Payment Card Industry (PCI)
Data Security Standard
Qualification Requirements

For Approved Scanning Vendors (ASV)

Version 3.0
February 2017

Document Changes

Date	Version	Description
October 2008	1.2	To align version number with PCI DSS v1.2; no other changes made.
February 2011	2.0	PCI DSS Validation Requirements for Approved Scanning Vendors (ASVs) Version 2.0, this is the third release of the Validation Requirements for Approved Scanning Vendors (ASVs). Constructed and finalized by PCI SSC's Technical Working Group (TWG) and approved by the PCI SSC Executive Committee.
December 2013	2.1	Documented the remediation process and made minor changes to be consistent with v2.0 of the PCI Data Security Standards.
February 2017	3.0	▪ Updated ASV Company qualification requirements to more closely align with QSA Qualification Requirements v2.1 and other PCI SSC Program qualification requirements: ○ Updated/clarified and enhanced various terms ○ Code of Professional Responsibility ○ Updated/clarified Background checks ○ Enhanced Internal Quality Assurance requirements ○ Enhanced Protection of Confidential and Sensitive Information ○ Updated/clarified Remediation ○ Updated/clarified Revocation ○ Increased the Violation look-back period from two years to three years ▪ Updated ASV Agreement ▪ Clarified ASV Lab Scan Test failure appeal requirements ▪ Removed PCI ASV Application Process Checklist ▪ Moved previous Appendix C: Insurance to Appendix B ▪ Added Appendix C: ASV Company Application Form ▪ Added Appendix D: ASV Employee Application Form

© 2008-2017 PCI Security Standards Council, LLC

Table of Contents

© 2008-2017 PCI Security Standards Council, LLC

1 Introduction

Developed in response to requests from merchants for a unified set of payment account data security requirements, the Payment Card Industry (PCI) Data Security Standard ("PCI DSS," as further described below) is a single set of requirements for cardholder data protection across the entire industry, maintained by 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.

Organizations recognized by PCI SSC to validate adherence to the PCI DSS by performing vulnerability scans of internet facing environments of merchants and service providers as part of the PCI SSC Approved Scanning Vendor Compliance Test Program (the "ASV Program") are known as "Approved Scanning Vendor companies" or "ASV Companies" (defined below).

PCI SSC provides a variety of tools to promote the compliance of internet-facing systems with the PCI DSS, including specific requirements for vulnerability scans of merchants and service providers, and for periodic remote testing, vulnerability scanning, and/or vulnerability assessment services performed by ASV Companies as part of the ASV Program (collectively, "PCI Scanning Services," as more fully described below).

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

This document describes the necessary requirements for ASV Companies (and their ASV Employees) to be qualified by PCI SSC to perform PCI Scanning Services.

To achieve (and maintain) such qualification, ASV Companies and ASV Employees must comply with all applicable ASV Requirements, including without limitation the requirements set forth in this document.

1.1 Terminology

Throughout this document, the terms set forth in this Section 1.1 shall have the corresponding meanings appearing in the table below:

Term	Meaning
ASV Agreement	The then current version of (or successor document to) the PCI ASV Compliance Test Agreement, the current version of which is attached as Appendix A to the *ASV Qualification Requirements*.
ASV Company	A data security company that has been qualified, and continues to be qualified, by PCI SSC to use an ASV scan solution of such company appearing on the ASV List to determine compliance of its Scan Customers with the external vulnerability scanning requirement of PCI DSS Requirement 11.2.2 for ASV Program purposes.

© 2008-2017 PCI Security Standards Council, LLC

Term	Meaning
ASV Employee	An individual who is employed by an ASV Company and has satisfied, and continues to satisfy, all ASV Requirements applicable to employees of ASV Companies who will use an ASV scan solution to determine compliance of their customers with the external vulnerability scanning requirement of *PCI DSS* Requirement 11.2.2 for ASV Program purposes, as described in further detail herein.
ASV Lab Scan Test (or "Test")	The testing of a candidate or validated ASV scan solution by an ASV Validation Lab to demonstrate for ASV Program purposes whether such solution performs in accordance with the *ASV Program Guide*. The terms "Test," "Tested," and "Testing" will be interpreted accordingly.
ASV List	The then-current list of ASV Companies and corresponding ASV scan solutions published by PCI SSC on the Website.
ASV Program Guide	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Data Security Standard (DSS) Approved Scanning Vendors Program Guide*, as from time to time amended and made available on the Website.
ASV Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Approved Scanning Vendors (ASV)*, as from time to time amended and made available on the Website.
ASV Requirements	With respect to a given ASV Company or ASV Employee, the requirements and obligations thereof pursuant to the *ASV Qualification Requirements*, the ASV Agreement, the *ASV Program Guide*, each addendum, supplement, and other agreement entered into between such ASV Company or ASV Employee and PCI SSC, and any and all other policies, procedures, requirements or obligations imposed, mandated, provided for or otherwise established by PCI SSC from time to time in connection with any PCI SSC program in which such ASV Company or ASV Employee (as applicable) is then a participant, including but not limited to, ASV Lab Scan Test requirements and the requirements of all applicable PCI SSC training programs, quality assurance and remediation programs, program guides, and other related PCI SSC program materials.
ASV scan solution	A set of security services, tool(s), and processes that is offered by an ASV to validate the compliance of a Scan Customer in accordance with PCI DSS Requirement 11.2.2 and that has been and remains validated by an ASV Validation Lab in accordance with ASV program requirements. ASV scan solutions include the tools, techniques, methods, procedures, associated scan reports, processes for exchanging information between the ASV and the Scan Customer, and the processes used by ASV Employees to: ▪ Operate the ASV scan solution ▪ Review and interpret scan results, as needed ▪ Generate the scan report ▪ Submit the scan report to the Scan Customer

© 2008-2017 PCI Security Standards Council, LLC

Term	Meaning
ASV Validation Lab	An independent, third-party testing facility designated by PCI SSC for purposes of Testing candidate and validated ASV scan solutions.
PCI SSC Code of Professional Responsibility	The then-current version of (or successor documents to) the PCI SSC Code of Professional Responsibility, as from time to time amended and made available on the Website.
PCI DSS	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Data Security Standard and Security Assessment Procedures,* as from time to time amended and made available on the Website.
PCI Scanning Services (or "PCI Scan")	Remote scanning services performed by an ASV Company and ASV Employee(s), using an ASV scan solution appearing on the ASV List, for purposes of validating compliance of a Scan Customer with the external vulnerability scanning requirement of *PCI DSS* Requirement 11.2.2 for ASV Program purposes.
PCI SSC	PCI Security Standards Council, LLC.
Scan Customer	Defined in the ASV Agreement.
Testing	See definition of ASV Lab Scan Test.
Website	The then-current PCI SSC website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.

1.2 Goal

To be qualified as an ASV Company by PCI SSC, the ASV Company, its ASV Employees and ASV scan solution(s) must meet or exceed all applicable ASV Requirements, and the ASV Company must execute and have in full force and effect an ASV Agreement with PCI SSC. Companies that qualify are identified on the ASV List subject to and in accordance with the ASV Agreement.

The requirements defined in this document serve as a **qualification baseline**, and provide a transparent process for ASV Company and ASV Employee qualification and requalification for ASV Program purposes. Among other things, the ASV Company and ASV Employees must adhere to all requirements in these *ASV Qualification Requirements*, and must provide all of the required provisions described herein.

1.3 Qualification Process Overview

The ASV qualification process consists of four parts:

1. The first involves the initial qualification of the security company itself.
2. The second relates to the initial qualification of the company's employee(s) responsible for performing PCI Scanning Services.
3. The third consists of the Testing of the company's candidate and/or validated ASV scan solution(s).
4. The final step is listing the ASV Company and its validated ASV scan solution on the ASV List.

© 2008-2017 PCI Security Standards Council, LLC

All ASV Companies are identified on the ASV List. If a security company is not on this list, its work product is not recognized by PCI SSC.

In the event PCI SSC determines that an applicant does not meet ASV Program requirements, PCI SSC will notify the applicant, and the applicant may appeal within 30 days from the notice date. Appeals must be addressed to the ASV Program Manager at *asv@pcisecuritystandards.org* and provide specific details to support the appeal. If a company is unsuccessful on appeal, its name will not be placed on the ASV List.

To initiate the qualification process, the security company must submit its completed ASV Company application and signed ASV Agreement (in unmodified form) to PCI SSC. All information provided to PCI SSC to support the ASV Program application process must be accurate and complete as of the date of its submission.

1.4 Document Structure

This document defines the minimum set of requirements a security company must satisfy to become and maintain Good Standing (defined in the ASV Agreement) as an ASV Company. The document is structured in five sections as follows.

Section 1: **Introduction** offers a high-level overview of the ASV Program application 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 two of its employees.

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

Section 5: **ASV List and Annual Requalification** briefly outlines the annual requalification process, as well as remediation and revocation procedures for ASV Companies and ASV Employees) failing to satisfy applicable ASV Requirements.

1.5 Related Publications

This document should be used in conjunction with the current publically available versions of the following other PCI SSC publications (or successor documents), each available through the PCI SSC web site:

- *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*
- *Payment Card Industry (PCI) Approved Scanning Vendors Program Guide*
- *PCI Security Standards Council (PCI SSC) Code of Professional Responsibility*
- *Payment Card Industry (PCI) Continuing Professional Education (CPE) Maintenance Guide*

© 2008-2017 PCI Security Standards Council, LLC

1.6 ASV Application Process

This document describes the information that must be provided to PCI SSC as part of the application and qualification 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.

All application materials (see Appendices C and D) and the signed ASV Agreement must be submitted in English. The ASV Agreement is binding in English even if the ASV Agreement was translated and reviewed in another language. All other documentation provided to PCI SSC by the ASV Company (or applicant) in a language other than English must be accompanied by a certified English translation (examples include business licenses and insurance certificates).

All application packages must include a signed ASV Agreement and the required documentation. Completed application packages must be submitted either by e-mail to the ASV Program Manager at *asv@pcisecuritystandards.org* or via postal mail to the following address:

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

Note: *PCI SSC reserves the right to reject any application from any applicant (company or employee) that PCI SSC determines has committed, within three (3) years prior to the application date, any conduct that would have been considered a "Violation" (see Section 5.4 below) if committed by an ASV Company or ASV Employee. The period of ineligibility will be a minimum of one (1) year, as determined by PCI SSC in a reasonable and non-discriminatory manner.*

1.7 Additional Information Requests

In an effort to maintain the integrity of the ASV Program, PCI SSC may from time to time request that ASV Companies and/or ASV Employees submit additional information or materials in order to demonstrate adherence to applicable requirements or as part of the qualification or requalification process. All such additional information and materials must be submitted in English or with a certified English translation. ASV Companies are required to respond to each such request with the requested information or documentation no later than three (3) weeks from receipt of the corresponding written request.

© 2008-2017 PCI Security Standards Council, LLC

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 Company (or applicant, as applicable) must be recognized as a legal entity.

2.1.2 Provisions

The following information must be provided to PCI SSC (see Appendix C: ASV Company Application):

- Copy of current ASV Company (or applicant, as applicable) organizational document or equivalent approved by PCI SSC (the "Business License"), including year of incorporation and location(s) of offices (see the Website – Business License Requirements)
- Written statements describing any past or present allegations or convictions of any fraudulent or criminal activity involving the ASV Company (or applicant, as applicable) or any of its principals, and the status and resolution thereof

2.2 Independence

2.2.1 Requirement

Each ASV Company 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.

Each ASV Company (and applicant, as applicable) must have a code of conduct policy, and provide this code of conduct policy to PCI SSC upon request.

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

Note: *The ASV Company's code of conduct policy must support—and never contradict—the* PCI SSC Code of Professional Responsibility.

- The ASV Company must not undertake to perform PCI Scanning Services of entities that it controls or entities that it is controlled by or with which it is under common control or in which it holds any investment.
- The ASV Company and its employees must (and will) not have offered, been offered, provided or received any gift, gratuity, service, or other inducement to any employee of PCI SSC, or to any actual or proposed Scan Customer, in order to enter into the ASV Agreement or any agreement with such Scan Customer, or to provide any ASV Program-related services.
- The ASV Company must fully disclose to the applicable Scan Customer in a separate document attached to each applicable scan report for that Scan Customer, if that Scan Customer uses any security-related device, application, solution, or service that has been developed or manufactured by the ASV Company, or to which the ASV Company owns any right, or that the ASV Company has configured or manages, including any of the following:

© 2008-2017 PCI Security Standards Council, LLC

- Application or network firewalls
- Intrusion detection/prevention systems
- Database or other storage solutions
- Encryption solutions
- Security audit log or log-management solutions
- File integrity monitoring solutions
- Anti-virus solutions

- The ASV Company must have separation of duties controls in place to ensure ASV Employees conducting PCI Scans are independent and not subject to any conflict of interest, including consulting services.
- The ASV Company must notify its ASV Employees of the independence requirements provided for in this document, as well as the ASV Company's independence policy, at least annually.
- The ASV Company agrees that when the ASV Company recommends remediation actions that include one of its own solutions or products, the ASV Company will also recommend other market options that exist.
- The ASV Company agrees that it will not use its status as an ASV Company to market services unnecessary to bring Scan Customers into compliance with the PCI DSS or any other PCI SSC Standard.
- The ASV Company must not, and agrees that it will not, misrepresent any requirement of the PCI DSS or any other PCI SSC Standard in connection with its promotion or sales of services to actual or proposed Scan Customers, or state or imply that the PCI DSS or any other PCI SSC Standard requires use of the ASV Company's products or services.

2.2.2 Provisions

The ASV Company (and/or applicant, as applicable) must attest to having and adhering to company practices to maintain scanning independence (see Appendix C: ASV Company Application) including but not limited to practices, organizational structure, separation of duties, and employee education in place to prevent conflicts of interest.

2.3 Insurance Coverage

2.3.1 Requirement

At all times while its ASV Agreement is in effect, the ASV Company shall maintain such insurance, coverage, exclusions, and deductibles with such insurers as PCI SSC may reasonably request or require to adequately insure the ASV Company for its obligations and liabilities under the ASV Agreement, including without limitation, the ASV Company's indemnification obligations.

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

2.3.2 Provisions

© 2008-2017 PCI Security Standards Council, LLC

The ASV Company (and/or applicant, as applicable) must provide a proof of coverage statement to PCI SSC to show that insurance coverage matches PCI SSC requirements and locally set insurance coverage requirements.

2.4 ASV Program Fees

2.4.1 Requirement

Fees payable by each ASV Company (and/or applicant, as applicable) in connection with the ASV Program ("ASV Program Fees") include (without limitation) the following:

- An ASV scan solution test fee for each ASV Lab
- Scan Test performed for a candidate ASV scan solution.
- ASV Employee training fees for each ASV Employee (or applicant, as applicable) registered for such training.
- Annual ASV Program requalification fees for subsequent years, which include fees for annual ASV Lab Scan Testing of each candidate and/or validated ASV scan solution and ASV Employee annual requalification training fees.

Note: *All ASV Program Fees are specified on the Website (see PCI SSC Programs Fee Schedule) and are subject to change.*

ASV scan solution test fees (initial and requalification) are due within 30 days of notice from PCI SSC.

Instructions for enrolling in applicable training are provided by PCI SSC. Each ASV Company applicant must enroll at least two ASV Employee candidates in training, and must pay associated initial training fees once the application is approved. Training fees for requalification are paid as part of the requalification training registration process.

Payment remittance details are included in the invoice that the applicant ASV Company receives from PCI SSC.

2.5 ASV Agreement

2.5.1 Requirement

PCI SSC requires that an ASV Agreement between PCI SSC and the applicant ASV Company be signed by a duly authorized officer of the applicant ASV Company, and submitted to PCI SSC in unmodified form with the completed ASV application package.

The ASV Agreement requires, among other things, that the ASV Company and its ASV Employees comply with all applicable ASV Requirements.

© 2008-2017 PCI Security Standards Council, LLC

3 ASV Capability Requirements

This section describes the minimum ASV Program capability requirements and related documentation that each applicant or qualified ASV Company and ASV Employees must provide to PCI SSC in order to demonstrate requisite information security vulnerability assessment expertise, work history, and industry experience.

3.1 ASV Company – Services and Experience

3.1.1 Requirement

Each ASV Company must:

- Possess information security/vulnerability scanning assessment experience similar to the PCI Scanning Services.
- Have a dedicated security practice that includes staff with specific job functions that support the information security/vulnerability scanning practice.
- At all times have at least two ASV Employees performing or managing PCI Scanning Services.

3.1.2 Provisions

The following information must be provided to PCI SSC by the applicant ASV Company (see Appendix C: ASV Company Application):

- Description of the applicant ASV Company's experience and knowledge with information security vulnerability assessment engagements including penetration testing, preferably related to payment systems
- Description of the applicant ASV Company's relevant areas of specialization within information security (for example, network security, database and application security, and incident response)
- Brief description of other core business offerings
- Description of size and types of market segments in which the applicant ASV Company tends to focus, such as Fortune 500, financial industry, insurance industry, or small-medium sized businesses
- List of languages supported by the applicant ASV Company
- Contact information for two client references from security engagements performed by the applicant ASV Company within the last 12 months

© 2008-2017 PCI Security Standards Council, LLC

3.2 ASV Employee – Skills and Experience

At least two ASV Employees performing or managing PCI Scanning Services must be qualified by PCI SSC for each ASV Company. ASV Employees are responsible for performance of the PCI Scanning Services in accordance with the *ASV Program Guide*.

3.2.1 Requirement

Each ASV Employee(s) performing or managing PCI Scanning Services must satisfy the following requirements:

- Pass background checks required per Section 4.2.
- Possess sufficient information security knowledge and experience to conduct PCI Scanning Services using the ASV scan solution.
- Demonstrate sufficient knowledge about the PCI DSS and the ASV Program by attending annual training provided by PCI SSC, and legitimately pass—of his or her own accord without any unauthorized assistance—the ASV Program training examination.

  Note: *If an ASV Employee (or applicant) fails to pass any exam in connection with such training, the ASV Employee (or applicant) must not perform or manage PCI Scanning Services until successfully passing all required ASV Program training exams on a future attempt.*

- Possess EACH of the following:
  - A minimum of one (1) year of experience in vulnerability scanning and/or penetration testing
  - A minimum of one (1) year of experience in at least two (2) of the following areas of expertise (for a total of at least two (2) years' experience overall across the following four (4) disciplines):
    - Network security
    - Application security
    - Computer systems security
    - IT security auditing and risk assessment
- Possess ONE of the following:
  - A current industry-recognized security certification such as CISA, CISM, CISSP

    OR
  - An additional two (2) years of experience in at least two (2) of the following areas of expertise (for a total of at least two (2) additional years' experience overall across the following four (4) disciplines):
    - Network security
    - Application security
    - Computer systems security
    - IT security auditing and risk assessment
- Adhere to the ASV Company's documented process for protection of confidential and sensitive information.
- Adhere to the PCI SSC Code of Professional Responsibility.

© 2008-2017 PCI Security Standards Council, LLC

3.2.2 Provisions

The following must be provided to PCI SSC for each individual to be considered for qualification as an ASV Employee:

- A record of working experience and responsibilities outlined in Section 3.2.1 above, by completing and submitting Appendix D: ASV Employee Application for each applicant ASV Employee; and
- Résumé or curriculum vitae (CV) of each applicant ASV Employee.

3.3 Code of Professional Responsibility

3.3.1 Requirement

PCI SSC has adopted a Code of Professional Responsibility (the "Code"), available on the Website, to help ensure that all ASV Companies and ASV Employees adhere to high standards of ethical and professional conduct. All ASV Companies and ASV Employees must advocate, adhere to, and support the Code.

© 2008-2017 PCI Security Standards Council, LLC

4 ASV Company Administrative Requirements

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

4.1 Contact Person

4.1.1 Requirement

The ASV Company (or applicant, as applicable) 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 (see Appendix C: ASV Company Application):

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

4.2 Background Checks

4.2.1 Requirement

Each ASV Company must perform background checks that satisfy the provisions described below (to the extent legally permitted within the applicable jurisdiction) with respect to each applicant ASV Employee.

Major offenses—for example, felonies or non-US equivalents—may disqualify an applicant from qualifying as an ASV Employee. Minor offenses—such as misdemeanors or non-US equivalents—are allowed. Upon request, each ASV Company must provide to PCI SSC the background check history for each ASV Employee (or applicant ASV Employee), to the extent legally permitted within the applicable jurisdiction.

Note: *PCI SSC reserves the right to decline or reject any application or applicant ASV Employee.*

4.2.2 Provisions

The ASV Company (or applicant ASV Company) must provide PCI SSC with responses to each of the following (see Appendix C: ASV Company Application):

- Attestation that its policies and hiring procedures include performing background checks: Examples of background checks include previous employment history, criminal record, credit history, and reference checks.
- Attestation that it successfully completed such background checks for each applicant ASV Employee.
- A summary description of current ASV personnel background check policies and procedures, which must require and include the following:
  - Verification of aliases (when applicable)

© 2008-2017 PCI Security Standards Council, LLC

- Comprehensive country and (if applicable) state-level review of records of any criminal activity such as felony (or non-US equivalent) convictions or outstanding warrants, within the past five (5) years minimum.
- Annual background checks consistent with this section for each of its ASV Employees for any change in criminal records, arrests or convictions.

4.3 Internal Quality Assurance

Each ASV Company must have an implemented quality assurance (QA) process, documented in a QA manual that includes a description of the controls for QA reviewing of processes, documentation, and controls to maintain the integrity of the ASV's scan solution, including the scanning tools and methods used as part of the ASV scan solution. All ASV scan reports must be prepared in accordance with the procedures documented in the *ASV Program Guide.* For each PCI Scan, the resulting ASV scan report must follow the most current ASV Scan Report templates available in Appendices B and C of the *ASV Program Guide*. Each ASV scan report must be accompanied by an Attestation of Scan Compliance in the form then available in Appendix A of the *ASV Program Guide*, which summarizes whether the Scan Customer meets the requirements of PCI DSS Requirement 11.2.2.

4.3.1 Requirement

- Each ASV Company must adhere to all PCI SSC quality assurance requirements (which includes ASV Program quality assurance requirements described in this document or otherwise established by PCI SSC from time to time).
- Each ASV Company's must have and adhere to a change management policy and processes for changes to the ASV scan solution.
- Each ASV Company must maintain and adhere to a documented quality assurance process and manual, which includes all of the following:
  - Requirement to document its PCI Scanning Services and a description of the review process for generating scan reports in accordance with the requirements of the *ASV Program Guide,* including at least the following:
    - Reviews of scanning procedures, scan reports, and supporting documentation, and additional information required pursuant to the ASV Program Guide related to the appropriate selection of system components
    - Requirement that all ASV Employees must adhere to the ASV Program Guide
    - Requirement that the ASV Company (or applicant) has and shall keep in place controls to maintain the integrity of its ASV scan solution. Each ASV scan solution must:
      - Be protected from unauthorized access.
      - Adhere to the ASV Company's change management policy and processes for changes to the ASV scan solution.
      - Be monitored or able to produce alerts when changes are made.
      - Ensure the ASV Company's systems cannot be used to gain unauthorized access to a Scan Customer's environment.
  - A resource planning process for PCI Scanning Services which includes:
    - onboarding requirements for ASV Employees, résumés and current skill sets for ASV Employees, and a process for ongoing training, monitoring,

© 2008-2017 PCI Security Standards Council, LLC

and evaluation of ASV Employees to ensure their skill sets stay current and relevant for PCI Scanning Services

- Descriptions of all job functions and responsibilities within the ASV Company relating to its status and obligations as an ASV Company
- Identification of QA manual process owner
- Requirements for handling and retention of evidence associated with PCI Scanning Services (defined in the ASV Agreement; see also Section 4.5 for specific evidence-retention policy requirements and specifications)
- Distribution and availability of the QA manual
- Evidence of annual review by the QA manual process owner
- Coverage of all activities relevant to the particular and applicable PCI SSC Program, and references to the corresponding PCI SSC Qualification Requirements for that program (as applicable) and to other applicable PCI SSC Program documentation for information concerning other PCI SSC Program-specific requirements
- Requirement for all ASV Employees to regularly monitor the Website for updates, guidance, and new publications relating to the ASV Program

- Each ASV Company must inform each Scan Customer of the ASV Feedback Form (available on the Website) at the completion of the corresponding PCI Scanning Services engagement
- PCI SSC, at its sole discretion, reserves the right to conduct audits of the ASV Company at any time and further reserves the right to conduct site visits at the expense of the ASV Company
- Upon request, the ASV Company (or applicant) must provide a complete copy of the quality assurance manual to PCI SSC

4.3.2 Provisions

The applicant ASV Company must provide a completed version of Appendix C: ASV Company Application to PCI SSC.

4.4 Protection of Confidential and Sensitive Information

4.4.1 Requirement

Each ASV Company must maintain the privacy and confidentiality of information obtained in the course of performing its duties and obligations as an ASV Company, unless (and to the extent) disclosure is required by legal authority or pursuant to the ASV Agreement.

Each ASV Company must have a policy and adhere to a documented process for protection of confidential and sensitive information. This must include a confidentiality agreement signed by each ASV Employee as well as adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect confidential and sensitive information against any threats or unauthorized access during storage, processing, and/or communicating of this information. ASV Employees must acknowledge and agree to adhere to the policy.

.

© 2008-2017 PCI Security Standards Council, LLC

4.4.2 Provisions

The ASV Company (or applicant) must attest that its documented process for protection of confidential and sensitive information includes the following (see Appendix C: ASV Company Application):

- Physical, electronic, and procedural safeguards including:
  - Systems storing customer data do not reside on Internet-accessible systems
  - Protection of systems storing customer data by network and application layer controls including technologies such as firewall(s) and IDS/IPS
  - Restricting access (e.g., via locks) to the physical office space
  - Restricting access (e.g., via locked file cabinets) to paper files
  - Restricting logical access to electronic files via least-privilege/role-based access control
  - Strong encryption of Scan Customer data when transmitted over public networks
  - Secure transport and storage of backup media
  - Strong encryption of Scan Customer data on portable devices such as laptops and removable media
- Upon PCI SSC request, a copy of the ASV Company's (or applicant's) template confidentiality agreement that each ASV Employee is required to sign

4.5 Evidence Retention

4.5.1 Requirements

Each ASV Company must securely maintain digital and/or hard copies of all case logs, scanning results, work papers, notes and any other technical information created and/or obtained in connection with its PCI Scanning Services for a minimum of three (3) years, and make the foregoing available to PCI SSC and/or its affiliates upon PCI SSC's request during such time period.

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

Each ASV Company (or applicant) must provide a copy of its evidence-retention policy and procedures to PCI SSC upon request.

4.5.2 Provisions

A description of the ASV Company's (or applicant's) evidence-retention policy and procedures that covers the foregoing evidence-retention requirements must be provided to PCI SSC upon request (see Appendix C: ASV Company Application).

© 2008-2017 PCI Security Standards Council, LLC

5 ASV List and Annual Requalification

This section describes the process after initial qualification, and activities related to annual ASV Company and ASV Employee requalification.

5.1 ASV List

Once a company has met all requirements for initial ASV Company qualification, PCI SSC will add the ASV Company to the ASV List. Only companies on the ASV List are authorized by PCI SSC to perform PCI Scanning Services.

If, at any time, an ASV Company and/or ASV Employee does not meet the applicable ASV Requirements, PCI SSC reserves the right to immediately revoke the corresponding ASV Company or ASV Employee qualification ("Revocation," further defined in the ASV Agreement), and as part of such Revocation, remove the ASV Company/Employee from the ASV List (as applicable), regardless of prior warning or Remediation. Refer to Sections 5.3 and 5.4 below for additional information relating to Remediation and Revocation.

PCI SSC will notify the ASV Company of its removal from the ASV List, typically via registered or overnight mail and/or e-mail.

5.2 ASV Annual Requalification

5.2.1 Requirements

All ASV Companies and ASV Employees must be requalified by PCI SSC on an annual basis, based on the ASV Company's or ASV Employee's original qualification date as applicable. Requalification by PCI SSC is subject to timely payment of annual fees, proof of attendance at all required training, achieving passing results on required annual ASV Lab Scan Tests, and satisfactory feedback from the ASV Company's Scan Customers (the merchants or service providers that receive PCI Scanning Services) to PCI SSC.

5.2.2 Provisions

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

- Proof of information systems vulnerability assessment training within the last 12 months in accordance with the *CPE Maintenance Guide,* available on the Website. This is in addition to training provided by PCI SSC
- Successful completion of required annual ASV Lab Scan Test
- Payment of annual ASV Program Fees

© 2008-2017 PCI Security Standards Council, LLC

5.3 ASV Remediation

ASV Companies that do not meet all applicable ASV Requirements may be offered the opportunity to participate in PCI SSC's ASV Company Quality Remediation program ("Remediation").

Without limiting the foregoing, failure to meet any of the ASV Requirements, including without limitation, timely submission of annual requalification fees, satisfaction of annual training or Continuing Professional Education (CPE) requirements, or successful completion of required annual ASV Lab Scan Test, is grounds for Remediation.

ASV Companies that participate in Remediation and resolve all open issue(s) to PCI SSC's satisfaction within the applicable time period—typically ninety (90) calendar days, except as provided in the next paragraph—established as part of the Remediation process (the "Remediation Period") are returned to Good Standing. ASV Companies that fail to resolve such issues within the applicable Remediation Period are Revoked, and accordingly, removed from the ASV List (see Section 5.4 below).

5.3.1 Failure to pass the Annual ASV Lab Scan Test

Notwithstanding the foregoing, an ASV Company that fails to satisfactorily complete the annual ASV Lab Scan Test within thirty (30) calendar days past its requalification date will be offered the opportunity to participate in Remediation, and the corresponding Remediation Period will end no later than ninety (90) calendar days past that requalification date. Accordingly, ASV Companies are strongly encouraged to begin the process of requalification at least 60 days prior to their requalification date.

Note: *When an ASV Company qualifies for Remediation, its Primary Contact (designated in accordance with the ASV Agreement) will be notified and its listing on the ASV List will appear in red. The Remediation Statement on the Website affirms the Council's position on Remediation, and any external queries about an ASV Company's status will be directed to the ASV Company in question.*

ASV Companies in Remediation may continue to perform PCI Scanning Services for which they are qualified by PCI SSC unless otherwise instructed by PCI SSC in connection with the Remediation process.

5.3.2 Unfavorable feedback

Unfavorable feedback is handled on a case-by-case basis and may result in Remediation.

5.4 ASV Revocation

Each of the events below is an example of a "Violation" (as defined in the ASV Agreement) and, accordingly, regardless of prior warning or Remediation, may result in immediate Revocation of ASV Company and/or ASV Employee qualification (including removal of the ASV Company from the ASV List) and/or termination of the ASV Agreement. This list is not exhaustive. Among other things, ASV Company and/or ASV Employee qualification may be revoked if PCI SSC determines that the ASV Company or any of its ASV Employees has breached any provision of the ASV Agreement or otherwise failed to satisfy any applicable ASV Requirement (each also a Violation), including but not limited to:

- Failure to meet applicable PCI SSC Program quality standards or comply with applicable ASV Requirements
- Failure to pass the annual ASV Lab Scan Test within ninety (90) calendar days past the applicable requalification date (see additional information below)

© 2008-2017 PCI Security Standards Council, LLC

- Failure to pay applicable PCI SSC Program fees
- Failure to meet applicable PCI SSC Program training requirements (annual or otherwise)
- Failure to meet applicable PCI SSC Program continuing education requirements
- Failure to provide quality services, based on customer feedback or evaluation by PCI SSC or its affiliates
- Failure to maintain applicable PCI SSC Program insurance requirements
- Failure to comply with or validate compliance in accordance with applicable Program Qualification Requirements (defined in the ASV Agreement), PCI SSC Standards or program guides, or the terms of the ASV Agreement or supplements or addenda thereto
- Failure to maintain physical, electronic, or procedural safeguards to protect confidential or sensitive information
- Failure to report unauthorized access to any system storing confidential or sensitive information
- Engaging in unprofessional or unethical business conduct, including without limitation, improper use of third-party work product in ASV scan reports
- Failure to adhere to the PCI SSC Code of Professional Responsibility
- Failure to comply with any provision or obligation regarding non-disclosure or use of confidential information or materials
- Cheating on any exam in connection with PCI SSC Program training; submitting exam work in connection with PCI SSC Program training that is not the work of the individual applicant taking the exam; theft of or unauthorized access to PCI SSC Program exam content; use of an alternate, stand-in or proxy during any PCI SSC Program exam; use of any prohibited or unauthorized materials, notes, or computer programs during any such exam; or providing or communicating in any way any unauthorized information to another person, device, or other resource during any PCI SSC Program exam
- Providing false or intentionally incomplete or misleading information to the Council in any application or other materials
- Failure to be in Good Standing (as defined in the ASV Agreement) as an ASV Company or to be in Good Standing (as defined in the applicable Program Qualification Requirements) with respect to any other PCI SSC qualification then held by such ASV Company or ASV Employee (as applicable), in each case including but not limited to failure to successfully complete applicable quality assurance audits and/or comply with all applicable requirements, policies, and procedures of PCI SSC's quality assurance, remediation, and oversight programs and initiatives as established or imposed from time to time by PCI SSC in its sole discretion
- Failure to promptly notify PCI SSC of any event described above that occurred within three (3) years of the ASV Company's or ASV Employee's initial qualification date

ASV Company Revocation will result in immediate removal from the ASV List and notification that the company is no longer an ASV Company or recognized by PCI SSC to perform PCI Scanning Services.

© 2008-2017 PCI Security Standards Council, LLC

ASV Company Revocation is subject to appeal in accordance with the ASV Agreement. Subject to successful appeal, and except as specified in Section 5.4.1, "Failure to pass the Annual ASV Lab Scan Test," below, each Revoked ASV Company that desires to be reinstated must: (a) wait six (6) months from the notice of Revocation before re-applying to the ASV Program and (b) when re-applying, complete and submit a new ASV Company application.

5.4.1 Failure to pass the Annual ASV Lab Scan Test

ASV Companies that do not pass the annual ASV Lab Scan Test within ninety (90) calendar days past the applicable requalification date will be Revoked, notified accordingly, and removed from the ASV List. Notwithstanding the foregoing, an ASV Company that has been Revoked *solely* because it did not pass the annual ASV Lab Scan Test within ninety (90) calendar days past the applicable requalification date may be restored as an ASV Company and reinstated on the ASV List, without submitting a new ASV Company application, if it meets the following criteria within 120 calendar days past the applicable requalification date:

(i) successfully passes the ASV Lab Scan Test; (ii) submits a written request to PCI SSC requesting reinstatement as an ASV Company, identifying the ASV Validation Lab and date of the corresponding passed ASV Lab Scan Test; and (iii) meets all other ASV Requirements at the time of such request.

The following table summarizes the actions that occur at the indicated calendar days past the requalification date as a result of failure to timely pass the annual ASV Lab Scan Test.

Number of days past requalification date	Action
30	**Remediation:** ASV Company listing turns red on the ASV List.
90	**Revocation:** Company's listing is removed from the ASV List; Company no longer qualified by PCI SSC to perform PCI Scanning Services.
120	**Abbreviated reinstatement ends:** Company's ability to be reinstated after successful completion of annual ASV Lab Scan Test but without submitting new ASV Company application ends.

© 2008-2017 PCI Security Standards Council, LLC

Appendix A: PCI ASV Compliance Test Agreement

A.1 Introduction

This document (the "Agreement") is an agreement between PCI Security Standards Council, LLC ("PCI SSC") and the undersigned vendor company ("Vendor"), regarding Vendor's qualification and designation to perform the Services (as defined in this document). PCI SSC and Vendor are each sometimes referred in this document as a "party" and collectively as the "parties". Effective upon the date both parties have signed below (the "Effective Date"), for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, Vendor and PCI SSC agree to the terms and conditions set forth in this Agreement.

A.2 General Information

Vendor Company					
Company Name:					
Business Address:		City:			
State/Province:		Country:		Postal Code:	
Primary Contact					
Name:		Job Title:			
Direct Telephone Number:		E-mail:			
Location:		Fax:			
Secondary Contact					
Name:		Job Title:			
Direct Telephone Number:		E-mail:			
Location:		Fax:			
Vendor Company Officer					
Vendor Officer Name:		Job Title:			
Vendor's Officer Signature ↑			*Date* ↑		
PCI SSC					
Name:					
Job Title:					
PCI SSC Signature ↑			*Date* ↑		

© 2008-2017 PCI Security Standards Council, LLC

A.3 Terms and Conditions

A.3.1 Vendor Services

Subject to the terms and conditions of this Agreement, while Vendor is in Good Standing (defined in Section A.5.1(a) below) as an ASV Company or in compliance with Remediation, PCI SSC hereby approves Vendor to perform PCI Scanning Services of merchants, service providers and other Scan Customers, in accordance with applicable ASV Requirements, using those of Vendor's ASV scan solutions that then appear on the ASV List. For purposes of this Agreement: (i) such PCI Scanning Services, collectively with all other services provided by Vendor to PCI SSC, Scan Customers or others in connection with this Agreement or the ASV Program, are referred to herein as the "Services"; (ii) "Scan Customer" means any person or entity for which an ASV Company performs PCI Scanning Services, including without limitation, any member financial institution of a Participating Payment Brand (each a "Financial Institution"), issuer of Participating Payment Brand payment cards (each an "Issuer"), merchant authorized to accept any Participating Payment Brand 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"); (iii) "*ASV Qualification Requirements*" means the most current version of (or successor document to) the *Payment Card Industry (PCI) Data Security Standard Qualification Requirements for Approved Scanning Vendors (ASV)* document as available through the Website, as may be amended from time to time in PCI SSC's discretion, including without limitation, any and all additional supplements or addenda thereto which are applicable to Vendor as a result of its participation in the ASV Program and related approved scanning vendor initiatives operated by PCI SSC (each of which initiatives is hereby deemed to be included within the meaning of the term "ASV Program" for purposes of this Agreement); (iv) "Compliance Notification" means a letter or electronic correspondence in the form attached as Schedule 1 hereto (or in such other form as PCI SSC may approve from time to time); (v) "Member" means an entity that 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 "Member"); (vi) "Participating Payment Brand" means a payment card brand (or affiliate thereof) that is then a Member and owner of PCI SSC; and (vii) all capitalized terms used in this Agreement without definition shall have the meanings ascribed to them in the *ASV Qualification Requirements* or *ASV Program Guide*, as applicable. The *ASV Qualification Requirements*, *ASV Program Guide* and Compliance Notification are each hereby incorporated into and made a part of this Agreement by reference, and Vendor acknowledges and agrees that it has reviewed the current versions of the foregoing.

Vendor acknowledges that data security practices exist within a rapidly changing environment and agrees to monitor the Website at least weekly for changes to the PCI DSS, other PCI SSC standards relevant to the ASV Program (collectively with the PCI DSS, "PCI SSC Standards"), *ASV Qualification Requirements*, *ASV Program Guide* and other ASV Program-related Website content (the foregoing, collectively, the "*ASV Program Materials*"). Vendor will incorporate all such changes into all PCI Scanning Services initiated on or after the effective date of such changes.

© 2008-2017 PCI Security Standards Council, LLC

A.3.2 ASV Requirements; Performance of Services

Vendor agrees to comply with all ASV Requirements, including without limitation, Vendor's responsibilities and obligations pursuant to this Agreement, all ASV Program quality assurance and Remediation requirements, and all other requirements applicable to ASV Companies pursuant to the *ASV Program Materials*. Vendor warrants, represents and agrees that it will only perform PCI Scanning Services for which is has been and is at the time qualified by PCI SSC, and that it will perform all such PCI Scanning Services in strict compliance with the then applicable *ASV Program Materials*, using only those of its ASV scan solutions then appearing on the ASV List. Vendor shall provide all reasonable assistance to PCI SSC and its contractors and agents as may be needed for the purpose of Testing and the ASV Program.

A.3.3 Vendor Service Staffing

Without limiting the foregoing, Vendor agrees to comply with all requirements of, make all provisions provided for in, and ensure that its ASV Employees comply with all applicable ASV Requirements relating to employees, including but not limited to all requirements and provisions regarding employee background checks pursuant to the *ASV Qualification Requirements*. Vendor hereby represents, warrants and agrees that it has (and will have) obtained all required consents to all such background checks from each employee now or in the future performing any of the Services on Vendor's behalf hereunder, prior to such employee performing such Services. Additionally, Vendor shall ensure that an ASV Employee that is fully qualified in accordance with all applicable ASV Requirements supervises all aspects of the PCI Scanning Services performed for each Scan Customer, including without limitation, reviewing the work product that supports Vendor's PCI Scanning Services procedures and ensuring adherence to all applicable ASV Requirements and PCI SSC Standards. Vendor hereby designates the individual identified as the "Primary Contact" in Section A.2 above as Vendor's primary point of contact and "Primary Contact" for purposes of the ASV Program and this Agreement. Vendor may change its Primary Contact at any time upon written notice to PCI SSC, and hereby represents that each Primary Contact shall have authority to make and execute any and all decisions on Vendor's behalf concerning ASV Program matters.

A.3.4 Accuracy of Information

Vendor represents, warrants and agrees that, to the best of Vendor's ability to determine, all information provided or to be provided to PCI SSC in connection with this Agreement, Testing and/or Vendor's participation in the ASV Program and any other program provided or operated by PCI SSC (each a "PCI SSC Program") has been and shall be accurate and complete as of the date such information is provided. In the event of any change as a result of which any such information is no longer accurate or complete (including but not limited to any change in Vendor's circumstances or compliance with applicable ASV Requirements), Vendor shall promptly (and in any event within thirty (30) days after such change) notify PCI SSC of such change and provide such information as may be necessary to ensure that the information PCI SSC has received is then accurate and complete.

© 2008-2017 PCI Security Standards Council, LLC

A.3.5 ASV Lab Scan Testing

Vendor acknowledges and agrees as follows:

(a) In connection with Vendor's performance of PCI Scanning Services, it shall only advertise, offer, or use those of its ASV scan solutions that have been successfully Tested and qualified by (or on behalf of) PCI SSC, have received a corresponding Compliance Notification that has not been revoked, cancelled, expired or terminated, and appear on the ASV List throughout the course of the corresponding PCI Scanning Services engagement. PCI SSC shall have no obligation with respect to Vendor or any candidate or validated ASV scan solution having not successfully completed Testing other than informing Vendor that Vendor (or the applicable candidate or validated ASV scan solution) is not compliant with the PCI DSS by sending a non-compliance notification to Vendor.

(b) Even though an ASV scan solution has received a Compliance Notification, all ASV scan solutions are subject to successful completion of annual maintenance Testing for ASV Program purposes, including but not limited to, successful completion of assessment of capabilities for identifying newly reported public domain vulnerabilities. Vendor shall submit each of its ASV scan solutions appearing on the ASV List for such annual Testing within three (3) months of PCI SSC's notification or request.

(c) Vendor shall immediately notify PCI SSC of each significant or material change in any of its ASV scan solutions appearing on the ASV List, and PCI SSC may in its sole discretion (i) determine that such ASV scan solution is deemed to remain compliant with the PCI DSS by sending a new Compliance Notification or (ii) require Vendor pursuant to a non-compliance notification to (A) resubmit a modified ASV scan solution for a new Testing within one (1) month of receipt by PCI SSC of such notice and (B) pay all applicable Fees (defined below) for such new Testing.

(d) Notwithstanding the preceding paragraph, if at any time PCI SSC determines that an ASV scan solution is no longer compliant with the PCI DSS or otherwise fails to adequately protect cardholder data, PCI SSC shall be entitled to take such action as PCI SSC deems appropriate under the circumstances pursuant to the *ASV Program Materials*, including without limitation: (i) removing such ASV scan solution from the ASV List, (ii) annotating its listing on the ASV List to indicate current qualification and/or compliance status and/or (iii) requiring Vendor to resubmit such ASV scan solution for new Testing within three (3) months of such request from PCI SSC and subject to Vendor's payment of all applicable Fees.

(e) Vendor shall only disclose Test results (and any other technical information exchanged in the scope of Testing) in accordance with the provisions of Section A.6.2 below, and agrees that as between PCI SSC and Vendor, for purposes of such section, such results and information shall be deemed to be Confidential Information of PCI SSC. Vendor shall have no "right of access" to any data associated with the ASV Program or Testing, except as allowed by PCI SSC under this Agreement.

(f) If a candidate or validated ASV scan solution of Vendor receives a failing score on the corresponding ASV Lab Scan Test solely for reasons outside the scope of Vendor's responsibility or immediate control (for example, failure to complete applicable Testing by applicable deadlines due to delay(s), technical failure(s) or other issue(s) caused solely by the ASV Validation Lab), Vendor may appeal such failing Test result by providing a notice to the ASV Program Manager via electronic mail (addressed to asv@pcisecuritystandards.org) within 14 calendar days after the debriefing phone call with the ASV Validation Lab, which notice sets forth the following: (i) in the "Subject" line of the electronic mail, the words "Appeal of ASV Lab Scan Test Result"; (ii) in the body of

© 2008-2017 PCI Security Standards Council, LLC

the electronic mail: (A) the name of the ASV Validation Lab that conducted the Test, (B) the date on which the Test was conducted, (C) the specific time(s) during the Test window in which each asserted delay, technical failure, or other issue occurred, (D) a concise statement of what Vendor in good faith has reasonably determined to be the root cause of the Test failure, (E) a detailed description of such root cause and Vendor's analysis and determination thereof, tied to the factual evidence provided pursuant to clause A.3.5(f)(iii) below, and (F) a clear statement of the specific relief Vendor seeks from PCI SSC if the appeal is successful; and (iii) attached to the e-mail, applicable and defensible factual evidence supporting the appeal and Vendor's good faith, reasonable root cause analysis and determination. Vendor acknowledges and agrees that PCI SSC's decision regarding any such appeal will be final, binding on Vendor and based solely on the factual evidence received in connection the appeal; and that accordingly, PCI SSC will disregard all speculation, hyperbole, and/or unfounded statements, suspicions, or assertions so received. Vendor acknowledges and agrees that the ASV Validation Lab Testing process is operated by ASV Validation Labs independently of (and without technical disclosure to) PCI SSC, and that accordingly, PCI SSC cannot and will not change or reverse any technical finding(s) of any ASV Lab Scan Test. Vendor acknowledges and agrees that, in connection with all Vendor appeals, PCI SSC may request (and Vendor shall promptly provide) additional information from Vendor and, to the extent PCI SSC deems necessary for purposes of rendering its decision in connection with such appeal, PCI SSC may share such additional information and the details of the appeal with ASV Validation Labs, Participating Payment Brands, or others.

A.4 Fees

Vendor agrees to pay all applicable fees imposed by PCI SSC relating to Vendor's and its ASV Employees' participation in the ASV Program (collectively, "Fees"), in each case as and in the manner provided for in the applicable *ASV Program Materials* or "*PCI SSC Programs Fee Schedule*" posted on the Website. Such Fees may include, without limitation, initial application or processing fees, qualification fees, requalification fees, training fees, fees in connection with quality assurance and/or Remediation, fees to cover administrative costs, re-listing, penalties and other costs, and other fees. Vendor agrees to pay all such Fees as and when required by PCI SSC and that all Fees are nonrefundable (regardless of whether Vendor's application to participate in the ASV Program is approved, Vendor or any Vendor product or solution has been approved or removed from the ASV List, this Agreement has been terminated, or otherwise). Vendor acknowledges and agrees that PCI SSC from time to time may require Vendor to provide representatives and/or ASV Employees to attend any mandatory training programs in connection with the ASV Program, which may require the payment of attendance and other fees by Vendor.

Vendor acknowledges that PCI SSC may review and modify its Fees at any time and from time to time. Whenever a change in Fees occurs, PCI SSC shall notify Vendor in accordance with the terms of Section A.10.1. Such change(s) will be effective immediately as of the date of such notification. However, should Vendor not agree with such change(s), Vendor shall have the right to terminate this Agreement upon written notice to PCI SSC in accordance with the provisions of Section A.10.1 at any time within 30 days after such notification from PCI SSC. Except to the extent otherwise expressly provided in the applicable *ASV Program Materials*, all Fees must be paid in US dollars (USD), by check, by credit card or by wire transfer to a PCI SSC bank account specified for such purpose by PCI SSC. Vendor acknowledges and agrees that such Fees do not include any taxes, such as value added taxes (VAT), sales, excise, gross receipts and withholding taxes, universal service fund fee, or any similar tax or other government imposed fees or surcharges which may be applicable thereto. Vendor shall pay all such taxes and fees as invoiced in accordance with local law, and agrees to pay or reimburse PCI SSC for all such taxes or fees to the extent paid by PCI SSC, excluding tax on PCI

© 2008-2017 PCI Security Standards Council, LLC

SSC's income. In respect of withholding tax, Vendor will pay such additional amounts as may be necessary, such that PCI SSC receives the amount it would have received had no withholding been imposed.

A.5 Advertising and Promotion; Intellectual Property

A.5.1 ASV List and Vendor Use of PCI Materials and Marks

(a) So long as Vendor is qualified by PCI SSC as an ASV Company, PCI SSC may, at its sole discretion, display the identification of Vendor and each of its ASV scan solutions on the ASV List, along with information identifying Vendor, such ASV scan solutions, and corresponding qualification or compliance status information (including without limitation, good standing, Remediation and/or revocation status). Vendor shall provide all requested information necessary to ensure to PCI SSC's satisfaction that the identification and information relating to Vendor and/or its ASV scan solutions on the ASV List is accurate. Without limiting the rights of PCI SSC set forth in the first sentence of this Section or elsewhere, PCI SSC expressly reserves the right to remove Vendor and any of its ASV scan solutions from the ASV List (or modify the listing thereof thereon) at any time during which Vendor is not in Good Standing as an ASV Company. Vendor shall be deemed to be in "Good Standing" as an ASV Company as long as this Agreement is in full force and effect, Vendor has been approved as an ASV Company and such approval has not been revoked, a Vendor ASV scan solution has successfully completed the Testing phase of the ASV Program and is in compliance with the requirements of all applicable ASV Program Materials, and Vendor is not in breach of any of the terms or conditions of this Agreement (including without limitation, any term or provision regarding compliance with the ASV Requirements or payment).

(b) So long as Vendor is in Good Standing (or in compliance with Remediation) as an ASV Company and PCI SSC has issued a then effective Compliance Notification (in the form set out in Schedule 1) confirming that a given ASV scan solution of Vendor is deemed compliant with the PCI DSS and that PCI SSC has approved Vendor as an ASV Company, 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 (or in compliance with Remediation) as an ASV Company, Vendor's rights pursuant to the preceding sentence shall immediately cease and the ASV scan solution and related Vendor's information shall be removed from the ASV List. In the event that Vendor is otherwise in Good Standing (or in compliance with Remediation) as an ASV Company, but a given ASV scan solution of Vendor's is no longer deemed compliant with the PCI DSS, Vendor's rights pursuant to the first sentence of this Section A.5.1(b) with respect to such noncompliant ASV scan solution shall immediately cease and such noncompliant ASV scan solution shall be removed from the ASV List. While Vendor is in Good Standing (or in compliance with Remediation) as an ASV Company 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) Except as expressly authorized herein, Vendor shall not use any PCI SSC trademark, service mark, certification mark, logo or other indicator of origin or source (each a "Mark") without the prior written consent of PCI SSC in each instance. Without limitation of the foregoing, absent the prior written consent of PCI SSC in each instance and except as otherwise expressly authorized herein, Vendor shall have no authority to make, and consequently shall not make, any statement that would constitute any implied or express endorsement, recommendation or warranty by PCI SSC regarding Vendor, any of its services or products (including but not limited to Vendor's ASV scan solution(s)), or the

© 2008-2017 PCI Security Standards Council, LLC

functionality, quality or performance of any aspect of any of the foregoing. Vendor shall not: (i) make any false, misleading, incomplete or disparaging statements or remarks regarding, or misrepresent the requirements of, PCI SSC or any PCI SSC Standard, including without limitation, any requirement regarding the implementation of any PCI SSC Standard or the application thereof to any third party, or (ii) state or imply that any PCI SSC Standard requires usage of Vendor's products or services. Subject to the foregoing, and except with respect to (A) factual references that Vendor includes from time to time in its contracts with Scan Customers that are required or appropriate in order for Vendor to accurately describe the nature of the Services Vendor will provide pursuant to such contracts, and (B) references permitted pursuant to Section A.5.1(b) above, Vendor shall not, without the separate prior written agreement or consent of PCI SSC in each instance: (1) copy, create derivative works of, publish, disseminate or otherwise use or make available any PCI SSC Standard, PCI Materials (defined in Section A.7.3), PCI SSC mark or any copy of, or statement or material (in any form) that incorporates any of the foregoing or any portion thereof or (2) incorporate any of the foregoing, the name of PCI SSC or the term "PCI SSC" into any product or service (in any form). Prior review and/or approval of such statements, materials or products by PCI SSC does not relieve Vendor of any responsibility for the accuracy and completeness of such statements, materials or products or for Vendor's compliance with this Agreement or any applicable law. Except as otherwise expressly agreed by PCI SSC in writing, any violation of this Section A.5, including but not limited to any dissemination or use of promotional or other materials or publicity in violation hereof, shall be deemed a material breach of this Agreement and upon any such violation, PCI SSC may terminate Vendor's qualification as an ASV Company (including but not limited to removing Vendor's name and ASV scan solutions from the ASV List) and/or this Agreement, in its sole discretion.

A.5.2 Uses of Vendor Name and Designated Marks

Vendor grants PCI SSC and each Participating Payment Brand the right to use Vendor's name and trademarks, as designated in writing by Vendor, to list Vendor on the ASV List and to include reference to Vendor in publications to Financial Institutions, Issuers, Merchants, Acquirers, Processors, and the public regarding the ASV Program. Neither PCI SSC nor any Participating Payment Brand shall be required to include any such reference in any materials or publicity regarding any PCI SSC Program. Vendor warrants and represents that it has authority to grant the foregoing rights to PCI SSC and the Participating Payment Brands.

A.5.3 No Other Rights Granted

Except as expressly stated in this Section A.5, no rights to use any party's or Member's marks or other Intellectual Property Rights (as defined below) are granted herein, and each party respectively reserves all of its rights therein. Without limitation of the foregoing, except as expressly provided in this Agreement, no rights are granted to Vendor with respect to any Intellectual Property Rights in the PCI DSS or any other PCI Materials.

A.5.4 Intellectual Property Rights

(a) All Intellectual Property Rights, title and interest in and to each PCI SSC Program, the PCI DSS and all other PCI Materials, all materials Vendor receives from PCI SSC or any contractor, representative, or agent thereof, and each portion, future version, revision, extension, enhancement, improvement or derivative work of or based upon any of the foregoing, are and at all times shall remain solely and exclusively the property of PCI SSC or its licensors, as applicable. Subject to the foregoing and to the restrictions set forth in Section A.6 below, so long as Vendor is in Good Standing as an ASV Company or in

© 2008-2017 PCI Security Standards Council, LLC

compliance with Remediation, Vendor may, on a non-exclusive, non-transferable, worldwide, revocable basis, use the PCI Materials (and any portion thereof), provided that such use is solely for Vendor's internal review purposes or as otherwise expressly permitted in this Agreement or pursuant to a separate written consent or agreement between PCI SSC and Vendor in each instance. For purposes of this Agreement, "Intellectual Property Rights" shall mean all present and future patents, trademarks, 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.

(b) All right, title and interest in and to the Intellectual Property Rights in all materials generated by or on behalf of PCI SSC with respect to Vendor and/or results of assessments or Testing performed by or on behalf of PCI SSC (including without limitation, all results of ASV Lab Scan Tests) are and at all times shall remain the property of PCI SSC. Subject to the provisions of Section A.6, Vendor may use and disclose such materials solely for the purposes expressly permitted by this Agreement. Vendor shall not revise, abridge, modify or alter any such materials. Vendor shall not assert or imply that assessment or Testing results other than those upon which a given Compliance Notification was issued by PCI SSC are connected or related to that Compliance Notification. While a given ASV scan solution remains on the ASV List, Vendor shall have the right to make copies of the corresponding Compliance Notification to inform third parties that the ASV scan solution described therein is in compliance with the PCI DSS and that Vendor has been approved as an ASV Company.

(c) Vendor shall not during or at any time after the completion, expiry or termination of this Agreement in any way question or dispute PCI SSC's or its licensors' (as applicable) Intellectual Property Rights in any PCI SSC Program or any of the PCI Materials or Testing results.

(d) Except as otherwise expressly agreed by the parties, as between PCI SSC and Vendor, all Intellectual Property Rights, title and interest in and to the materials created by Vendor and submitted by Vendor to PCI SSC in connection with its performance under this Agreement are and at all times shall remain vested in Vendor, or its licensors.

A.6 Confidentiality

A.6.1 Definition of Confidential Information

As used in this Agreement, "Confidential Information" means (i) all terms of this Agreement, all Test results and any other technical information exchanged in the scope of Testing; (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, assessment reports, trade secrets or know-how, information concerning either party's past, current, or planned products, services, fees, finances, member institutions, Acquirers, Issuers, 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 connection with any PCI SSC Program or activity in which Vendor is a participant and 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

© 2008-2017 PCI Security Standards Council, LLC

and all other information that reasonably should be understood to be confidential. "Personal Information" means any and all Participating Payment Brand payment card account numbers, Participating Payment Brand transaction information, IP addresses or other PCI SSC, 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 Participating Payment Brand accountholder that is associated with or organized or retrievable by an identifier unique to that accountholder, including accountholder names, addresses, or account numbers.

A.6.2 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, accountants, representatives and agents of the Receiving Party who have a need to know and be used solely as required in connection with (A) the performance of this Agreement and/or (B) the operation of such party's or its Members' respective payment card data security compliance programs (if applicable) 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 applicable to such Confidential Information that are in form and substance similar to the provisions of this Section A.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.

A.6.3 Scan Customer Data

To the extent any data or other information obtained or generated by Vendor relating to any Scan Customer in the course of providing Services thereto may be subject to any confidentiality restrictions between Vendor and such Scan Customer, Vendor shall provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such Scan Customer in writing) that (i) Vendor may disclose such data or other information to PCI SSC and/or Participating Payment Brands, as requested by the Scan Customer, (ii) to the extent any Participating Payment Brand obtains such data or other information in accordance with the preceding clause A6.3(i), such Participating Payment Brand may disclose (a) such data or other information on an as needed basis to other Participating Payment Brands and to such Participating Payment Brands' respective Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies and (b) that such Participating Payment Brand has received such data or other information with respect to such Scan Customer (identified by name) and whether such data or other information was satisfactory, and (iii) Vendor may disclose such data or other information as necessary to comply with its obligations and

© 2008-2017 PCI Security Standards Council, LLC

requirements pursuant to Section A.10.2(b) below. Accordingly, notwithstanding anything to the contrary in Section A.6.2(a) above, to the extent requested by a Scan Customer, PCI SSC may disclose Confidential Information relating to such Scan Customer and obtained by PCI SSC in connection with this Agreement to Participating Payment Brands in accordance with this Section A.6.3, and such Participating Payment Brands may in turn disclose such information to their respective member Financial Institutions and other Participating Payment Brands. Vendor hereby consents to such disclosure by PCI SSC and its Participating Payment Brands. As between any Member, on the one hand, and Vendor or any Scan Customer, on the other hand, the confidentiality of data and other information provided to Members by Vendor or any Scan Customer is outside the scope of this Agreement and may be subject to such confidentiality arrangements as may be established from time to time between such Member, on the one hand, and Vendor or such Scan Customer (as applicable), on the other hand.

A.6.4 Personal Information

In the event that Vendor receives Personal Information from PCI SSC or any Member or Scan Customer in the course of providing 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 (as defined in Section A.9.1) maintain such data protection handling practices as may be required by PCI SSC from time to time, including without limitation, as a minimum, physical, electronic and procedural safeguards designed: (i) to maintain the security and confidentiality of such Personal Information (including, without limitation, encrypting such Personal Information in accordance with applicable Participating Payment Brand guidelines, if any); (ii) to protect against any anticipated threats or hazards to the security or integrity of such information; and (iii) to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the natural persons to whom such Personal Information relates. Vendor will make available to PCI SSC and the Participating Payment Brands, and will require in its agreements with Scan Customers that Scan Customers will make so available, such appropriate reviews and reports to monitor Vendor's compliance with the foregoing commitments as PCI SSC or any Participating Payment Brand may reasonably request from time to time. Without limitation of the foregoing, Vendor acknowledges and agrees that if it performs the Services or any other services for PCI SSC, any Participating Payment Brand or any Scan Customer in a manner that will result in the storage, processing or transmission of data to which the PCI DSS applies, Vendor shall be required to be certified as compliant with the PCI DSS and any other applicable PCI SSC Standards as such may be modified by PCI SSC from time to time. If PCI DSS compliance is required, Vendor, at its sole cost and expense, shall: (i) conduct or have conducted the audits required for PCI DSS compliance; and (ii) take all actions required for Vendor to maintain PCI DSS compliance. If required to be PCI DSS compliant, Vendor acknowledges that it further has the obligation to keep up to date on any changes to the PCI DSS and implement any required changes.

A.6.5 Return

Within fourteen (14) days after notice of termination of this Agreement or demand by PCI SSC, Vendor promptly shall return to PCI SSC all property and Confidential Information of PCI SSC and of all third parties to the extent provided or made available by PCI SSC; provided, however, that Vendor may retain copies of Confidential Information of PCI SSC to the extent the same were, prior to such notice of termination or demand, either automatically generated archival copies or incorporated into Vendor's work papers as a result of providing services to a Scan Customer; and Vendor shall continue to maintain the confidentiality of all such retained Confidential Information in accordance with this Agreement. If agreed by PCI SSC, Vendor

© 2008-2017 PCI Security Standards Council, LLC

may instead destroy all such materials and information and provide a certificate of destruction to PCI SSC, with sufficient detail regarding the items destroyed, destruction date, and assurance that all copies of such information and materials also were destroyed.

A.6.6 Remedies

In the event of a breach of Section A.6.2 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 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).

A.7 Indemnification and Limitation of Liability

A.7.1 Indemnification

Vendor shall defend, indemnify, and hold harmless PCI SSC and its Members, and their respective subsidiaries, and all affiliates, subsidiaries, directors, officers, employees, agents, representatives, independent contractors, attorneys, successors, and assigns of any of the foregoing (collectively, including without limitation, PCI SSC and its Members, "Indemnified Parties") from and against any and all claims, losses, liabilities, damages, 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) that arise or result from any claim by any third party with respect to Vendor's (i) breach of its agreements, representations or warranties contained in this Agreement; (ii) participation in any PCI SSC Program or use of any PCI Materials or PCI SSC Program-related information (a) in violation of this Agreement or (b) in violation of any applicable law, rule or regulation; (iii) non-performance (or deficient performance) of any Services or portion thereof for any Scan Customer that has engaged Vendor to perform any Services, including without limitation claims asserted by Scan Customers or Members; (iv) negligence or willful misconduct in connection with any PCI SSC Program, this Agreement or Vendor's performance of any Services, except to the extent arising out of negligence or willful misconduct of an Indemnified Party; (v) ASV scan solutions, candidate ASV scan solutions and/or the use of any of the forgoing; or (vi) breach, violation, infringement or misappropriation of any third-party Intellectual Property Right. All indemnities provided for under this Agreement shall be paid by Vendor 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 the corresponding claim or liability arises solely from a defect in the PCI Materials provided by an Indemnified Party and such PCI Materials are used by Vendor without modification and in accordance with all then applicable publicly available updates, guidance, and best practices provided by PCI SSC.

© 2008-2017 PCI Security Standards Council, LLC

A.7.2 Indemnification Procedure

Vendor's indemnity obligations are contingent on the Indemnified Party's providing notice of the claim or liability to Vendor, provided that the failure to provide any such notice shall not relieve Vendor of such indemnity obligations except and to the extent such failure has materially and adversely affected Vendor's ability to defend against such claim or liability. Upon receipt of such notice, Vendor will be entitled to control, and will assume full responsibility for, the defense of such matter. PCI SSC 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 PCI SSC and/or its Members may, at their own cost and expense, participate in such investigation, trial and defense and any appeal arising therefrom or assume the defense of any Indemnified Party. In any event, PCI SSC and/or its Members will each have the right to approve counsel engaged by Vendor to represent any Indemnified Party affiliated therewith, which approval shall not be unreasonably withheld. Vendor will not enter into any settlement of a claim that imposes any obligation or liability on PCI SSC or any other Indemnified Party without the express prior written consent of PCI SSC or such Indemnified Party, as applicable.

A.7.3 No Warranties; Limitation of Liability

(a) PCI SSC PROVIDES THE ASV PROGRAM, ALL OTHER PCI SSC PROGRAMS, ALL ASV PROGRAM MATERIALS, THE WEBSITE AND ALL RELATED AND OTHER MATERIALS PROVIDED OR OTHERWISE MADE ACCESSIBLE BY OR ON BEHALF OF PCI SSC IN CONNECTION WITH ANY PCI SSC PROGRAM (THE FOREGOING, COLLECTIVELY, THE "PCI MATERIALS") 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 ANY OF THE PCI MATERIALS.

(b) PCI SSC MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, THE ASV PROGRAM, ANY OTHER PCI SSC PROGRAM, THE PCI MATERIALS OR ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR ANY OTHER PCI SSC PROGRAM. PCI SSC SPECIFICALLY DISCLAIMS, AND VENDOR EXPRESSLY WAIVES, ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THIS AGREEMENT, THE ASV PROGRAM, EACH OTHER PCI SSC PROGRAM, THE PCI MATERIALS, AND ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR ANY PCI SSC PROGRAM, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITATION OF THE FOREGOING, PCI SSC SPECIFICALLY DISCLAIMS, AND VENDOR EXPRESSLY WAIVES, ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THE PCI MATERIALS AND ANY INTELLECTUAL PROPERTY RIGHTS SUBSISTING THEREIN OR IN ANY PART THEREOF, INCLUDING BUT NOT LIMITED TO ANY AND ALL EXPRESS OR IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, OR SUITABILITY FOR ANY PURPOSE RELATING TO ANY OF THE FOREGOING. THE FOREGOING DISCLAIMER IS MADE BY PCI SSC FOR ITSELF AND, WITH RESPECT TO EACH SUCH DISCLAIMER, ON BEHALF OF ITS LICENSORS AND MEMBERS.

(c) In particular, without limiting the foregoing, Vendor acknowledges and agrees that the accuracy, completeness, sequence or timeliness of the PCI Materials or any portion thereof cannot be guaranteed. In addition, PCI SSC makes no representation or warranty

© 2008-2017 PCI Security Standards Council, LLC

whatsoever, expressed or implied, and assumes no liability, and shall not be liable in any respect to Vendor regarding (i) any delay or loss of use of any of the PCI Materials, or (ii) system performance and effects on or damages to software or hardware in connection with any use of the PCI Materials.

(d) EXCEPT FOR DAMAGES CAUSED BY THE GROSS NEGLIGENCE OR WILLFUL MISCONDUCT OF A PARTY, AND EXCEPT FOR THE OBLIGATIONS OF VENDOR UNDER SECTIONS A.5 OR A.6, IN NO EVENT SHALL EITHER PARTY OR ANY MEMBER BE LIABLE TO THE OTHER FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT OR SPECIAL DAMAGES, HOWEVER CAUSED, WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY DOES NOT APPLY TO INDEMNIFICATION OWED TO AN INDEMNIFIED PARTY PURSUANT TO THIS SECTION A.7.

(e) PCI SSC shall be liable vis-à-vis Vendor only for any direct damage incurred by Vendor as a result of PCI SSC's gross negligence (contractual or extra-contractual) under this Agreement provided PCI SSC's aggregate liability for such direct damage under and for the duration of this Agreement will never exceed the fees paid by Vendor to PCI SSC under Section A.4.

(f) Except as otherwise expressly provided in this Agreement, neither PCI SSC nor any Participating Payment Brand shall be liable vis-à-vis Vendor for any other damage incurred by Vendor under this Agreement or in connection with any PCI SSC Program, 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 or participation in any such PCI SSC Program (regardless of whether such damages are reasonably foreseeable or PCI SSC has been advised of the possibility of such damages), or for any loss that results from force majeure.

A.7.4 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 ASV Companies (as applicable) participating in each of the PCI SSC Programs, including without limitation, the insurance requirements for ASV Companies set forth in Appendix B of the *ASV Qualification Requirements*. Vendor acknowledges and agrees that if it is a non-U.S. and non-European Union ASV Company, unless otherwise expressly agreed by PCI SSC 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 PCI SSC determines, in its sole discretion, is substantially equivalent to the insurance required by PCI SSC for U.S. and European Union ASV Companies participating in each of the PCI SSC Programs. Vendor hereby represents and warrants that it meets all applicable insurance requirements as provided for in this Section and that such insurance shall not be cancelled or modified without giving PCI SSC at least twenty (20) days' prior written notice. PCI SSC may modify its insurance requirements from time to time based on parameters affecting risk and financial capability that are general to ASV Companies or specific to Vendor, provided that PCI SSC is under no obligation to review and does not undertake to advise Vendor on the adequacy of Vendor's insurance coverage.

© 2008-2017 PCI Security Standards Council, LLC

A.8 Independence; Compliance with Law

Vendor agrees to comply with all applicable PCI SSC Program qualification requirements, including without limitation, all requirements and provisions of the *ASV Qualification Requirements* regarding independence, and hereby warrants and represents that Vendor is now, and shall at all times during the Term, remain in compliance with all such requirements and provisions. Vendor represents and warrants that by entering into this Agreement and performing any Services in connection with the ASV Program, it will not breach any obligation to any third party. Vendor represents and warrants that it will comply with all applicable laws, ordinances, rules, and regulations in any way pertaining to this Agreement, its performance of the Services or its obligations under this Agreement.

A.9 Term and Termination

A.9.1 Term

This Agreement shall commence as of the Effective Date and, unless earlier terminated in accordance with this Section A.9, continue for an initial term of one (1) year (the "Initial Term") and thereafter, for additional subsequent terms of one year (each a "Renewal Term" and together with the Initial Term, the "Term"), subject to Vendor's successful completion of all applicable requalification requirements for each Renewal Term.

A.9.2 Termination by Vendor

Vendor may terminate this Agreement at any time upon thirty (30) days' written notice to PCI SSC. Notwithstanding Section A.10.1 below, any notice or other written communication (including by electronic mail) from Vendor pursuant to which or to the effect that Vendor requests, notifies, elects, opts, chooses, decides or otherwise indicates its desire to cease participation in the ASV Program, be removed from the ASV List or terminate this Agreement shall be deemed to constitute notice of termination of this Agreement and Vendor's corresponding qualification as an ASV Company by Vendor pursuant to this Section, and thereafter, notwithstanding the thirty (30) day notice period provided for in the preceding sentence and without any further action by Vendor, PCI SSC may immediately remove Vendor from the ASV List and may terminate this Agreement effective upon written notice to Vendor.

A.9.3 Termination by PCI SSC

PCI SSC may terminate this Agreement effective as of the end of the then-current Term by providing Vendor with written notice of its intent to terminate or not to renew this Agreement at least sixty (60) days prior to the end of the then-current Term. Additionally, PCI SSC may terminate this Agreement: (i) with written notice upon Vendor's voluntary or involuntary bankruptcy, receivership, reorganization dissolution or liquidation under state or federal law that is not otherwise dismissed within thirty (30) days; (ii) with written notice upon Vendor's breach of any representation or warranty under this Agreement; (iii) with fifteen (15) days' prior written notice following Vendor's breach of any other term or provision of this Agreement (including without limitation, Vendor's failure to pay applicable Fees or otherwise comply with any of the ASV Requirements), provided such breach remains uncured when such 15-day period has elapsed; (iv) with written notice if PCI SSC determines, in its sole discretion, that Vendor has (a) failed to achieve successful results in connection with (1) initial Testing, (2) annual maintenance Testing performed pursuant to Section A.3.5(b) and/or (3) any Testing performed pursuant to Section A.3.5(c) or A.3.5(d) or (b) failed to resubmit a given ASV scan solution within the applicable timelines provided pursuant to Sections A.3.5(b), A.3.5(c) or A.3.5(d); (v) in accordance with Section A.9.5 below; or (vi) if PCI SSC ceases to operate the ASV Program, whether with or without replacing it with any other program; provided, however,

© 2008-2017 PCI Security Standards Council, LLC

that if PCI SSC has terminated pursuant to Section A.9.3(iv) above, and Vendor thereafter determines that it has satisfied each of the requirements set forth in such Section, Vendor may request a new compliance review by PCI SSC in accordance with Section A.3.5(d) of this Agreement, PCI SSC may undertake such review at PCI SSC's sole discretion, and if PCI SSC determines as a result of such review that Vendor is in compliance with all applicable ASV Requirements, then PCI SSC may reinstate this Agreement and Vendor's status as an ASV Company effective as of the date of such determination, subject to Vendor's payment of all outstanding Fees (if any). Without limiting the foregoing, Vendor acknowledges and agrees that PCI SSC 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, at any time and from time to time, in its discretion.

A.9.4 Effect of Termination

Upon any termination or expiration of this Agreement: (i) Vendor's qualification as an ASV Company shall automatically terminate, and Vendor and each of its ASV scan solutions will be removed from the ASV List and/or the corresponding listing(s) thereupon may be annotated as PCI SSC deems appropriate; (ii) Vendor shall immediately cease all advertising and promotion of its qualification and/or status as an ASV Company, and the listing(s) of Vendor and its ASV scan solutions on the ASV List, and ensure that it and its employees do not state or imply that any employee of Vendor is an "ASV Employee," an "ASV" or otherwise qualified by PCI SSC in connection with the ASV Program; (iii) Vendor shall immediately cease soliciting for and performing all PCI Scanning Services, provided that Vendor shall complete any and all PCI Scanning Services contracted with Scan Customers prior to such expiration or the notice of termination if and to the extent instructed by PCI SSC in writing; (iv) to the extent Vendor is instructed to complete any PCI Scanning Services pursuant to preceding clause (iii), Vendor will complete such PCI Scanning Services within the time contracted with the Scan Customer; (v) Vendor shall comply with all outstanding information requests within the time contracted with its Scan Customers and shall remain responsible for all of the obligations, representations and warranties hereunder with respect to PCI Scanning Services provided prior to or after such termination or expiration; (vi) Vendor shall return or destroy all PCI SSC and third-party property and Confidential Information in accordance with the terms of Section A.6; (vii) if requested by PCI SSC, Vendor shall obtain (at Vendor's sole cost and expense) the services of a replacement ASV Company acceptable to PCI SSC for purposes of completing those Services for which Vendor was engaged prior to such expiration or the notice of termination but which Vendor has not been instructed to complete pursuant to Section A.9.4(iii) above; (viii) Vendor shall, within fifteen (15) days of such expiration or the notice of termination, in a manner acceptable to PCI SSC, notify those of its Scan Customers with which Vendor is then engaged to perform any PCI Scanning Services or other Services of such expiration or termination; (ix) if requested by PCI SSC, Vendor shall within fifteen (15) days of such request, identify to PCI SSC in writing all Scan Customers with which Vendor was engaged to perform Services immediately prior to such expiration or notice of termination and the status of such Services for each; and (x) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify any of its Members and any acquirers, Scan Customers or others of such expiration or termination and the reason(s) therefor. The provisions of Sections A.3.5(e), A.5.1(c), A.5.3, A.5.4, A.6, A.7, A.9.4 and A.10 of this Agreement shall survive the expiration or termination of this Agreement for any or no reason.

© 2008-2017 PCI Security Standards Council, LLC

A.9.5 Revocation

(a) Without limiting the rights of PCI SSC as set forth elsewhere in this Agreement, in the event that PCI SSC determines in its sole but reasonable discretion that Vendor meets any condition for revocation of its qualification as an ASV Company as established by PCI SSC from time to time (satisfaction of any such condition, a "Violation"), including without limitation, any of the conditions identified or described as examples of Violations herein or in the *ASV Qualification Requirements or ASV Program Guide*, PCI SSC may, effective immediately upon notice of such Violation to Vendor, revoke such qualification from Vendor ("Revocation"), and such revoked qualification shall be subject to reinstatement pending a successful appeal in accordance with Section A.9.5(b) below and applicable PCI SSC policies and procedures.

(b) In the event of any Revocation: (i) Vendor and each of its ASV scan solutions will be removed from the ASV List and/or the corresponding listing(s) thereupon may be annotated as PCI SSC deems appropriate, (ii) Vendor must comply with Section A.9.4 above in the manner otherwise required if this Agreement had been terminated as of the effective date of such Revocation, (iii) Vendor will have a period of thirty (30) days from the date Vendor is given notice of the corresponding Violation to submit its written request for appeal to the ASV Program Manager; (iv) Vendor shall, within fifteen (15) days of such Revocation, in a manner acceptable to PCI SSC, provide notice of such Revocation to those of its Scan Customers with which Vendor is then engaged to perform PCI Scanning Services and, if applicable, of any conditions, restrictions or requirements of such Revocation that may impact its ability to perform such PCI Scanning Services for such Scan Customers going forward; and (v) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify any of its Members and any acquirers, Scan Customers or others of such Revocation and the reason(s) therefor. In the event Vendor fails to submit a request for appeal within the allotted 30-day period or such request is denied, then effective immediately as of the end of such period or such denial, as applicable, this Agreement shall automatically terminate, the Revocation of Vendor's qualification as an ASV Company shall become permanent, and Vendor's right to such (or any) appeal of such Revocation shall be deemed forfeited.

(c) All Revocation appeal proceedings will be conducted in accordance with such procedures as PCI SSC may establish from time to time, PCI SSC will review all relevant evidence submitted by Vendor and each complainant (if any) in connection with therewith, and PCI SSC shall determine whether termination of Vendor's qualification as an ASV Company is warranted or, in the alternative, no action, or specified remedial actions shall be required. All determinations of PCI SSC regarding Revocation and any related termination or appeals shall be final and binding upon Vendor. If PCI SSC determines that termination is warranted, then effective immediately and automatically upon such determination, Vendor's qualification as an ASV Company and this Agreement shall terminate. If PCI SSC determines that such termination is not warranted, the Revocation shall be lifted, such ASV Company qualification shall be reinstated, and the listing of Vendor on the ASV List shall be reinstated. If PCI SSC determines that remedial action is required, PCI SSC shall notify Vendor and may establish a date by which such remedial action must be completed; provided, however, that unless otherwise agreed by PCI SSC in writing the Revocation shall not be lifted, and Vendor shall not be reinstated on the ASV List, unless and until such time as Vendor has completed such remedial action; and provided, further, that if Vendor fails to complete any required remedial actions by the date (if any) established by PCI SSC for completion thereof, PCI SSC may terminate Vendor's ASV Company qualification and this Agreement, effective immediately as of or any time after such date.

© 2008-2017 PCI Security Standards Council, LLC

A.10 General Terms

A.10.1 Notices

All notices required under this Agreement shall be in writing and shall be deemed given when delivered (a) personally, (b) by overnight delivery upon written verification of receipt, (c) by facsimile or electronic mail transmission upon electronic transmission confirmation or delivery receipt, or (d) by certified or registered mail, return receipt requested, five (5) days after the date of mailing. Notices from PCI SSC to Vendor shall be sent to the attention of the Primary Contact named, and at the applicable location or address specified, on the signature page of this Agreement. Except as otherwise expressly provided in this Agreement, notices from Vendor to PCI SSC shall be sent to PCI SSC, 401 Edgewater Place, Suite 600, Wakefield, Massachusetts 01880, Attention: ASV Program Manager. A party may change its addressee and address for notices by giving notice to the other party pursuant to this Section A.10.1. Notwithstanding (and without limitation of) the foregoing: (i) any notice from PCI SSC to Vendor hereunder may be given and shall be deemed to have been effectively delivered in writing when posted to the secure portal designated or reserved by PCI SSC for the ASV Program; and (ii) any notice from PCI SSC to Vendor of any change in Fees may be given and shall be deemed to have been effectively delivered in writing when posted to the PCI SSC Program Fee Schedule on the Website.

A.10.2 Audit and Financial Statements

(a) Vendor shall allow PCI SSC or its designated agents access during normal business hours throughout the Term and for six (6) months thereafter to perform audits of Vendor's facilities, operations and records of Services to determine whether Vendor has complied with this Agreement. Vendor also shall provide PCI SSC or its designated agents during normal business hours with books, records and supporting documentation adequate to evaluate Vendor's performance hereunder. Upon request, Vendor shall provide PCI SSC with a copy of its most recent audited financial statements or those of its parent company which include financial results of Vendor, a letter from Vendor's certified public accountant or other documentation acceptable to PCI SSC setting out Vendor's current financial status and warranted by Vendor to be complete and accurate. PCI SSC acknowledges that any such statements that are non-public are Confidential Information, and shall restrict access to them in accordance with the terms of this Agreement.

(b) Notwithstanding anything to the contrary in Section A.6 of this Agreement, in order to assist in ensuring the reliability and accuracy of Vendor's PCI Scanning Services, Vendor hereby agrees to comply with all quality assurance procedures and requirements established or imposed by PCI SSC from time to time in connection with the ASV Program (including but not limited to conditions and requirements imposed in connection with Remediation, revocation or any other ASV Company qualification status) and that, within 15 days of any written request by PCI SSC, Vendor hereby agrees to provide to PCI SSC such PCI Scanning Results and Related Materials (defined below) as PCI SSC may reasonably request with respect to any Scan Customer for which Vendor has performed PCI Scanning Services. Each agreement between Vendor and each of its Scan Customers (each a "Client Agreement") shall include such provisions as may be necessary or appropriate, or otherwise required by PCI SSC, to ensure that Vendor has all rights, licenses and other permissions necessary for Vendor to comply with its obligations and requirements pursuant to this Agreement, with no conditions, qualifications or other terms (whether in such Client Agreement or otherwise) that might tend to nullify, impair or render unenforceable Vendor's right to disclose such PCI Scanning Results and Related Materials as required by this Section. Any failure of Vendor to comply with this Section

© 2008-2017 PCI Security Standards Council, LLC

A.10.2 shall be deemed to be a breach of Vendor's representations and warranties under this Agreement for purposes of Section A.9.3, and upon any such failure, PCI SSC may terminate Vendor's qualification as an ASV Company, remove Vendor and its ASV scan solutions from the ASV List and/or terminate this Agreement in its sole discretion, upon notice to Vendor. For purposes of the foregoing, "PCI Scanning Results and Related Materials" means: (1) all Testing results, reports and related or similar information, reports, materials and assessment results generated and/or obtained in connection with Vendor's performance of PCI Scanning Services, including without limitation, all work papers, notes and other materials and information generated or obtained in connection therewith in any form, and (2) complete and accurate copies of the provisions of each Client Agreement that relate to or otherwise impact Vendor's ability to comply with its disclosure obligations pursuant to this Agreement; provided that, in each case: (A) any materials otherwise required to be provided to PCI SSC pursuant to this Section may (or shall, as the case may be) be redacted to the extent necessary to comply with applicable law and/or permitted pursuant to PCI SSC policies and procedures, including but not limited to redaction of information regarding pricing, delivery process, and/or confidential and proprietary information of the Scan Customer (and/or its customers) if such redaction is in accordance with PCI SSC policy, does not eliminate or obscure any language (or the intent or meaning thereof) that may tend to nullify, impair or render unenforceable Vendor's right to disclose PCI Scanning Results and Related Materials to PCI SSC as required by this Section, and is as limited as reasonably possible; and (B) upon request, Vendor shall provide to PCI SSC a written certification that such redaction complies with preceding clause (A) executed by an officer of Vendor.

A.10.3 Governing Law; Severability

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. 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.

A.10.4 Entire Agreement; Modification; Waivers

The parties agree that this Agreement, including the *ASV Qualification Requirements* and any other documents, addenda, supplements, amendments, appendices, exhibits, schedules or other materials incorporated herein by reference (each of which is hereby incorporated into and made a part of this Agreement by this reference), is the exclusive statement of the agreement between the parties with respect to the subject matter hereof, which supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the parties with respect to such subject matter (including without limitation, if applicable, each prior *PCI ASV Compliance Test Agreement* between Vendor and PCI SSC). This Agreement may be modified, altered or amended only (i) by written instrument duly executed by both parties or (ii) by PCI SSC 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 upon written notice of its intention to so

© 2008-2017 PCI Security Standards Council, LLC

terminate to PCI SSC. Any such unilateral modification, alteration or amendment will be effective as of the end of such 30-day period unless the Agreement is earlier terminated by Vendor pursuant to the preceding sentence. 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.

A.10.5 Assignment

Vendor may not assign this Agreement, or assign, delegate or subcontract any of its rights and/or obligations under this Agreement (including but not limited to by subcontracting any of the foregoing to a related party or affiliate), without the prior written consent of PCI SSC, which consent PCI SSC may grant or withhold in its absolute discretion.

A.10.6 Independent Contractors

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.

A.10.7 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.

A.10.8 Counterparts

This Agreement may be signed in two or more counterparts, any or all of which may be executed by exchange of facsimile and/or electronic transmission, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

A.10.9 Conflict

In the event of any express conflict or inconsistency between the terms and provisions of this Agreement and terms and provisions of the *ASV Program Materials*, this Agreement shall control. Any and all disputes or disagreements regarding any such conflict or inconsistency shall be resolved by PCI SSC in its sole but reasonable discretion, and all determinations of PCI SSC in this regard shall be final and binding.

A.10.10 No Third-Party Beneficiaries

Except as expressly provided herein, the provisions of this Agreement are for the benefit of the parties hereto only, no third-party beneficiaries are intended and no third party may seek to enforce or benefit from the provisions hereof.

[remainder of page intentionally left blank]

© 2008-2017 PCI Security Standards Council, LLC

Schedule 1: 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 PCI SSC, the ASV scan solution described below has successfully completed the Testing phase of the ASV Program and you have been certified as a PCI SSC-Approved Scanning Vendor company ("ASV Company").

ASV scan solution:

<Name of the solution>

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

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

Subject to your compliance with the terms and conditions of the Agreement, you are entitled to advertise your status as a "PCI SSC-Approved Scanning Vendor" and that the abovementioned ASV scan solution has "successfully completed PCI SSC ASV Compliance Testing" and/or that such ASV scan 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 PCI SSC's prior written approval.

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

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

Because ASV Company 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 ASV Companies published on the PCI SSC web site at www.pcisecuritystandards.org.

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

Yours Sincerely,

*******ASV scan solution to be identified in an appendix to this Compliance Notification*******

© 2008-2017 PCI Security Standards Council, LLC

Appendix B: Insurance

Prior to the commencement of the Services under this ASV Agreement, ASV Company shall procure the following insurance coverage, at its own expense, with respect to the performance of all 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 ASV 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.

CRIME/FIDELITY BOND including first-party employee dishonesty, robbery, fraud, theft, forgery, alteration, mysterious disappearance and destruction. Coverage must also include third-party employee dishonesty, i.e., coverage for claims made by the ASV Company's client against the ASV Company for theft committed by the ASV Company's Employees. The minimum limit shall be $1,000,000 each loss and annual aggregate. The policy Coverage Territory must be Worldwide.

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 ASV Agreement with a minimum limit of two million dollars ($2,000,000) each claim and annual aggregate. The policy Coverage Territory must be Worldwide.

If any of the above insurance is written on a claims-made basis, then ASV Company shall maintain such insurance for two (2) years after the termination of this ASV Agreement. Without limiting ASV Company'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 Company's performance of the Services under this ASV Agreement. The insurers shall agree that the ASV Company's insurance is primary and any insurance maintained by PCI SSC shall be excess and non-contributing to the ASV Company's insurance. The above limits can be written in other currencies, but should be the equivalent of the limits expressed above in US dollars.

Prior to commencing of services under this ASV Agreement and annually thereafter, ASV Company 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 Company 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 Company shall provide copies of the actual insurance policies if requested by PCI SSC at any time. ASV Company 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 Company of any liability hereunder or modify ASV Company obligations to indemnify PCI SSC.

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

© 2008-2017 PCI Security Standards Council, LLC

WAIVER OF SUBROGATION: ASV Company agrees to waive subrogation against PCI SSC for any injuries to its employees arising out of or in any way related to ASV Company's performance of the Service under this ASV Agreement. Further, ASV Company 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 Company's performance of the Services under this ASV Agreement.

© 2008-2017 PCI Security Standards Council, LLC

Appendix C: ASV Company Application

Please provide the information requested in Section 1 below, check each applicable box and complete the fields in Sections 2–4 below, and sign where indicated at the end of this ASV Company Application.

Applicant ASV Company (the "Company") Information – Section 1					
Company Name:					
Business Address:		City:			
State/Province:		Country:		ZIP:	
URL:					
Primary Contact Name:		Job Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
Secondary Contact Name:		Job Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	
QA Contact Name:		Job Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	

☐ The Company hereby acknowledges and agrees that in order to participate as an ASV Company in the ASV Program, it must satisfy all of the requirements specified in the *ASV Qualification Requirements* and supporting documents.

ASV Company Business Requirements – Section 2
☐ The Company hereby acknowledges the minimum business requirements and related information that must be provided to PCI SSC regarding the Company's business legitimacy, independence, and required insurance coverage pursuant to Section 2 of the *ASV Qualification Requirements,* and agrees to comply with such requirements.
Business Legitimacy – 2.1.2 Provisions
☐ The Company certifies that it is a legal entity.
☐ The Company certifies that it is providing to PCI SSC herewith a copy of its current formation document or equivalent (the "Business License"). Refer to the Documents Library on the Website—*Business License Requirements*—for more information.
Year of incorporation/formation of Company:
Location(s) of Company offices:
Describe any past or present allegations or convictions of any fraudulent or criminal activity involving the Company (and/or company principals), and the status and resolution:

© 2008–2017 PCI Security Standards Council

ASV Company Business Requirements – Section 2
Describe any past or present appeals or revocations of any qualification issued by PCI SSC to the Company (or any predecessor entity or, unless prohibited by applicable law, any ASV Employee of any of the foregoing), and the current status and any resolution thereof:

Independence – 2.2.2 Provisions

☐ The Company hereby acknowledges and agrees that it 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 SSC Assessments.

☐ The Company hereby certifies that it has a code-of-conduct policy, and agrees to provide that policy to PCI SSC upon request.

☐ The Company hereby agrees to adhere to all independence requirements as established by PCI SSC, including without limitation, all items listed in Section 2.2.1 of the *ASV Qualification Requirements.*

☐ Below or attached hereto is a description of the Company's practices for maintaining and assuring assessor independence, including but not limited to, the Company's practices, organizational structures, separation of duties, rules, and employee education in place to prevent conflicts of interest.

☐ The Company hereby:

- Agrees to maintain and 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 SSC Assessments.
- Agrees to maintain and adhere to a code-of-conduct policy, and provide the policy to PCI SSC upon request.
- Agrees to adhere to all independence requirements as established by PCI SSC, including without limitation, all items listed in Section 2.2.1 of the *ASV Qualification Requirements.*
- Agrees not to undertake to perform any PCI Scanning Services of any entity that it controls, is controlled by, is under common control with, or in which it holds any investment.
- Agrees that it has not and will not have offered or provided (and has not and will not have been offered or received) to (or from) any employee of PCI SSC or any customer, any gift, gratuity, service, or other inducement (other than compensation in an arms length transaction), in order to enter into the ASV Agreement or any agreement with a customer, or to provide PCI Scanning Services.
- Agrees to fully disclose in the scan report if the Company assesses any Scan Customer that uses any security-related devices or security-related applications that have been developed or manufactured by the Company, or to which the Company owns the rights, or that the Company has configured or manages, including, but not limited to the items described in Section 2.2.1 of the *ASV Qualification Requirements.*
- Agrees that when any of its ASV Employees recommends remediation actions that include any solution or product of the Company, the ASV Employee will also recommend other market options that exist.
- Agrees that the Company has and will maintain separation of duties controls in place to ensure that its ASV Employees conducting PCI Scanning Services are independent and not subject to any conflict of interest.
- Agrees not to use its status as a "listed ASV" to market services unnecessary to help bring Scan Customers into compliance with the PCI DSS.
- Agrees not to misrepresent any requirement of the PCI DSS in connection with its promotion or sales of services to clients, and not to state or imply that the PCI DSS requires usage of any of the Company's products or services.

☐ The Company hereby agrees that at all times while its ASV Agreement is in effect, Company will maintain sufficient insurance, insurers, coverage, exclusions, and deductibles that PCI SSC reasonably requests to adequately insure the Company for its obligations and liabilities under the ASV Agreement, including without limitation the Company's indemnification obligations.

© 2008–2017 PCI Security Standards Council

ASV Company Business Requirements – Section 2	
Insurance Coverage – 2.3.2 Provisions	
☐	The Company hereby acknowledges and agrees to adhere to all requirements for insurance coverage required by PCI SSC, including without limitation the requirements in Appendix B: Insurance Coverage, which includes details of required insurance coverage.
☐	The Company hereby certifies to PCI SSC that, along with this application, the Company is providing to PCI SSC a proof-of-coverage statement demonstrating that its insurance coverage matches locally set insurance coverage requirements.
☐	A copy of the Company's bound insurance coverage is attached to this application.
Fees – 2.4.1 Requirements	
☐	The Company hereby agrees to pay all such fees upon invoice from PCI SSC (or as part of the ASV Employee training registration process, if applicable), and that any such fees invoiced by PCI SSC will be made payable to PCI SSC according to instructions provided on the corresponding invoice.
ASV Agreement – 2.5.1 Requirements	
☐	The Company hereby acknowledges and agrees that along with its completed application package it is providing to PCI SSC an ASV Agreement between PCI SSC and the Company, in unmodified form, signed by a duly authorized officer of the Company. (A copy of the ASV Agreement is attached to this application.)

ASV Capability Requirements – Section 3	
ASV Company Skills and Experience – 3.1.2 Provisions	
☐	The Company hereby represents and warrants that it currently possesses (and at all times while it is a ASV Company will continue to possess) technical security assessment experience similar or related to PCI Scanning Services, and that it has (and must have) a dedicated security practice that includes staff with specific job functions that support the security practice.
	Description of the Company's relevant areas of specialization within information security—for example, network security, database and application security, and incident response:
	Description of the Company's experience and knowledge with information security vulnerability assessment engagements including penetration testing:

Total number of Company employees on staff:
The number of ASV Employees expected to perform PCI Scanning Services (minimum of two (2) required):
Describe any additional evidence of a dedicated security practice within the Company:
Describe other core business offerings:
Describe the size and types of market segments in which the applicant ASV Company tends to focus, such as Fortune 500, financial industry, insurance industry, or small-to-medium sized businesses:
Languages supported by the Company:

© 2008–2017 PCI Security Standards Council

ASV Capability Requirements – Section 3 (continued)			
Provide two client references from security engagements within the last 12 months:			
Client:		From (date):	To (date):
Contact name:		Job title:	
Contact phone number:		E-mail address:	
Description of security engagement:			
Client:		From (date):	To (date):
Contact name:		Job title:	
Contact phone number:		E-mail address:	
Description of security engagement:			

PCI SSC Code of Professional Responsibility – 3.3.1 Requirement

☐ The Company hereby acknowledges and agrees that it has read and understands the PCI SSC Code of Professional Responsibility, and hereby agrees to advocate, continuously adhere to, and support the terms and provisions thereof.

ASV Administrative Requirements – Section 4

☐ The Company hereby acknowledges and agrees to the administrative requirements for ASV Companies set forth in the *ASV Qualification Requirements*, including company contacts, background checks, adherence to PCI DSS procedures, quality assurance, and protection of confidential and sensitive information.

Background Checks – 4.2

☐ The Company hereby agrees that its policies and hiring procedures must include performing background checks and satisfying the provisions in Section 4.2.2 (to the extent legally permitted within the applicable jurisdiction) when hiring each applicant ASV Employee.

☐ The Company hereby attests that its policies and hiring procedures include performing background checks in full accordance with Section 4.2.

☐ The Company hereby attests that it successfully completes background checks for each applicant ASV Employee in accordance with the provisions of Section 4.2.2

Below is a summary description of the Company's personnel background check policies:

The Company's personnel background check policies and procedures include the following (*to the extent legally permitted within the applicable jurisdiction*):

☐ Verification of aliases (when applicable)

☐ Reviewing records of any criminal activity, such as felony (or non-US equivalent) convictions or outstanding warrants

☐ Annually review records of any criminal activity, such as felony (or non-US equivalent) convictions or outstanding warrants

☐ Minor offenses (for example, misdemeanors or non-US equivalents) are allowed, but major offenses (for example, felonies or non-US equivalents) automatically disqualify an employee from serving as a ASV Employee

☐ The Company hereby understands and agrees that, upon request, it must provide to PCI SSC the background check history for each of its ASV Employees, to the extent legally permitted within the applicable jurisdiction.

© 2008–2017 PCI Security Standards Council

ASV Administrative Requirements – Section 4 (continued)

Internal Quality Assurance – 4.3.2 Provisions

☐ The Company hereby acknowledges and agrees that it must adhere to all quality assurance requirements described in the *ASV Qualification Requirements* and supporting documentation, must have a quality assurance program, documented in its Quality Assurance manual, and must maintain and adhere to a documented quality assurance process and manual that includes all items described in Section 4.3 of the *ASV Qualification Requirements*.

☐ The Company hereby acknowledges and agrees that its internal quality assurance reviews must be performed by qualified personnel and must cover scan scope validation, assessment procedures performed, supporting documentation as applicable, evidence to support any exceptions, false-positives or compensating controls noted in the scan report, remediation recommendations, proper use of definitions, consistent findings, and documentation of results as applicable.

☐ The Company hereby acknowledges and agrees that it must have and adhere a change management policy and processes for changes to the ASV scan solution.

☐ The Company hereby acknowledges and agrees that it has and shall keep in place controls to maintain the integrity of its ASV scan solution. Each ASV scan solution must:

- Be protected from unauthorized access
- Adhere to the ASV Company's change management policy and processes for changes to the ASV scan solution
- Be monitored or able to produce alerts when changes are made
- Ensure the ASV Company's systems cannot be used to gain unauthorized access to a Scan Customer's environment

The Company hereby acknowledges and agrees that as an ASV Company, it must at its sole cost and expense:

☐ At all times maintain and adhere to the internal quality assurance requirements as described in Section 4.3 of the *ASV Qualification Requirements.*

☐ Provide to PCI SSC, upon request, a complete copy of the Company's quality assurance manual, in accordance with the *ASV Qualification Requirements* and supporting documentation.

☐ Permit PCI SSC, upon request, to conduct audits of the Company and/or to conduct site visits.

☐ Inform each Scan Customer of the *ASV Feedback Form* (available on the Website), upon commencement of the PCI Scanning Services for that Scan Customer.

Protection of Confidential and Sensitive Information – 4.4.2 Provisions

☐ The Company currently has and hereby agrees to have a policy and adhere to a documented process for protection of confidential and sensitive information, which includes adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect confidential and sensitive information against any threats or unauthorized access during storage, processing, and/or communicating of this information.

☐ The Company must maintain the privacy and confidentiality of information obtained in the course of performing its duties under the ASV Agreement, unless (and to the extent) disclosure is expressly permitted thereunder.

☐ The Company's confidential and sensitive data protection handling policies and practices include all physical, electronic, and procedural safeguards described in Section 4.4 of the *ASV Qualification Requirements.*

☐ The Company agrees to provide PCI SSC, upon request, a copy of the confidentiality agreement template that it requires each ASV to sign.

© 2008–2017 PCI Security Standards Council

ASV Administrative Requirements – Section 4 (continued)

Evidence Retention – 4.5 Provisions

- ☐ The Company has an evidence-retention policy and procedures per Section 4.5 of the *ASV Qualification Requirements* and agrees to retain all records created and/or obtained during each PCI Scan for a minimum of three (3) years.
- ☐ The Company agrees to make the foregoing materials and information available to PCI SSC upon request for a minimum of three (3) years.
- ☐ The Company agrees to provide a copy of the foregoing evidence-retention policy and procedures to PCI SSC upon request.

Signature

By signing below, the undersigned hereby:

(a) Represents and certifies to PCI SSC that (s)he is an officer of the Company and is duly authorized to legally bind the Company to the terms of this ASV Company Application; and

(b) Both individually and by and on behalf of the Company: (i) represents and certifies that the information provided in this ASV Company Application is true, correct, and complete, and (ii) acknowledges, accepts, agrees to, and makes the attestations and certifications set forth in (as the case may be) each of the statements checked (or otherwise marked) in this ASV Company Application above.

Legal Name of Applicant ASV Company			
Officer:		Job Title:	
Duly authorized officer signature ↑		*Date* ↑	

© 2008–2017 PCI Security Standards Council

Appendix D: ASV Employee Application

For each individual applying for qualification as a ASV Employee (each an "Applicant"), the ASV Company or applicant ASV Company employing such individual (the "Company") must submit to PCI SSC a copy of this ASV Employee Application, completed and executed by such Applicant.

Company Information					
Company Name:					
Applicant Information					
Applicant Name:		Job Title:			
Telephone:		E-mail:			
Business Address:		City:			
State/Province:		Country:		ZIP:	

3.2.1 ASV Employee Skills, Experience and Education

Provide examples of the Applicant's work and/or description of experience demonstrating a minimum of one (1) year of experience in vulnerability scanning and/or penetration testing:

From (date):	To (date):	Total time: Years Months

Provide examples of the Applicant's work and/or description of experience in the following areas of expertise.

Note: *If the Applicant possesses a professional industry certification, they must have a minimum of one (1) year of experience in at least two (2) of the following areas. If the Applicant does not possess a professional industry certification, they must have a minimum of three (3) years' experience in at least two of the following areas.*

Examples of Applicant's work and/or description of experience in **network security** (for example, implementation and administration of routers, access control lists, firewalls, intrusion prevention systems, etc.):

From (date):	To (date):	Total time: Years Months

Examples of Applicant's work and/or description of experience in **application security** (for example, secure software development, software QA testing and vulnerability assessment, OWASP, etc.):

From (date):	To (date):	Total time: Years Months

Examples of Applicant's work and/or description of experience in **computer systems security** (for example, implementing and maintaining security controls for computers, servers, or other systems. Include operating systems, versions, and hardware platform identifiers as applicable):

From (date):	To (date):	Total time: Years Months

Examples of Applicant's work and/or description of experience in **auditing information systems and processes, security risk assessment or risk management** (for example assessing security controls on networks, systems, software. Include audit methods and/or frameworks as applicable):

From (date):	To (date):	Total time: Years Months

© 2008-2017 PCI Security Standards Council, LLC

3.2.1 ASV Employee Skills, Experience and Education (continued)

List relevant professional industry certifications currently held (and in good standing) by the Applicant (for example, CISSP, CISM, CISA, GSNA, etc.):

Certification:	Certification number:	Expiry date:
Certification:	Certification number:	Expiry date:
Certification:	Certification number:	Expiry date:

Attach, copy/paste or upload Applicant's Résumé or curriculum vitae (CV).

☐ The Applicant hereby agrees to adhere to the ASV Company's documented process for protection of confidential and sensitive information, which includes adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect confidential and sensitive information against any threats or unauthorized access during storage, processing, and/or communicating of this information.

☐ The Applicant hereby acknowledges and agrees that they have read and understand the PCI SSC Code of Professional Responsibility, and hereby agrees to advocate, continuously adhere to, and support the terms and provisions thereof.

Signature

By signing below, I hereby acknowledge and agree that:

(a) The information provided above is true, accurate and complete; and

(b) I have read and understand the *ASV Qualification Requirements* and will comply with the terms thereof

Applicant Name:		Job Title:	
Applicant signature ↑			*Date* ↑

© 2008-2017 PCI Security Standards Council, LLC