for PCICo, its Members or any Vendor Client, Vendor may be required to be certified as compliant with the PCI Standard as such may be modified by PCICo from time to time. If compliance with the PCI Standard is required, Vendor, at its sole cost and expense, shall: (i) conduct or have conducted the audits required for such compliance; and (ii) take all actions required for Vendor to maintain such compliance. If required to be compliant with the PCI Standard, Vendor acknowledges

that it further has the obligation to keep up to date on any changes to the PCI Standard and implement any required changes.

6.4 Return

Upon termination of this Agreement or upon demand, Vendor promptly shall return to PCICo all property and Confidential Information of PCICo and of third parties provided by PCICo. If agreed by PCICo, a certificate of destruction may be provided instead, with sufficient detail regarding the items destroyed, destruction date, and assurance that all copies also were destroyed.

6.5 Remedies

In the event of a breach of this clause 6 by the Receiving Party, the Receiving Party acknowledges that the Disclosing Party will likely suffer irreparable damage that cannot be fully remedied by monetary damages. Therefore, in addition to any other remedy that the Disclosing Party may possess pursuant to applicable law, the Disclosing Party retains the right to seek and obtain injunctive relief against any such breach in any court of competent jurisdiction. In the event any such breach results in a claim by any third party, the Receiving Party shall indemnify, defend and hold harmless the Disclosing Party from any claims, damages, interest, attorney's fees, penalties, costs and expenses arising out of such third-party claim(s).

7 Term and Termination

7.1 This Agreement shall enter into force upon the Effective Date and, unless earlier terminated in accordance with this clause 7, shall remain in force for an initial term of one (1) year (the "Initial Term") and automatically renew thereafter for successive additional periods of one (1) year (each a "Renewal Term", and collectively with the Initial Term, the "Term").

7.2 PCICo shall have the right, without prejudice to its other rights or remedies, to terminate this Agreement immediately by written notice to Vendor if: (a) Vendor shall have failed to pay in accordance with the terms of this Agreement any fee due and that fee remains unpaid for fifteen (15) days after receiving written notice from PCICo that it has not been paid; (b) PCICo determines, at PCICo's discretion, that Vendor has failed to comply with any of Vendor's obligations pursuant to clause 2.6 of this Agreement; (c) PCICo determines, in its sole discretion, that Vendor has failed to achieve successful results in connection with (i) the initial Testing, (ii) the annual maintenance Testing performed pursuant to clause 2.4 and/or (iii) any Testing performed pursuant to clause 3.1 or 3.2; (d) Vendor fails to resubmit a given Security Solution within the timelines provided in clauses 2.4, 3.1 and 3.2; or (e) PCICo ceases to operate the ASV Program, whether with or without replacing it with any other program; provided, however, that if Vendor thereafter determines that it has satisfied each of the requirements set forth in the preceding clauses (a) through (d), Vendor may request a new compliance review by PCICo in accordance with clause 3.2. PCICo may undertake such review, at PCICo's sole discretion, and if PCICo determines that Vendor is in compliance with all applicable requirements, then PCICo may reinstate this Agreement and Vendor's status as an ASV effective as of the date of such determination, subject to payment of all outstanding fees (if any), the related new Testing fee and the applicable Additional Testing fee as required by clause 3.2. Upon termination of this Agreement in accordance with this clause 7.2 or clause 7.3(b)(iii)(B), PCICo shall reimburse Vendor on a pro rata temporis basis the fees already paid by Vendor up to the date of such termination.

7.3 Either Party shall have the right to terminate this Agreement (a) effective as of the last day of the then current Term, for any or no reason, upon at least thirty (30) days notice to the other Party or (b) at any time by giving thirty (30) days prior written notice to the other

Party: (i) if the other Party (the "Defaulting Party") is in material breach of any of its obligations under this Agreement and either that breach is incapable of remedy or the Defaulting Party shall have failed to remedy that breach within thirty (30) days after receiving written notice from the other Party requiring it to remedy that breach on the understanding that consent to extend the remedy period shall not be unreasonably be withheld, so long as the Defaulting Party has commenced remedy during the said thirty (30) days and pursues remedy of the breach on a best efforts basis; (ii) upon the other Party's insolvency, receivership, or voluntary or involuntary bankruptcy (or the institution of any proceeding therefore), or any assignment for the benefit of the other Party's creditors or on the occurrence of any event which is analogous to any of the above under the laws of the jurisdiction in which such Party is incorporated; or (iii) in the event that Vendor does not agree with (A) modified fees as provided in clause 2.5 or (B) any unilateral modification, alteration or amendment of this Agreement as provided in clause 14.2.

7.4 Termination of this Agreement shall automatically imply termination of Vendor's compliance with the ASV Program. Consequently, (a) identification of each Vendor Security Solution and (b) Vendor's related information shall be removed from the ASV List and Vendor shall return or destroy (as PCICo shall instruct), on its own account, to PCICo any such material supplied by PCICo and any copies made thereof, no later than fourteen (14) days after termination. Vendor shall furnish PCICo with a certificate, certifying that the same has been done. Upon any termination or expiration of this Agreement: (i) Vendor shall immediately cease all advertising and promotion of its status as an ASV and all references to the PCI Standard; (ii) Vendor shall immediately cease soliciting for any further Vendor Services and shall only complete Vendor Services contracted with Vendor Clients prior to the notice of termination; (iii) Vendor will comply with all outstanding information requests within the time contracted with its Vendor Clients and shall remain responsible after termination for all of the obligations, representations and warranties hereunder with respect to Vendor Services provided prior to or after termination. The provisions of clauses 1, 4, 5.1(c), 5.3, 6, the last sentence of clause 7.2, 7.4, 9, 10 and 12 through 14 of this Agreement shall survive the expiration or termination of this Agreement for any reason.

8 Representations and warranties

8.1 Vendor represents and warrants that by entering into this Agreement and performing any Testing under this Agreement, Vendor will not breach any obligation to any third party.

8.2 Vendor represents and warrants that it will comply with all applicable laws, ordinances, rules, and regulations in any way pertaining to this Agreement, the Vendor Services or to the Testing performed under this Agreement.

8.3 Vendor agrees to comply with the ASV Requirements, including without limitation, all requirements regarding independence, and hereby warrants and represents that Vendor is now, and shall at all times during the Term, remain in compliance with the ASV Requirements.

9 Indemnification

9.1 Vendor hereby agrees to indemnify and hold harmless PCICo, its Members, officers, employees, agents, representatives and contractors (each, an "Indemnified Party") from and against any and all losses, liabilities, damages, claims, suits, actions, government proceedings, taxes, penalties or interest, associated auditing and legal expenses and other costs (including without limitation, reasonable attorney's fees and related costs) arising out of or related to (a) Vendor's breach of its agreements, representations and warranties contained in this Agreement, (b) Vendor's use of the ASV Program or related information (i)

in violation of this Agreement, or (ii) in violation of any applicable law, rule or regulation, (c) Vendor's non-performance of Vendor Services for any Vendor Client or (d) Vendor's negligence or willful misconduct, except to the extent arising out of the negligence or willful misconduct of an Indemnified Party. All indemnities provided for under this clause shall be paid as incurred by the Indemnified Party. This indemnification shall be binding upon Vendor and its executors, heirs, successors and assigns. Nothing in this Agreement shall be construed to impose any indemnification obligation on Vendor to the extent any claim or liability arises solely from a defect in the PCI Standard or other materials provided by an Indemnified Party and used by Vendor without modification and in accordance with this Agreement.

9.2 Vendor's indemnity obligations are contingent on PCICo's providing notice of the claim or liability to Vendor. Upon receipt of such notice, Vendor will be entitled to control, and will assume full responsibility for, the defense of such matter. PCICo will cooperate in all reasonable respects with Vendor, at Vendor's expense, in the investigation, trial and defense of such claim or liability and any appeal arising there from; provided, however, that PCICo and its Members may, at their own cost and expense, participate in such investigation, trial and defense and any appeal arising there from or assume the defense of any Indemnified Party. In any event, PCICo will have the right to approve counsel engaged by Vendor to represent any Indemnified Party, which approval shall not be unreasonably withheld. Vendor will not enter into any settlement of a claim that imposes any obligation or liability on PCICo or any other Indemnified Party without such Indemnified Party's prior written consent.

10 No warranties - Limitation of liability

10.1 PCICO PROVIDES THE ASV PROGRAM ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND. VENDOR ASSUMES THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE ARISING OUT OF ITS USE OF THE ASV PROGRAM.

10.2 PCICO MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE SUBJECT MATTER OF THIS AGREEMENT. PCICO SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITATION, PCICO SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THE PCI STANDARD AND ANY INTELLECTUAL PROPERTY RIGHTS SUBSISTING THEREIN OR ANY PART THEREOF, INCLUDING BUT NOT LIMITED TO ANY AND ALL IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, OR SUITABILITY FOR ANY PURPOSE (WHETHER OR NOT PCICO HAS BEEN ADVISED, HAS REASON TO KNOW, OR IS OTHERWISE IN FACT AWARE OF ANY INFORMATION).

10.3 In particular, without limiting the foregoing, the accuracy, completeness, sequence or timeliness of the ASV Program cannot be guaranteed. In addition, PCICo makes no representations or warranties whatsoever, expressed or implied, and assumes no liability to Vendor regarding (i) any delay or loss of use of the ASV Program, or (ii) system performance and effects on or damages to software and hardware in connection with any use of the ASV Program.

10.4 PCICo shall be liable vis-à-vis Vendor only for any direct damage incurred by Vendor as a result of PCICo's fault or negligence (contractual or extra-contractual) under this Agreement provided PCICo's aggregate liability for such direct damage under and for the duration of this Agreement will never exceed the fees paid by Vendor to PCICo under clause 2.5.

10.5 PCICo shall not be liable vis-à-vis Vendor for any other damage incurred by Vendor under this Agreement, including but not limited to, loss of business, revenue, goodwill, anticipated savings or other commercial or economic loss of any kind arising in any way out of the use of the ASV Program (regardless of whether such damages are reasonably foreseeable or PCICo has been advised of the possibility of such damages), or for any loss that results from force majeure.

11 Insurance

At all times while this Agreement is in effect, Vendor shall maintain insurance in such amounts, with such insurers, coverages, exclusions and deductibles which, at a minimum, meet the applicable insurance requirements for U.S. or European Union ASVs, as applicable, as may be required by PCICo, including without limitation the requirements set forth in Appendix D of the Validation Requirements for Approved Scanning Vendors. Vendor acknowledges and agrees that if it is a non-U.S. and non-European Union ASV, unless otherwise expressly agreed by PCICo in writing, at all times while this Agreement is in effect, Vendor shall maintain insurance in such amounts, with such insurers, coverages, exclusions and deductibles that PCICo determines, in its sole discretion, is substantially equivalent to the insurance required by PCICo for U.S. and European Union ASVs. Vendor hereby represents and warrants that it meets all applicable insurance requirements as provided for in this clause 11 and that such insurance shall not be cancelled or modified without giving PCICo at least twenty (20) days prior written notice. PCICo may modify its insurance requirements from time to time based on parameters affecting risk and financial capability that are specific to Vendor, provided that PCICo is under no obligation to review and does not undertake to advise Vendor on the adequacy of Vendor's insurance coverage.

12 Notices

All notices required under this Agreement shall be in writing and shall be deemed given when delivered personally, by overnight delivery upon written verification of receipt, by facsimile transmission upon electronic acknowledgment of receipt, or by certified or registered mail, return receipt requested, five (5) days after the date of mailing. Notices from PCICo to Vendor shall be sent to the Principal Contact and at the location set forth on the signature page of this Agreement. Notices from Vendor to PCICo shall be sent to the attention of General Manager at the address set forth on the first page of this Agreement. A Party may change its addressee and address for notices by giving notice to the other Party pursuant to this clause 12.

13 Consent to receive records electronically

13.1 Notwithstanding clause 12, either Party consents to receive electronically any documentation, notices, reports, documents, communications, or other records related to the ASV Program (hereinafter referred to individually or collectively as "Records") to be sent by the other Party. Either Party consents to receive such Records by electronic mail.

13.2 All Records provided to either Party electronically will be deemed to be "in writing." Either Party reserves the right to provide records in paper format at any time. The receiving Party agrees, however, that the Party sending such Records is not required to provide the receiving Party with Records in paper format. If the receiving Party wishes to retain a paper copy of any Records provided electronically, the receiving Party may print a copy from its computer.

14 Miscellaneous

14.1 *Entire Agreement*. The Parties agree that this Agreement, including documents incorporated herein by reference, is the exclusive statement of the agreement between the Parties with respect to the ASV Program, which supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the Parties with respect to such subject matter.

14.2 *Amendment*. This Agreement may be modified, altered or amended only (i) by written instrument duly executed by both Parties or (b) by PCICo upon thirty (30) days written notice to Vendor, provided, however, that if Vendor does not agree with such unilateral modification, alteration or amendment, Vendor shall have the right, exercisable at any time within the aforementioned thirty (30) day period, to terminate this Agreement in accordance with the provisions of clause 7.3(b)(iii)(B) upon written notice of its intention to so terminate to PCICo (regardless of the notice requirements set forth in clause 7.3(b)). Any such unilateral modification, alteration or amendment will be effective as of the end of such thirty (30) day period.

14.3 *Waiver.* The waiver or failure of either Party to exercise in any respect any right provided for in this Agreement shall not be deemed a waiver of any further right under this Agreement.

14.4 *Assignment.* This Agreement is a personal services Agreement and may not be assigned by Vendor, except with the written consent of PCICo, which consent PCICo may grant or withhold in its absolute discretion.

14.5 *Severability.* Should any individual provision of this Agreement be or become void, invalid or unenforceable, the validity of the remainder of this Agreement shall not be affected thereby and shall remain in full force and effect, in so far as the primary purpose of this Agreement is not frustrated.

14.6 *Relationship.* The Parties to this Agreement are independent contractors and neither Party shall hold itself out to be, nor shall anything in this Agreement be construed to constitute either Party as the agent, representative, employee, partner, or joint venture of the other. Neither Party may bind or obligate the other without the other Party's prior written consent.

14.7 *Remedies.* All remedies in this Agreement are cumulative, in addition to and not in lieu of any other remedies available to either Party at law or in equity, subject only to the express limitations on liabilities and remedies set forth herein.

14.8 *Dispute Settlement- Jurisdiction- Governing Law.* Any dispute in any way arising out of or in connection with the interpretation or performance of this Agreement, which cannot be amicably settled within thirty (30) days of the written notice of the dispute given to the other Party by exercising the best efforts and good faith of the Parties, shall be finally settled by the courts of Delaware (United States of America) in accordance with Delaware law without resort to its conflict of laws provisions. Each of the Parties irrevocably submits to the nonexclusive jurisdiction of the United States District Courts for the State of Delaware and the local courts of the State of Delaware and waives any objection to venue in said courts.

14.9 *Counterparts*. This Agreement may be signed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

[remainder of page intentionally left blank]

IN WITNESS WHEREOF, the Parties have executed this Agreement in two (2) original copies by their duly authorized representatives. Each Party acknowledges having received one (1) original copy.

Vendor			
Vendor Name:			
Location/Address:			
State/Province:	Country:	Postal Code:	
Principal Contact			
Person's Name:			
Direct Telephone Number:		Fax:	
Location/Address:			
State/Province:	Country:	Postal Code:	
Regions Applying For (see Appendix D):			
Vendor's Signature			
Vendor's Officer Signature ↑		*Date* ↑	
Applicant Officer Name:	Title:		

For PCI SSC Use Only:			
Effective Date:			
PCI SECURITY STANDARDS COUNCIL, LLC			
PCI SSC Officer Signature ↑			
PCI SSC Officer Name:	Title:		

Schedule 1: Fees

Vendor acknowledges and agrees that PCICo reserves the right to change the following fees from time to time in accordance with clause 2.5.

Testing stage	Observation	Scope	Fee
Initial Testing	Includes 1 Testing session	Initial registration Administrative process Test infrastructure reservation and actual Test Assessment of scan results and scan report (English version)	$10,000 USD invoiced upon Effective Date
Annual Maintenance Testing	Includes 1 Testing session	Administrative process Test infrastructure reservation and actual Test Assessment of scan results and scan report (English version)	$10,000 USD invoiced upon the date when Annual Maintenance Testing is performed
New Testing as per clauses 3.1 and 3.2	Testing of each Security Solution in case of significant changes as provided in clauses 3.1 and 3.2 Includes 1 Testing session	Administrative process Test infrastructure reservation and actual Test Assessment of scan results and scan report (English version)	$10,000 USD invoiced upon the date when New Testing is performed
Additional Testing	If during initial Testing, annual maintenance Testing and/or Testing pursuant to clauses 3.1 and 3.2, any Security Solution failed to reach satisfactory level of compliance, a maximum of 2 additional Testing sessions may be requested by Vendor	Test infrastructure reservation and actual Test Assessment of scan results and scan report (English version)	$10,000 USD invoiced upon the first additional testing request $10,000 USD invoiced upon the second and each subsequent additional testing

Any additional cost such as but not limited to translation (from English to other languages) costs should be agreed upon between the Parties.

Payment terms:

All invoices shall be payable by Vendor within thirty (30) days calculated as from the date of receipt of the invoice. Payment to PCICo should be made in US dollars (USD) by wire transfer to PCICo's bank account as mentioned on the PCICo invoice(s).

The amounts listed in this Schedule 1 do not include taxes, such as value added taxes (VAT), sales, excise, gross receipts and withholding taxes, universal service fund fee, and any similar tax or any government imposed fees or surcharges which may be applicable thereto and Vendor agrees to pay all such applicable taxes or fees, which will be invoiced to Vendor in accordance with local law. Vendor agrees to pay or reimburse PCICo for all such taxes or fees, excluding tax on PCICo's income. In respect of withholding tax, Vendor will pay such additional amounts as may be necessary, such that PCICo receives the amount it would have received had no withholding been imposed.

Schedule 2: Compliance Notification – sample

<<Date>>

<<Contact Name>>

<<Company Name>>

<<Company Address>>

Dear **<<Contact Name>>**,

We are pleased to notify you that in accordance with the PCI Scanning Vendor Compliance Test Agreement (the "Agreement") entered into between your company and PCICo, the Security Solution described below has successfully completed the Testing phase of the ASV Program and you have been certified as a PCICo-Approved Scanning Vendor ("ASV").

Security Solution:

<Name of the solution>

Successful completion of the abovementioned Testing at this date indicates that the abovementioned Security Solution (whose configuration is identified in the appendix below) complies with the current PCI Standard and that you have completed all applicable ASV requirements as of the date of this letter.

Even though you have been approved as an ASV and the abovementioned Security Solution has successfully completed PCICo Testing and is deemed to be compliant with the PCI Standard at this date, all rights and remedies resulting from your presenting yourself as an ASV or your sale, licensing, distribution or use of the abovementioned Security Solution shall be provided by your organization and not by PCICo.

Subject to your compliance with the terms and conditions of the Agreement, you are entitled to advertise your status as a "*PCICo-Approved Scanning Vendor*" and that the abovementioned Security Solution has "*successfully completed PCICo ASV Compliance Testing*" and/or that such Security Solution is "*ASV Program compliant*".

If you wish to provide for any other statements or announcements public or not, whether in writing or not, you must request PCICo's prior written approval.

The terms and conditions of the Agreement apply mutatis mutandis to this Compliance Notification.

Your ASV compliant status, and that of the abovementioned Security Solution, is effective upon dispatch of this Compliance Notification and shall remain valid as provided in the Agreement.

Because ASV compliant status is subject to various limitations, including certain events of termination, you and any third parties should confirm that such compliance status is current and has not been terminated by referring to the list of ASVs published on the PCICo web site at http://www.pcisecuritystandards.org.

Thank you for your support of the PCI Approved Scanning Vendor Compliance Test Program.

Yours Sincerely,

**********Security Solution to be identified in an appendix to this Compliance Notification**********

Appendix B. PCI ASV Application Process Checklist

This checklist is provided as a tool to help you organize the PCI Approved Scanning Vendor company application information that must be submitted along with your completed/signed PCI Approved Scanning Vendor (ASV) Compliance Test Agreement.

ASV Business Requirements

Requirement	Information/Documentation Needed
Legitimate Business Entity	☐ Copy of business license ☐ Year of incorporation ☐ Location(s) of office(s) ☐ Written statement describing any past or present allegations or convictions of any fraudulent or criminal activity involving the security company and its principles
Independence	☐ Company signature on the Agreement ☐ Description of company's practices to maintain independence.
Insurance Coverage	☐ Company signature on the Agreement ☐ Proof of insurance coverage that meets PCI SSC requirements ☐ Commercial General Liability including contractual liability with a combined single limit of liability of $1,000,000 per occurrence and ☐ Technology Errors and Omissions and Cyber-Risk Liability with a minimum limit of $2,000,000 per occurrence and annual aggregate

ASV Capability Requirements

Requirement	Information/Documentation Needed
Company Services and Experience	☐ High-level description of the security company's experience and knowledge with information security and payment system scanning engagements ☐ High-level description of the security company's experience relevant areas of specialization within information security, scanning engagements preferably related to the payment systems ☐ A description of the total number of employees, the number and specific roles of the information security employees on staff and the percentage of their time dedicated to performing PCI Scanning Services ☐ A description of the size and types of market segments in which the ASV tends to focus, such as, Fortune 500, financial industry, insurance industry, and small-medium sized business ☐ List of languages supported by the security company ☐ A description of company's practices to maintain scanning independence, including but not limited to, practices, organizational structure/separation, employee education, etc., in place to prevent conflicts of interest in a variety of scenarios ☐ Two client references from recent security engagements
Company Employee Skills and Experience	☐ Education (subject, degrees and certificates, institutions) ☐ Area(s) of expertise (network security, application security, and consultancy, system integration, auditing, special skills) with at least 1 year (total) in three separate areas ☐ Years of working experience and responsibilities ☐ Years of working experience related to payment card industry and responsibilities ☐ Résumé ☐ A description of a minimum of five years' information security experience

ASV Administrative Requirements

Requirement	Information/documentation Needed	
Contact Person—Primary and Secondary	☐ Name ☐ Title ☐ Address	☐ Phone ☐ Fax ☐ E-mail
Background Checks	☐ For each ASV employee to be qualified, statement that employee successfully completed the background check in accordance with the ASV's policies and procedures ☐ Company signature on the Agreement ☐ A description of the current ASV company personnel background check policies and procedures	
Quality Assurance	☐ A description of the quality assurance procedure that will be used forthe PCICo Technical and Operational Scanning Requirements (Report Requirements). The description should outline the security company's review process for ensuring PCICo Technical and Operational Scanning Requirements (Report Requirements) accuracy. ☐ Company signature on the Agreement	
Protection of Confidential and Sensitive Information	☐ A description of the security company's sensitive data protection handling practices, including physical, electronic, and procedural safeguards. Includes requirements and processes used to ensure employee confidentiality of customer data. ☐ Blank copy of confidentiality agreements required to be signed by employees ☐ Company signature on the Agreement	
Evidence Retention	☐ Description of the security company's evidence retention policy and procedures ☐ Company signature on the Agreement	

Appendix C. Sample ASV Feedback Form

This form is used to review ASVs and their work product, and is intended to be completed after a PCI Scanning Service by the ASV client. While the primary audience of this form are ASV scanning clients (merchants or service providers), there are several questions at the end, under "ASV Feedback Form for Payment Brands and Others," to be completed as needed by Payment Brand participants, banks, and other relevant parties.

This form can be obtained directly from the ASV during the PCI Scanning Service, or can be found online in a useable format at https://www.pcisecuritystandards.org. Please send this completed form to PCI SSC at: compliance@pcisecuritystandards.org.

ASV Feedback Form

	Client (merchant or service provider)	*Approved Scanning Vendor Company (ASV)*
Name		
Contact		
Title		
Telephone		
E-mail		

	Location of Assessment			*ASV employee who performed Assessment*	
Street				Name	
City		Country		ID number	
State/ Province		Postal Code		Telephone	
				E-mail	

For each statement, please indicate the response that best reflects your experience and provide comments.
5 = Strongly Agree 4 = Agree 3 = Neutral 2 = Disagree 1 = Strongly Disagree

Statement	Select One	Comments
1. During the initial engagement, the ASV explained the objectives, timing, and review process, and addressed your questions and concerns.	***1-5***	
2. The ASV employee(s) understood your business and technical environment, as well as the payment card industry.	***1-5***	
3. The ASV employee(s) had sufficient security and technical skills to effectively perform this PCI Scanning Service.	***1-5***	
4. The ASV sufficiently understood the PCI Data Security Standard and PCI Security Scanning Procedures.	***1-5***	

For each statement, please indicate the response that best reflects your experience and provide comments.
5 = Strongly Agree 4 = Agree 3 = Neutral 2 = Disagree 1 = Strongly Disagree

Statement	Select One	Comments
5. The ASV effectively minimized interruptions to operations and schedules.	***1-5***	
6. The ASV provided an accurate estimate for time and resources needed.	***1-5***	
7. The ASV provided an accurate estimate for scan report delivery.	***1-5***	
8. The ASV did not attempt to market products or services for your company to attain PCI compliance.	***1-5***	
9. The ASV did not imply that use of a specific brand of commercial product or service was necessary to achieve compliance.	***1-5***	
10. In situations where remediation was required, the ASV presented product and/or solution options that were not exclusive to their own product set.	***1-5***	
11. The ASV used secure transmission to send any confidential reports or data.	***1-5***	
12. The ASV demonstrated courtesy, professionalism, and a constructive and positive approach.	***1-5***	
13. There was sufficient opportunity for you to provide explanations and responses during the scans.	***1-5***	
14. During the review wrap-up, the ASV clearly communicated findings and expected next steps.	***1-5***	
15. The ASV provided sufficient follow-up to address false positives until eventual scan compliance was achieved.	***1-5***	
Please provide any additional comments here about the ASV, your PCI Scanning Service, or the PCI documents.		

ASV Feedback Form for Payment Brands and Others

	ASV Client (merchant or service provider reviewed)	*Approved Scanning Vendor (ASV)*	
Company Name			
Payment Brand Reviewer		**ASV employee who performed assessment**	
Name			
Title		Employee ID number:	
Telephone			
E-mail			

For each statement, please indicate the response that best reflects your experience and provide comments.

5 = Strongly Agree 4 = Agree 3 = Neutral 2 = Disagree 1 = Strongly Disagree

Question	Select One	Comments
1. The ASV clearly understood how to notify your payment brand about compliance and non-compliance issues, and the status of merchants and service providers.	***1-5***	
2. No complaints were received about ASV activities related to this scan.	***1-5***	
3. The ASV demonstrated sufficient understanding of the PCI Data Security Standard and the PCI Security Scanning Procedures.	***1-5***	

Appendix D. Insurance

This is the expected insurance clause and coverage for all Approved Scanning Vendor (ASV) companies, except for in those locations where such insurance coverage is not available or provided. The below limits can be written in other currencies but should be the equivalent of the limits expressed below in US dollars.

Note: For an ASV to conduct work outside their home countries, the following additional insurance coverage is required: the insurer must respond on a global basis (and particularly respond to claims brought in the U.S. if this is applicable). (Most insurance is not automatically written so that the insurer will respond to claims outside of the country and many will specifically exclude the U.S.)).

The following is a typical insurance clause and includes expected coverage:

Prior to the commencement of the Services under this Agreement, ASV shall procure the following insurance coverage, at its own expense, with respect to the performance of such remote PCI Scanning Services. Such insurance shall be issued by financially responsible and properly licensed insurance carriers in the jurisdictions where the Services are performed and rated at least A VIII by Best's Rating Guide (or otherwise acceptable to PCI SSC) and with minimum limits as set forth below. Such insurance shall be maintained in full force and effect for the duration of this Agreement and any renewals thereof:

COMMERCIAL GENERAL LIABILITY INSURANCE including PRODUCTS, COMPLETED OPERATIONS, ADVERTISING INJURY, PERSONAL INJURY and CONTRACTUAL LIABILITY INSURANCE with the following minimum limits for Bodily Injury and Property Damage on an Occurrence basis: $1,000,000 per occurrence and $2,000,000 annual aggregate.

TECHNOLOGY ERRORS & OMISSIONS, CYBER-RISK and PRIVACY LIABILITY INSURANCE covering liabilities for financial loss resulting or arising from acts, errors or omissions in rendering computer or information technology Services, or from data damage/destruction/corruption, including without limitation, failure to protect privacy, unauthorized access, unauthorized use, virus transmission, denial of service and loss of income from network security failures in connection with the Services provided under this Agreement with a minimum limit of two million dollars ($2,000,000) each claim and annual aggregate.

If any of the above insurance is written on a claims-made basis, then ASV shall maintain such insurance for two (2) years after the termination of this Agreement. Without limiting ASV's indemnification duties as outlined in the Indemnification Section herein, PCI SSC shall be named as an additional insured under the Commercial General Liability for any claims and losses arising out of, allegedly arising out of or in any way connected to the ASV's performance of the Services under this Agreement. The insurers shall agree that the ASV's insurance is primary and any insurance maintained by PCI SSC shall be excess and non-contributing to the ASV's insurance.

Prior to commencing of services under this Agreement and annually thereafter, ASV shall furnish a certificate, satisfactory to PCI SSC, from each insurance company evidencing that the above insurance is in force in compliance with the terms of this insurance section, stating policy numbers, dates of expiration and limits of liability, and further providing that ASV will endeavor to provide at least thirty (30) days prior written notice in the event the insurance is canceled. In addition to the certificate of insurance, ASV shall provide copies of the actual insurance policies if requested by PCI SSC at any time. ASV shall send Certificate(s) of

Insurance confirming such coverage according to the directions in Section 2.3 of this document. Fulfillment of obligations to procure insurance shall not otherwise relieve ASV of any liability hereunder or modify ASV obligations to indemnify PCI SSC.

In the event that ASV subcontracts or assigns any portion of the Services in this Agreement, the ASV shall require any such subcontractor to purchase and maintain insurance coverage and waiver of subrogation as required herein.

WAIVER OF SUBROGATION: ASV agrees to waive subrogation against PCI SSC for any injuries to its employees arising out of or in any way related to ASV's performance of the Service under this Agreement. Further, ASV agrees that it shall ensure that the Workers' Compensation/Employer's Liability insurers agree to waive subrogation rights, in favor of PCI SSC, for any claims arising out of or in any way connected to ASV's performance of the Services under this Agreement.