Payment Card Industry (PCI)
Data Security Standard
Qualification Requirements

For Approved Scanning Vendors (ASV)

Version 2.1
December 2013

Document Changes

Date	DSS Version	Description
October 1, 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.

Table of Contents

Document Changes i

1 Introduction 1

1.1 Terminology 1
1.2 Goal 3
1.3 Qualification Process Overview 3
1.4 Document Structure 3
1.5 Related Publications 4
1.6 ASV Application Process 4
1.7 Additional Information Requests 5

2 ASV Business Requirements 6

2.1 Business Legitimacy 6
2.2 Independence 6
2.3 Insurance Coverage 7
2.4 ASV Fees 8
2.5 ASV Agreements 8

3 ASV Capability Requirements 9

3.1 ASV Company – Services and Experience 9
3.2 ASV Employee – Skills and Experience 9

4 ASV Administrative Requirements 12

4.1 Contact Person 12
4.2 Background Checks 12
4.3 Adherence to PCI Procedures 13
4.4 Quality Assurance 13
4.5 Protection of Confidential and Sensitive Information 14
4.6 Evidence Retention 15

5 ASV Initial Qualification and Annual Re-qualification 16

5.1 ASV List 16
5.2 ASV Re-qualification 16
5.3 ASV Remediation Process 16
5.4 ASV Revocation Process 18

Appendix A. PCI ASV Compliance Test Agreement 19

Appendix B. PCI ASV Application Process Checklist 38

Appendix C. Insurance 42

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" ("ASV Companies," as further described below).

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

Validation of 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:

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 firm that has been qualified, and continues to be qualified, by PCI SSC to use an ASV Scan Solution to determine compliance of their Scan Customers with the external vulnerability scanning requirement of *PCI DSS* Requirement 11.2.2 for ASV Program purposes.
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	The testing of an ASV Scan Solution by an ASV Validation Lab to demonstrate for ASV Program purposes that the ASV Scan Solution performs in accordance with the *ASV Program Guide*.
ASV List	The then current list of ASV Companies 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 are not limited, to 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 offered by an ASV Company to validate compliance of a Scan Customer with the external vulnerability scanning requirement of *PCI DSS* Requirement 11.2.2 for ASV Program purposes, including without limitation, all corresponding ASV Company scanning procedures, scanning tool(s), scan reports, processes for exchanging information between the ASV Company and the Scan Customer, and processes used by the applicable ASV Company and its ASV Employees to: • Operate the ASV Scan Solution • Submit the scan report to the Scan Customer and • Review and interpret scan results, as needed.
ASV Validation Lab	A third party testing facility designated by PCI SSC for purposes of evaluating and determining whether ASV Scan Solutions perform in accordance with the *ASV Program Guide*.
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	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	A merchant, service provider that undergoes a quarterly external vulnerability scan performed by an ASV Company for purposes of validating such Scan Customer's compliance with the external vulnerability scanning requirement of *PCI DSS* Requirement 11.2.2 for ASV Program purposes.
Website	The then-current PCI SSC Web site (and its accompanying Web pages), which is currently available at http://www.pcisecuritystandards.org.

1.2 Goal

To be qualified as an ASV Company by PCI SSC, the ASV Company and its ASV Employees and ASV Scan Solution(s) must meet or exceed all applicable ASV Requirements, and the ASV Company must execute the ASV Agreement with PCI SSC. Companies that qualify are identified on PCI SSC's ASV List on the PCI SSC's Website 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 re-qualification 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 three parts: the first involves the qualification of the security company itself. The second relates to the qualification of the company's employee(s) responsible for the PCI Scanning Services. The third consists of the security testing of the company's ASV Scan Solution(s).

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

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

1.4 Document Structure

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

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

Section 2: ASV Company 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 Qualification Maintenance briefly outlines the yearly re-qualification process, as well as remediation and revocation procedures if there is a breach of the ASV Agreement.

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*

1.6 ASV Application Process

In addition to explaining the requirements that an ASV Company and its ASV Employees must meet to be recognized by PCI SSC to perform PCI Scanning Services, 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.

To facilitate preparation of the application package, refer to Appendix B: "ASV Application Process Checklist." All application materials 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 by the ASV Company 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. Applicants should send the completed packages by mail to the following address:

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

E-mail submissions will not be accepted.

Important Note: PCI SSC reserves the right to reject any application from any applicant (company or employee) that PCI SSC determines has committed, within two (2) years prior to

the application date, any conduct that would have been considered a "Violation" (defined in 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, in light of the circumstances.

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 ASV Employees submit additional information or materials in order to demonstrate adherence to applicable requirements or as part of the applicable qualification or re-qualification 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 required information or documentation no later than three (3) weeks from receipt of the corresponding written request.

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 must be recognized as a legal entity.

2.1.2 Provisions

The following information must be provided to PCI SSC:

- Copy of current ASV Company 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 (and ASV principals), and the status and resolution

2.2 Independence

2.2.1 Requirement

The 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.

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

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

- 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 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 Scan Customer, in order to enter into the ASV Agreement or any agreement with any Scan Customer, or to provide ASV-related services.
- The ASV Company must fully disclose in a separate document and attach to the scan report if they perform PCI Scanning Services to customers who use any security-related devices or security-related applications that have been developed or manufactured by the ASV Company, or to which the ASV Company owns the rights, or that the ASV Company has configured or manages, including the following:
  - Application or network firewalls
  - Intrusion detection/prevention systems

  - Database or other encryption solutions
  - Security audit log solutions
  - File integrity monitoring solutions
  - Anti-virus solutions
- The ASV Company must have an internal separation of duties between the scanning service they provide and any managed security services provided to Scan Customers.
- The ASV Company agrees that when the ASV Company recommends remediation actions which 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 a "listed ASV" to market services unnecessary to bring ASV Company subjects into compliance with the *PCI DSS*.
- The ASV Company must not, and agrees that it will not, misrepresent requirements of the *PCI DSS* in connection with its promotion or sales of services to ASV Company clients, or state or imply that the *PCI DSS* requires use of the ASV Company's products or services.

2.2.2 Provisions

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

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

The description must include details with respect to compliance with the independence requirements described in Section 2.2.1 above.

2.3 Insurance Coverage

2.3.1 Requirement

At all times while its ASV Agreement is in effect, the ASV Company shall maintain sufficient insurance, insurers, coverages, exclusions, and deductibles that PCI SSC reasonably requests to adequately insure the Vendor for its obligations and liabilities under the 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 C – Insurance Coverage, which includes details of required insurance coverage.

2.3.2 Provisions

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

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

2.4 ASV Fees

2.4.1 Requirement

Each ASV Company applicant must provide to PCI SSC an Initial Test for New Solution fee (see the Website - PCI SSC Programs Fee Schedule). Notification will be sent providing instructions for enrolling in training, and the ASV Company applicant must provide ASV Training – Initial Qualification fees for a minimum of two employees. The fee check(s) should be made payable to PCI SSC and mailed once the ASV application is approved. See Section 1.6 of this document for the mailing address.

- The Initial Test for New Solution fee, which must be paid in full within 30 days of notification.
- An annual ASV re-qualification test fee for subsequent years.
- For each ASV Employee, a fee for PCI SSC training. This is an annual fee.

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

2.5 ASV Agreements

2.5.1 Requirement

PCI SSC requires that all agreements between PCI SSC and the ASV Company (including the ASV Agreement) be signed by a duly authorized officer of the ASV Company, submitted in unmodified form to PCI SSC, and submitted 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.

3 ASV Capability Requirements

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

3.1 ASV Company – Services and Experience

3.1.1 Requirement

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

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

3.1.2 Provisions

The following information must be provided to PCI SSC:

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

3.2 ASV Employee – Skills and Experience

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

3.2.1 Requirement

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

- 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 examination conducted as part of training. If an ASV Employee fails to pass any exam in connection with such training, the ASV Employee must no longer perform or manage PCI Scanning Services until successfully passing all required exams on a future attempt.

- Possess a minimum of three (3) years of information security experience as follows:
    - A minimum of one (1) year in vulnerability scanning and/or penetration testing
    - At least two (2) years in any two of the following areas of expertise (with a minimum of one year in each discipline):
        - Network security
        - Application security
        - System security
        - IT security auditing
        - IT security risk assessment
- Possess ONE of the following:
    - A current industry-recognized security certification: CISA, CISM, CISSP

      OR
    - An additional two (2) years of information security experience, in at least two of the following areas of expertise, with a minimum of one year in each discipline:
        - Network security
        - Application security
        - System security
        - IT security auditing
        - IT security risk assessment

3.2.2 Provisions

Note: This section is intended to draw out specific experience from the Candidate (defined below). The Candidate must provide examples (including the timeframe) of how their work experience meets the ASV Program requirements. This section is intended to measure the Candidate's skills against the required skills.

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

- A current copy of the Candidate's Résumé or Curriculum Vitae :
- Years of working experience and responsibilities

- Years of experience related to payment industry and responsibilities
- A description of a minimum of three (3) years of information security experience as follows:
    - A description of a minimum of one (1) year in vulnerability scanning and/or penetration testing
    - A description of at least two (2) years in any two of the following areas of expertise (with a minimum of one year in each discipline):
        - Network security
        - Application security
        - System security
        - IT security auditing
        - IT security risk assessment
- ONE of the following:
    - A copy of a current industry-recognized security certification: CISA, CISM, CISSP

      OR
    - A description of an additional two (2) years of information security experience, in at least two of the following areas of expertise, with a minimum of one year in each discipline:
        - Network security
        - Application security
        - System security
        - IT security auditing
        - IT security risk assessment

4 ASV Administrative Requirements

This section describes the 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 must provide PCI SSC with a primary and secondary contact.

4.1.2 Provisions

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

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

4.2 Background Checks

4.2.1 Requirements

The ASV Company must perform a background check satisfying the Minimum Background Check Requirements (described below) when hiring each ASV Employee, to the extent legally permitted within the applicable jurisdiction.

The ASV Company must adhere to all legally permissible background check requirements as required by PCI SSC from time to time.

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

4.2.2 Provisions

The ASV Company must provide the following to PCI SSC to the extent legally permitted within the applicable jurisdiction:

- For each employee to be qualified, a written statement that the ASV Employee successfully completed the background check in accordance with the ASV Company's policies and procedures
- An officer of the ASV Company must sign the ASV Agreement, which includes a statement that the ASV Company will perform background checks for each ASV Employee, in accordance with applicable ASV procedures
- A summary description of current ASV Company personnel background check policies and procedures, to confirm the procedures include at least the following

minimum background check requirements to the extent legally permissible in the applicable jurisdiction (the "Minimum Background Check Requirements"):

- Verification of aliases (when applicable)
- Review of records of any criminal activity, arrests, or convictions, updated annually
- Misdemeanors and non-US equivalents are allowed, but felonies and non-US equivalents automatically disqualify an employee from consideration as an ASV Employee

4.3 Adherence to PCI Procedures

4.3.1 Requirements

- The ASV report must follow the procedures documented in the *ASV Program Guide*
- An officer of the ASV Company must sign the ASV Agreement, which includes a statement that the ASV Company will adhere to all ASV Requirements

4.4 Quality Assurance

4.4.1 Requirements

- The ASV Company must have an implemented quality assurance process, documented in a quality assurance manual that includes a description of the controls for quality assurance reviewing of processes and documentation and controls to maintain the integrity of the scanning tools.
- The ASV Company must adhere to all PCI SSC quality assurance requirements.
- The ASV Company must provide an ASV Feedback Form to their Scan Customer at the completion of the PCI Scanning Service. The ASV Feedback Form is an on-line form available on the PCI SSC Website.
- PCI SSC reserves the right to conduct site-visits and audit the ASV Company at the discretion of the PCI SSC.
- Upon request, the ASV Company must provide the quality assurance manual to PCI SSC.

4.4.2 Provisions

The ASV Company must provide the following to PCI SSC:

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

- Requirement that ASV Employees must adhere to the *ASV Program Guide*
- Requirement that the ASV Company has controls to maintain the integrity of their ASV Scan Solution tool(s). ASV Scan Solutions 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 an alert when changes are made
    - Ensure the ASV Company's systems cannot be used to gain unauthorized access to a Scan Customer's environment

4.5 Protection of Confidential and Sensitive Information

4.5.1 Requirements

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

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

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

4.5.2 Provisions

The ASV Company must provide the following:

- Description of the ASV Company's confidential and sensitive data protection handling practices, including physical, electronic, and procedural safeguards, including at least the following:
    - Systems storing customer data do not reside on Internet accessible systems
    - Protection of systems storing customer data by adequate network and application layer controls including a firewall and IDS/IPS
    - The following physical and logical access controls:
        - Restricting access (for example, via locks) to the physical office space
        - Restricting access (for example, via locked file cabinets) to paper files
        - Restricting logical access to electronic files by role-based access control
    - Encryption of sensitive customer information when transmitted over the Internet either by e-mail or other means
    - Secure transport and storage of backup media

- Encryption of customer data on employees' laptops
- Description of requirements and processes used to ensure employee confidentiality of customer data, including a (blank) copy of confidentiality agreements required to be signed by employees
- An officer of the ASV Company must sign the ASV Agreement, which includes a statement that the ASV Company will adhere to all ASV Requirements

4.6 Evidence Retention

4.6.1 Requirements

The ASV Company must securely maintain digital and/or hard copies of case logs, scanning results and work papers, notes, and any technical information that was created and/or obtained during the PCI Scanning Services for a minimum of three (3) years.

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

This information must be available upon request by PCI SSC and its Affiliates for a minimum of three (3) years.

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

4.6.2 Provisions

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

5 ASV Initial Qualification and Annual Re-qualification

This section describes the process after initial qualification and activities related to the annual ASV Company and Employee re-qualification. This section includes 1) the ASV List, 2) annual maintenance of ASV Company and Employee qualification, 3) remediation, if necessary, and 4) revocation, if necessary, of an ASV Company's or Employee's qualification.

5.1 ASV List

Once a company has met all requirements specified in this document, PCI SSC will add the ASV Company to the ASV List. Only those ASV Companies on this list are authorized by PCI SSC to perform PCI Scanning Services. This list is posted on the PCI SSC Website.

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

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

The company will have 30 days from the date of notification to appeal the decision. Appeals must be addressed to PCI SSC General Manager. If a company's appeal is denied, its name will not be placed on the ASV List.

5.2 ASV Re-qualification

5.2.1 Requirements

All ASV Companies and Employees must be re-qualified by PCI SSC on an annual basis, based on the ASV Company's original qualification date. Re-qualification by PCI SSC is based on payment of annual fees, proof of training attended, achieving a passing result on the annual ASV Lab Scan Test and satisfactory feedback from the ASV Company Scan Customers (the merchants or service providers that received PCI Scanning Services) to PCI SSC.

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

5.2.2 Provisions

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

- Proof of information systems vulnerability assessment training within the last 12 months to support professional certifications (even if the employee does not have professional certifications), of a minimum 20 hours per year and 120 hours over the rolling three year period. This is in addition to training provided by PCI SSC.
- Payment of annual re-qualification fees (fees can be found on the Website – PCI SSC Programs Fee Schedule).

5.3 ASV Remediation Process

ASV Companies that do not meet all applicable ASV Requirements may be required to participate in remediation. When an ASV Company qualifies for remediation, the Primary Contact will be notified and its listing on the ASV List will be flagged (e.g. updated to show the ASV Company in red).

The Remediation Statement on the Website affirms the Council's position on remediation, and any external queries about the ASV Company's status should be directed either to that statement, or to the ASV Program Manager. ASV Companies in remediation may continue to perform PCI Scanning Services unless otherwise instructed by PCI SSC in connection with the remediation process.

Issues such as failure to submit annual re-qualification fees, failure to meet annual training requirements, failure to meet Continuing Education (CE) requirements or failure to pass the annual ASV Lab Scan Test requirement within 30 days after the re-qualification date will result in remediation. ASV Companies who fail to meet such requirements will remain in remediation until the issue is resolved or until 60 days past the re-qualification date.

ASV Companies who are unable to resolve their issues 60 days past the re-qualification date may be removed from the ASV List. ASV Companies that have been removed from the ASV List in connection with remediation will receive an e-mail notifying them that they are no longer an ASV Company and are not recognized by PCI SSC to perform PCI Scanning Services. ASV Companies that are removed from the ASV List as part of the remediation process (for any reason other than failure to pass the annual ASV Lab Scan Test) and desire to be reinstated must re-apply to the ASV Program.

Failure to pass the Annual ASV Lab Scan Test

ASV Companies are encouraged to begin the process of re-qualification at least 60 days prior to their re-qualification date.

ASV Companies which have not passed the annual ASV Lab Scan Test within 30 days after their re-qualification date will be placed in remediation. ASV Companies which do not pass the annual ASV Lab Scan Test within 60 days past their re-qualification date will be removed from the ASV List. A de-listed company is no longer an ASV Company and is not recognized by PCI SSC to provide PCI Scanning Services.

ASV Companies which have not passed the annual ASV Lab Scan Test within 60 days past their re-qualification date may continue to attempt to pass the ASV Lab Scan Test for up to 120 days past their re-qualification date without the need to re-apply to the ASV Program. Under no circumstances can an ASV Company re-test at the ASV Lab more than 120 days past their re-qualification date; they will be required to re-submit their application to the ASV Program.

If an ASV Company fails three consecutive ASV Lab Scan Tests during the re-qualification process, they will be removed from the ASV List, will no longer be recognized by PCI SSC to perform PCI Scanning Services as an ASV Company, and cannot re-apply to the ASV Program for six months.

Unfavorable feedback

Unfavorable feedback is handled on a case-by-case basis and may result in qualifying an ASV Company for remediation.

5.4 ASV Revocation Process

Each of the events below is an example of a "Violation" (as defined in the ASV Agreement) that may result in immediate Revocation of ASV Company qualification (including removal from the ASV List), subject to reinstatement pending a successful appeal in accordance with the ASV Agreement, and/or termination of the ASV Agreement. This list is not exhaustive. Among other things, ASV Company qualification may be revoked if PCI SSC determines that the ASV Company is in breach of the ASV Agreement, including but not limited to:

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

When ASV Company qualification is revoked, the ASV Company will have 30 days from the date of notification to appeal the revocation. Appeals must be addressed to the PCI SSC General Manager.

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

- The ASV Company's name will be removed from the ASV List.
- PCI SSC may notify third parties, including but not limited to Members (defined in the ASV Agreement).

Appendix A. PCI ASV Compliance Test Agreement

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

PCI SSC and Vendor are hereinafter each referred to as a "Party" and collectively as the "Parties".

RECITALS

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

B. PCI SSC offers a global security solution called the PCI SSC Approved Scanning Vendor Compliance Test Program ("ASV Program"), which provides security compliance solution vendors with the ability to provide PCI Scanning Services (defined in the ASV Qualification Requirements) to deploy security compliance programs to assist their Scan Customer to better protect against illegitimate network intrusions and account data compromises (collectively, "Vendor Services").

C. PCI SSC publishes the PCI DSS (defined below).

D. Vendor is the provider of one or more ASV Scan Solutions that it believes are compliant with the PCI DSS.

E. PCI SSC is willing to assist and to check whether such ASV Scan Solutions are compliant with the PCI DSS and Vendor meets the requirements for PCI SSC-approved scanning vendor companies ("ASV Companies"). In case an ASV Scan Solution is deemed compliant with the PCI DSS and Vendor meets such requirements, Vendor will be entitled to present itself to Scan Customers as an ASV Company with respect to such ASV Scan Solution in the framework of the ASV Program, as provided in this Agreement.

F. Vendor has submitted an application package, requesting participation in the ASV Program, and PCI SSC has determined that Vendor is eligible to move to the initial approval Testing phase of the ASV Program.

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

1 Definitions

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

"**ASV Requirements**" has the meaning ascribed to it in the ASV Qualification Requirements;

"**ASV Qualification Requirements**" means 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;

"**Compliance Notification**" shall mean a letter or electronic correspondence in the form attached as Schedule 1 (or in such other form as PCI SSC may approve from time to time), which is hereby incorporated into this Agreement;

"Confidential Information" shall mean (i) all terms of this Agreement; (ii) any and all information designated in this Agreement as Confidential Information; (iii) any and all originals or copies of, any information that either Party has identified in writing as confidential at the time of disclosure; and (iv) any and all Personal Information, proprietary information, merchant information, technical information or data, scan reports, trade secrets or know-how, information concerning either Party's past, current, or planned products, services, fees, finances, member institutions, Issuers, Acquirers, concepts, methodologies, research, experiments, inventions, processes, formulas, designs, drawings, business activities, markets, plans, customers, equipment, card plastics or plates, software, source code, hardware configurations or other information disclosed by either Party or any Member, or their respective directors, officers, employees, agents, representatives, independent contractors or attorneys, in each case, in connection with the ASV Program or other PCI SSC activities 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 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, or Member or third party information relating to a natural person received in connection with the ASV Program or other PCI SSC activities, 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;

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

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

"**Participating Payment Brand**" means a payment card brand that, as of the time in question, is also a Member and owner of PCI SSC or affiliate thereof. Participating

Payment Brands as of the release of this version of the Agreement were American Express Travel Related Services Company, Inc., DFS Services LLC, JCB Advanced Technologies, Inc., MasterCard International Incorporated, Visa International Service Association (and their affiliates);

"**PCI DSS**" is defined in the ASV Qualification Requirements;

"**ASV Scan Solution**" is defined in the ASV Qualification Requirements. Each ASV Scan Solution is identified and referred to in the applicable Compliance Notification (as further described in Section 5.1(b) below);

"**Testing**" means evaluating an ASV Scan Solution to determine whether or not it complies with the PCI DSS for ASV Program purposes; "Test" and "Tested" will be interpreted accordingly;

"**Scan Customer**" means any person or entity for which Vendor performs Testing, 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"); and

"**Website**" Means the then-current PCI SSC Web site (and its accompanying Web pages), which is currently available at http://www.pcisecuritystandards.org.

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

1.3 This Agreement is comprised of the following:

Sections 1 to 14

Schedule 1: Compliance Notification (sample)

2 Vendor Services and obligations

2.1 Subject to the terms and conditions of this Agreement, while Vendor is in Good Standing (defined below) or as otherwise expressly approved by PCI SSC in writing, PCI SSC hereby approves Vendor to perform Vendor Services for Scan Customers in accordance with the ASV Program using those of Vendor's ASV Scan Solutions that appear on PCI SSC's then current published registry of validated ASV Scan Solutions. Vendor shall provide all reasonable assistance as well as accurate information and documentation to PCI SSC and its agents as may be needed for the purpose of Testing and the ASV Program.

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

2.3 Vendor acknowledges and agrees that it shall only advertise, offer, or use for ASV Program purposes those ASV Scan Solutions that have been Tested and qualified by PCI SSC, and that it shall use such ASV Scan Solutions in accordance with Section 5.1(b). Consequently,

Vendor shall immediately inform PCI SSC of any significant or material change in any ASV Scan Solution as provided in Section 3.1.

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

2.5 Vendor shall make nonrefundable payment to PCI SSC of all applicable ASV Program Fees (defined in the ASV Qualification Requirements) in accordance with the ASV Qualification Requirements. Vendor acknowledges that PCI SSC may review and modify these fees at any time and from time to time. Whenever a change in such fees occurs, PCI SSC shall notify Vendor in accordance with the terms of Section 12 of this Agreement. Such change(s) will be effective immediately after the date of PCI SSC's notification of such changes. However, should Vendor not agree with such change(s), Vendor shall have the right to terminate this Agreement in accordance with the provisions of Section 6.2(iii) (A) at any time within thirty days of delivery of the aforementioned notice. Except to the extent otherwise expressly provided in the ASV Qualification Requirements, all ASV Program Fees must be paid in US dollars (USD) to PCI SSC as specified on the applicable PCI SSC invoice. Vendor acknowledges and agrees that the ASV Program 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, excluding tax on PCI 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.

2.6 Vendor shall comply with all ASV Requirements and agrees to monitor the Website at least weekly for changes to the ASV Qualification Requirements and the ASV Program Guide (defined in the ASV Qualification Requirements), and to implement all such changes within 15 days of the effective dates thereof.

3 Terms and conditions of Testing

3.1 In accordance with the terms of Section 2.3 (regarding Vendor's obligationto inform PCI SSC of any significant or material change in each ASV Scan Solution), PCI SSC may in its sole discretion (i) determine that such ASV Scan Solution is deemed to remain compliant by sending a new Compliance Notification or (ii) require Vendor to (a) resubmit a modified ASV Scan Solution for a new Testing within one (1) month of receipt by PCI SSC of said information given pursuant to Section 2.3 and (b) pay all applicable ASV Program Fees for such new Testing.

3.2 Notwithstanding Section 3.1, if at any time PCI SSC believes that an ASV Scan Solution is no longer compliant with the PCI DSS, PCI SSC shall be entitled to require Vendor to resubmit such ASV Scan Solution for a new Testing within three (3) months of such request from PCI SSC and subject to Vendor's payment of all applicable ASV Program Fees.

3.3 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.

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

3.5 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, in its discretion. Additionally, PCI SSC may from time to time require Vendor to provide a representative to attend any mandatory training programs in connection with the ASV Program, which may require the payment of attendance and other fees.

3.6 Notwithstanding anything to the contrary in Section 6 of this Agreement, in order to assist in ensuring the reliability and accuracy of Vendor's testing and assessment procedures for Scan Customers, Vendor hereby agrees to comply with all quality assurance procedures and requirements established or imposed upon Vendor by PCI SSC from time to time (including but not limited to conditions and requirements imposed in connection with remediation (further described in the ASV Qualification Requirements) or any other qualification status) and that, within 15 days of any written request by PCI SSC or any Participating Payment Brand (each a "Requesting Organization"), except to the extent prohibited by applicable law, Vendor agrees to provide to such Requesting Organization such Scan Customer Testing and Assessment Materials (defined below) as such Requesting Organization may reasonably request with respect to: (i) if the Requesting Organization is a Participating Payment Brand, any Scan Customer for which Vendor has performed Scan Customer testing and/or assessment for ASV Program purposes and that is a Financial Institution of such Participating Payment Brand, Issuer of such Participating Payment Brand, Merchant authorized to accept such Participating Payment Brand's payment cards, Acquirer of accounts of Merchants authorized to accept such Participating Payment Brand's payment cards or Processor performing services for such Participating Payment Brand's Financial Institutions, Issuers, Merchants or Acquirers or (ii) if the Requesting Organization is PCI SSC, any Scan Customer for which Vendor has performed Scan Customer testing and/or assessment as part of the ASV Program. Each agreement between Vendor and each of its Scan Customers (each a "Scan Customer Agreement") shall include such provisions as may be necessary 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 Scan Customer Agreement or otherwise) that might tend to nullify, impair or render unenforceable Vendor's right to disclose such Scan Customer Testing and Assessment Materials as required by this Section. Any failure of Vendor to comply with this Section 3.6 shall be deemed to be a material breach of this Agreement for purposes of Section 7.3(b)(i), and upon any such breach, PCI SSC may remove Vendor's name from the ASV List and/or terminate this Agreement in its sole discretion. Additionally, Vendor agrees to comply with all applicable quality assurance standards, requirements, policies and procedures established by PCI SSC from time to time, including without limitation, those relating to probation, fines, penalties, remediation, suspension and revocation. For purposes of the foregoing, "Scan Customer Testing and Assessment Materials" means (1) all Testing results, reports and related information, materials and assessment results generated and/or obtained in connection with Vendor Services, including without limitation, all work papers, notes and other materials and information generated or obtained in connection therewith and (2) complete and accurate copies of each Scan Customer Agreement; provided that such materials may be redacted in accordance with applicable PCI SSC policies and procedures, including but not limited to, redaction of pricing, delivery process and/or confidential and proprietary information of the Scan Customer, so long as (A) such redaction is in accordance with PCI SSC policy, (B) the redacted information does not obscure any language that may tend to nullify, impair or render unenforceable Vendor's

right to disclose Scan Customer Testing and Assessment Materials to PCI SSC as required by this Section, and (C) upon request, Vendor provides to PCI SSC a written certification that such redaction complies with preceding Section (B) executed by an executive officer of Vendor.

3.7 Vendor shall allow PCI SSC or its designated agents access during normal business hours during the Term (as defined in Section 7.1) and for a period of six (6) months thereafter to perform audits of Vendor's facilities, operations and records regarding Vendor Services to determine whether Vendor has complied with this Agreement. Vendor 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 or its designated agents 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. Any failure of Vendor to comply with this Section 3.7 shall be deemed a material breach of this Agreement for purposes of Section 7.3(b) (i), and upon any such breach, PCI SSC may remove Vendor's name from the ASV List and/or terminate this Agreement in its sole discretion.

4 Intellectual Property Rights

4.1 All Intellectual Property Rights, title and interest in and to the ASV Program, the PCI DSS, the PCI Materials (defined in Section 10.1 below), all materials Vendor receives from PCI SSC, and each portion, future version, revision, extension, and improvement of 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 6, so long as Vendor is in Good Standing, 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 agreement between PCI SSC and Vendor.

4.2 All Intellectual Property Rights, title and interest in all assessment results performed by or on behalf of PCI SSC (e.g. results of ASV Lab Scan Tests (defined in the ASV Qualification Requirements)) are and at all times shall remain the property of PCI SSC. Vendor may use and disclose, subject to the provisions of Section 6, the assessment results only for the purposes of this Agreement. Vendor shall not revise, abridge, modify or alter such assessment results. Vendor shall not assert or imply that assessment results other than those upon which a Compliance Notification was issued by PCI SSC are connected or related to such Compliance Notification. Vendor shall have the right to make copies of a given 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.

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

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

5 Advertising and Promotion

5.1 ASV List and Use of ASV Marks.

(a) As long as Vendor is in Good Standing (as defined below) as an ASV Company, PCI SSC may, at its sole discretion, display the identification of Vendor and each ASV Scan Solution of Vendor that has been qualified by PCI SSC for ASV Program Purposes, together with information as to such qualification, in the ASV List (defined in the ASV Qualification Requirements). Vendor shall provide all requested information necessary to ensure to PCI SSC's satisfaction that the identification and information provided on the ASV List are accurate. Vendor shall be deemed to be in "Good Standing" as an ASV 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 PCI DSS, and Vendor is not in breach of any of the terms or conditions of remediation or this Agreement (including without limitation, all provisions regarding compliance with the ASV Requirements and payment).

(b) If Vendor is in Good Standing and PCI SSC issues a Compliance Notification (in the form set out in Schedule 1) confirming that a given ASV Scan Solution 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 as an ASV Company, Vendor's rights pursuant to the preceding sentence shall immediately cease and the ASV Scan and related Vendor's information shall be removed from the ASV List. In the event that Vendor is otherwise in Good Standing as an ASV 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 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 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) Vendor shall make no use of any PCI SSC trademark, service mark, logo or other indicia of origin or source (collectively, "Marks") 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, 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, the Vendor Services or products (including but not limited to Vendor's ASV Scan Solution(s)) or the functionality, quality or performance of any aspect of any of the foregoing. Except with respect to (A) factual references to the ASV Program or to PCI Materials that Vendor includes from time to time in its contracts with Scan Customers and that are required or appropriate in order for Vendor to accurately describe the nature of the Vendor Services that Vendor will provide pursuant to such contracts, (B) references permitted pursuant to Section 5.1(b) above and (C) references that PCI SSC has expressly authorized pursuant to a separate written agreement with Vendor, Vendor may not publish, disseminate or otherwise make available any statements, materials or products (in any form) that refer to the PCI DSS, the PCI Materials or any portion of the foregoing, Vendor's listing on the ASV List, PCI SSC, or any PCI SSC Mark, unless such statement, material or product has been reviewed and approved in writing by PCI SSC prior to such publication or other dissemination, in each instance. 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 dissemination of promotional or other materials or publicity in violation of this Section 5 shall be deemed a material breach of this Agreement and upon any such violation, PCI SSC may remove Vendor's name from the ASV List and/or terminate this Agreement in its sole discretion.

5.2 Uses of ASV Company 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 the ASV Program. Vendor warrants and represents that it has authority to grant to PCI SSC and the Participating Payment Brands the right to use its name and designated marks as contemplated herein.

5.3 No Other Rights Granted. Except as expressly stated in this Section 5, no rights to use any Party's or Member's marks or other intellectual property are granted, and each Party respectively reserves all rights therein. Without limitation of the foregoing, except as expressly stated herein, no rights are granted to Vendor to any intellectual property in the PCI DSS, any PCI Materials or otherwise.

6 Confidentiality

6.1 General Restrictions

(a) Each Party (the "Receiving Party") agrees that all Confidential Information received from the other Party (the "Disclosing Party") shall: (i) be treated as confidential; (ii) be disclosed only to those Members, officers, employees, legal advisers and accountants of the Receiving Party who have a need to know and be used thereby solely as required in connection with (A) the performance of this Agreement or (B) the operation of such Party's or Member's 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 6.

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

6.2 Scan Customer Data

To the extent any data or other information obtained by Vendor relating to any Scan Customer in the course of providing Vendor Services is subject to any confidentiality restriction between Vendor and such Scan Customer, the applicable agreement containing

such restriction (and in the absence of any such agreement, a separate written agreement between Vendor and such Scan Customer) must (i) permit Vendor to disclose such information to PCI SSC and/or its Members, as requested by the Scan Customer, (ii) to the extent any Member obtains such information in accordance with preceding Section 6.2(a)(i), permit each Member to disclose such information on an as needed basis to other Members and to such Members' respective member Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies and (iii) permit Vendor to disclose any such information as necessary to comply with its obligations and requirements pursuant to Section 3.6 above. Accordingly, notwithstanding anything to the contrary in Section 6.1(a), 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 Members in accordance with this Section 6.2, and such Members may in turn disclose such information to their respective member Financial Institutions and other Members. Vendor hereby consents to such disclosure by PCI SSC and its Members. As between any Member, on the one hand, and Vendor or any Scan Customer, on the other hand, the confidentiality of any 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.

6.3 Personal Information

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

6.4 Return

Within fourteen (14) days after notice of termination of this Agreement or demand by PCI SSC, Vendor shall return to PCI SSC all property and Confidential Information of PCI SSC and of third parties provided 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 working 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, a certificate of destruction may be provided instead, with sufficient detail regarding the items destroyed, destruction date, and assurance that all copies also were destroyed.

6.5 Remedies

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

7 Term and Termination

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

7.2 PCI SSC shall have the right, without prejudice to its other rights or remedies, to terminate this Agreement immediately by written notice to Vendor: (a) if Vendor shall have failed to pay in accordance with the terms of this Agreement any fee due and that fee remains unpaid for fifteen (15) days after receiving written notice from PCI SSC that it has not been paid; (b) if PCI SSC determines, at PCI SSC's discretion, that Vendor has failed to comply with any of Vendor's obligations pursuant to Section 2.6 of this Agreement; (c) if PCI SSC determines, in its sole discretion, that Vendor has failed to achieve successful results in connection with (i) the initial Testing, (ii) the annual maintenance Testing performed pursuant to Section 2.4 and/or (iii) any Testing performed pursuant to Section 3.1 or 3.2; (d) if Vendor fails to resubmit a given ASV Scan Solution within the timelines provided in Sections 2.4, 3.1 and 3.2; (e) in accordance with Section 7.5 below; or (f) if PCI SSC ceases to operate the ASV Program, whether with or without replacing it with any other program; provided, however, that if PCI SSC has terminated pursuant to Section 7.2(a), (b), (c) or (d) above, and Vendor thereafter determines that it has satisfied each of the requirements set forth in the said Sections 7.2(a) through (d), Vendor may request a new compliance review by PCI SSC in accordance with Section 3.2. PCI SSC may undertake such review, at PCI SSC's sole discretion, and if PCI SSC determines that Vendor is in compliance with all applicable ASV R, 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 payment of all outstanding ASV Program Fees (if any).

7.3 Either Party shall have the right to terminate this Agreement (a) effective as of the last day of the then current Term, for any or no reason, upon at least thirty (30) days notice to the other Party or (b) at any time by giving thirty (30) days prior written notice to the other Party: (i) if such Party determines that the other Party (the "Defaulting Party") is in material breach of any of its obligations under this Agreement and either that breach is incapable of remedy or the Defaulting Party shall have failed to remedy that breach within thirty (30) days after receiving written notice from the other Party requiring it to remedy that breach on the understanding that consent to extend the remedy period shall not be unreasonably be withheld, so long as the Defaulting Party has commenced remedy during the said thirty (30)

days and pursues remedy of the breach on a best efforts basis; (ii) upon the other Party's insolvency, receivership, or voluntary or involuntary bankruptcy (or the institution of any proceeding therefore), or any assignment for the benefit of the other Party's creditors or on the occurrence of any event which is analogous to any of the above under the laws of the jurisdiction in which such Party is incorporated; or (iii) in the event that Vendor does not agree with (A) modified fees as provided in Section 2.5 or (B) any unilateral modification, alteration or amendment of this Agreement as provided in Section 14.2.

7.4 Termination of this Agreement shall automatically imply termination of Vendor's qualification as an ASV Company. Upon any such termination or any expiration of this Agreement: (i) Vendor and each Vendor ASV Scan Solution shall be removed from the ASV List, (ii) Vendor shall immediately cease all advertising and promotion of its status as an ASV Company and all references to the PCI DSS and other PCI Materials; (iii) Vendor shall immediately cease soliciting for and performing all Vendor Services, provided that, if and to the extent instructed by PCI SSC in writing, Vendor shall complete any and all Vendor Services for which Vendor was engaged prior to such expiration or the notice of termination; (iv) to the extent Vendor is instructed to complete any Vendor Services pursuant to preceding Section (iii), Vendor will complete such Vendor 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 Vendor Services provided prior to or after termination; (vi) 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 Vendor 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 (iii) above; (vii) 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 Vendor Services of such expiration or termination; (viii) 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 Vendor Services immediately prior to such expiration or notice of termination and the status of such Vendor Services for each; and (ix) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify third parties of such termination or expiration and the reason(s) therefor, including but not limited to any of its Members and/or their acquirers, and any Scan Customers. The provisions of Sections 1, 2.5, 3.5, 3.7 (subject to the period set forth therein), 4, 5.1(c), 5.3, 6, 7.4, 9, 10 and 12 through 14 of this Agreement shall survive the expiration or termination of this Agreement for any or no reason.

7.5 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 ASV Company qualification as established by PCI SSC from time to time (satisfaction of any such condition, a "Violation"), including without limitation, any of the conditions described in Section 5.2 of the ASV Qualification Requirements, PCI SSC may, effective immediately upon notice of such Violation to Vendor, revoke Vendor's qualification as an ASV Company ("Revocation"), and such qualification shall be subject to reinstatement pending a successful appeal in accordance with Section 7.5(b) below and applicable PCI SSC policies and procedures. In the event of any Revocation: (i) Vendor will be removed from the ASV List and/or its listing may be annotated as PCI SSC deems appropriate; (ii) Vendor shall comply with Section 7.4 above in the manner otherwise required if this Agreement had been terminated effective as of the date of Revocation; (iii) Vendor shall, within

fifteen (15) days of such Revocation, inform all Scan Customers with which it is then engaged to perform testing, scanning or assessment services as part of the ASV Program of such Revocation and, if applicable, of any conditions, restrictions or requirements of such Revocation that may impact its ability to perform Vendor Services for Scan Customers going forward; (iv) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify third parties of such Revocation and the reason(s) therefor, including but not limited to any of its Members and/or their acquirers, and any Scan Customers; and (v) Vendor will have a period of thirty (30) days from the date Vendor is given notice of the corresponding Violation to submit a written request for appeal to the PCI SSC General Manager. In the event Vendor fails to submit such a request within the allotted 30-day period, PCI SSC will deliberate without an appeal and may terminate this Agreement effective immediately as of the end of such period.

(b) 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 of Vendor. All determinations of PCI SSC regarding Revocation and any related appeals shall be final and binding upon Vendor. If PCI SSC determines that termination is warranted, this Agreement shall terminate effective immediately upon such determination. If PCI SSC determines that no action is required of Vendor, the Revocation shall be lifted and Vendor shall be reinstated on the ASV List. If PCI SSC determines that remedial action is required, PCI SSC may establish a date by which such remedial actions must be completed, provided that 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 actions; provided 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 this Agreement effective immediately as of such date.

8 Representations and warranties

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

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

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

9 Indemnification

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

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

9.2 Vendor's indemnity obligations are contingent on PCI SSC'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 its Members may, at their own cost and expense, participate in such investigation, trial and defense and any appeal arising there from or assume the defense of any Indemnified Party. In any event, PCI SSC will have the right to approve counsel engaged by Vendor to represent any Indemnified Party, which approval shall not be unreasonably withheld. Vendor will not enter into any settlement of a claim that imposes any obligation or liability on PCI SSC or any other Indemnified Party without such Indemnified Party's prior written consent.

10 No warranties - Limitation of liability

10.1 PCI SSC PROVIDES THE PCI DSS, ASV PROGRAM, PROGRAM GUIDE, ASV QUALIFICATION REQUIREMENTS, WEBSITE AND ALL RELATED AND OTHER MATERIALS PROVIDED OR OTHERWISE MADE ACCESSIBLE IN CONNECTION WITH THE ASV 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 THE PCI MATERIALS.

10.2 PCI SSC MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING WITHOUT LIMITATION, THE PCI MATERIALS OR ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR THE ASV PROGRAM. PCI SSC SPECIFICALLY DISCLAIMS, AND VENDOR EXPRESSLY WAIVES, ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THIS AGREEMENT, THE PCI MATERIALS, ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR THE ASV 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 (WHETHER OR NOT PCI SSC HAS BEEN ADVISED, HAS REASON TO KNOW, OR IS OTHERWISE IN FACT AWARE OF ANY INFORMATION). THE FOREGOING DISCLAIMER IS MADE BY PCI SSC FOR

ITSELF AND, WITH RESPECT TO EACH SUCH DISCLAIMER, ON BEHALF OF ITS LICENSORS AND MEMBERS.

10.3 In particular, without limiting the foregoing, the accuracy, completeness, sequence or timeliness of the ASV Program cannot be guaranteed. In addition, PCI SSC makes no representations or warranties 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 the ASV Program, or (ii) system performance and effects on or damages to software and hardware in connection with any use of the ASV Program.

10.4 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 2.5.

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

11 Insurance

At all times while this Agreement is in effect, Vendor shall maintain insurance in such amounts, with such insurers, coverages, exclusions and deductibles which, at a minimum, meet the applicable insurance requirements for U.S. or European Union ASV Companies, as applicable, as may be required by PCI SSC, including without limitation the requirements set forth in Appendix C 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. Vendor hereby represents and warrants that it meets all applicable insurance requirements as provided for in this Section 11 and that such insurance shall not be cancelled or modified without giving PCI SSC at least thirty (30) 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 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.

12 Notices

All notices required under this Agreement shall be in writing and shall be deemed given when delivered personally, by overnight delivery upon written verification of receipt, by facsimile transmission upon electronic confirmation of transmission, or 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 Principal Contact and at the location set forth on the signature page of this Agreement. Notices from Vendor to PCI SSC shall be sent to the attention of General Manager at the address set forth on the first page of this Agreement. A Party may change its addressee and address for notices by giving notice to the other Party pursuant to this Section 12.

13 Consent to receive records electronically

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

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

14 Miscellaneous

14.1 *Entire Agreement*. The Parties agree that this Agreement, including documents incorporated herein by reference, is the exclusive statement of the agreement between the Parties with respect to the ASV Program, which supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the Parties with respect to such subject matter (including without limitation, if applicable, each prior PCI ASV Compliance Test Agreement between Vendor and PCI SSC).

14.2 *Amendment*. 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 in accordance with the provisions of Section 7.3(b)(iii)(B) upon written notice of its intention to so terminate to PCI SSC (regardless of the notice requirements set forth in Section 7.3(b)). Any such unilateral modification, alteration or amendment will be effective as of the end of such thirty (30) day period.

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

14.4 *Assignment.* This Agreement is a personal services Agreement and the Vendor may not assign or delegate this Agreement or any of its rights or obligations under this Agreement, including by subcontracting, without the prior written consent of PCI SSC, which consent PCI SSC may grant or withhold in its absolute discretion.

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

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

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

14.8 *Dispute Settlement- Jurisdiction- Governing Law.* Any dispute in any way arising out of or in connection with the interpretation or performance of this Agreement, which cannot be

amicably settled within thirty (30) days of the written notice of the dispute given to the other Party by exercising the best efforts and good faith of the Parties, shall be finally settled by the courts of Delaware (United States of America) in accordance with Delaware law without resort to its conflict of laws provisions. Each of the Parties irrevocably submits to the nonexclusive jurisdiction of the United States District Courts for the State of Delaware and the local courts of the State of Delaware and waives any objection to venue in said courts.

14.9 *Counterparts*. This Agreement may be signed in two or more counterparts, 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.

14.10 *Conflict*. In the event of a conflict between this Agreement and the ASV Qualification Requirements, this Agreement shall control.

14.11 *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]

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

Vendor			
Vendor Name:			
Location/Address:			
State/Province: City:	Country:	Postal Code:	
Principal Contact			
Person's Name:			
Direct Telephone Number:		Fax:	
Location/Address:			
State/Province: City:	Country:	Postal Code:	
Applicable Fees:			
Vendor's Signature			
Vendor's Officer Signature ↑		*Date* ↑	
Applicant Officer Name:	Title:		

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

Schedule 1: 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 http://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**********

Appendix B. PCI ASV Application Process Checklist

This checklist is provided as a tool to help you organize the PCI Approved Scanning Vendor Company application information that must be submitted along with your completed/signed PCI Approved Scanning Vendor (ASV) Compliance Test Agreement. All application materials must be submitted in English or with a certified English translation.

ASV Business Requirements

Requirement	Information/Documentation Needed
Legitimate Business Entity	☐ Copy of business license ☐ Year of incorporation ☐ Location(s) of office(s) ☐ Written statement describing any past or present allegations or convictions of any fraudulent or criminal activity involving the security company and its principles
Independence	☐ Company signature on the ASV Agreement ☐ Description of company's practices to maintain independence
Insurance Coverage	☐ Company signature on the ASV Agreement ☐ Proof of insurance coverage that meets PCI SSC requirements, as per Appendix C, including: • Commercial General Liability; and • Technology Errors and Omissions and Cyber-Risk Liability with world-wide coverage

ASV Capability Requirements

Requirement	Information/Documentation Needed
Company Services and Experience	☐ High-level description of the security company's experience and knowledge with information security and payment system scanning engagements ☐ High-level description of the security company's experience relevant areas of specialization within information security, scanning engagements preferably related to the payment systems ☐ A description of the total number of employees, the number and specific roles of the information security employees on staff and the percentage of their time dedicated to performing PCI Scanning Services ☐ Brief description of core business offerings ☐ A description of the size and types of market segments in which the ASV Company tends to focus, such as, Fortune 500, financial industry, insurance industry, and small-medium sized business ☐ List of languages supported by the security company ☐ A description of company's practices to maintain scanning independence, including but not limited to, practices, organizational structure/separation, employee education, etc., in place to prevent conflicts of interest in a variety of scenarios ☐ Two client references from recent security engagements

Requirement	Information/Documentation Needed
Company Employee Skills and Experience	☐ Current copy of Résumé or Curriculum Vitae ☐ Years of working experience and examples of work or a description of the Candidate's responsibilities ☐ Years of working experience related to payment card industry and examples of work or a description of the Candidate's responsibilities ☐ Examples of work or a description of a minimum of three (3) years of information security experience as follows: • Examples of work or a description of a minimum of one (1) year in vulnerability scanning and/or penetration testing • Examples of work or a description of at least two (2) years in any two of the following areas of expertise (with a minimum of one year in each discipline): ▪ Network security ▪ Application security ▪ System security ▪ IT security auditing ▪ IT security risk assessment ☐ ONE of the following: • A copy of a current industry-recognized security certification: CISA, CISM, CISSP OR • Examples of work or a description of an additional two (2) years of information security experience, in at least two of the following areas of expertise, with a minimum of one year in each discipline: ▪ Network security ▪ Application security ▪ System security ▪ IT security auditing ▪ IT security risk assessment *Note: This section is intended to draw out specific experience from the Candidate. The Candidate must provide examples (including the timeframe) of how their work experience meets the ASV Program requirements. This section is intended to measure the Candidate's skills against the required skills.*

ASV Administrative Requirements

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

Appendix C. 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.

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.