Payment Card Industry (PCI)
Data Security Standard
Qualification Requirements

For Qualified Security Assessors (QSA)

Version 2.1

February 2016

Document Changes

Date	Version	Description
October 2008	1.2	To align version number with PCI DSS v1.2; no other changes made.
May 2015	2.0	▪ Made various grammar improvements; aligned terminology with PCI DSS v3.1 ▪ Increased Violation period to three (3) years ▪ Clarified QSA Company and Employee qualification requirements ▪ Enhanced Business Legitimacy requirements ▪ Enhanced separation of duties, independence, and conflict of interest requirements ▪ Clarified regional requirements ▪ Clarified subcontracting vs. partnership with active QSA Company ▪ Enhanced QSA Employee skills and experience requirements ▪ Added PCI SSC Code of Professional Responsibility ▪ Enhanced background check requirements ▪ Enhanced QSA Company internal quality assurance requirements ▪ Enhanced Evidence (Assessment workpaper) retention requirements ▪ Added Security Incident Response ▪ Enhanced annual requalification requirements ▪ Enhanced Assessor Quality Management process: QSA Audit, Quality Remediation and Revocation process ▪ Updated the QSA Agreement (Appendix A) ▪ Updated insurance requirements (Appendix B) ▪ Added QSA Company application (Appendix C) ▪ Added QSA Employee application (Appendix D)
February 2016	2.1	Updated Section 3.2.1 to clarify professional certification requirements.

Table of Contents

1 Introduction

In response to requests from members of the payment card industry ("PCI") for a unified set of payment account data security requirements, PCI Security Standards Council, LLC ("PCI SSC") adopted and maintains the PCI Data Security Standard or "PCI DSS," a set of requirements for cardholder data protection across the industry.

When implemented properly, PCI DSS requirements provide a well-aimed defense for merchants and service providers against data exposure and compromise. As a result, assessment of merchants and service providers for compliance with PCI DSS requirements has become increasingly critical in today's environment and is key to the success of the PCI DSS.

Independent security organizations qualified by PCI SSC to validate an entity's adherence to PCI DSS requirements are referred to as "Qualified Security Assessor Companies" or "QSA Companies." Validation of PCI DSS requirements by QSA Companies is important to the effectiveness of the PCI DSS; and the quality, reliability, and consistency of a QSA Company's work provides confidence that cardholder data is adequately protected. The proficiency with which a QSA Company conducts a PCI DSS Assessment can therefore have a tremendous impact on data protection and the consistent and proper application of PCI DSS measures and controls.

This document—the QSA Qualification Requirements—describes the necessary qualifications for security companies and their employees to be qualified by PCI SSC to perform PCI DSS Assessments.

In addition to the qualifications offered under the PCI SSC Qualified Security Assessor Program described in this document and related PCI SSC publications (the "QSA Program"), PCI SSC offers the following related assessor qualifications under its corresponding PCI SSC programs (each a "PCI SSC Program"): Payment Application – Qualified Security Assessor (PA-QSA), PCI Forensics Investigator (PFI), Qualified Security Assessor for Point-to-Point Encryption (QSA (P2PE)), and Payment Application – Qualified Security Assessor for Point-to-Point Encryption (PA-QSA (P2PE)). Qualification under each of these Programs requires QSA Company qualification and satisfaction of applicable PCI SSC Program-specific requirements.

1.1 Terminology

Capitalized terms used but not otherwise defined in this document have the meanings set forth in this Section 1.1, or in the QSA Agreement, as applicable.

Term	Definition
PCI DSS	The then-current version of 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 DSS Assessment	The onsite review of an entity by a QSA Company to determine the entity's compliance with the PCI DSS for QSA Program purposes.
PCI SSC Assessment	With respect to a given QSA Company, any assessment performed for purposes of validating the compliance of any third party (or any third-party product, application, service or solution) with any PCI SSC standard for purposes of any PCI SSC Program.

Term	Definition
PCI SSC Standard	With respect to a given PCI SSC Program, the then-current version of (or successor document to) the corresponding security standards, requirements, and assessment procedures published by PCI SSC from time to time in connection with such PCI SSC Program and made available on the Website, including but not limited to any and all appendices, exhibits, schedules and attachments to any of the foregoing and all materials incorporated therein, in each case, as from time to time amended.
QSA Agreement	The then-current version of (or successor document to) the *PCI QSA Agreement*, the current version of which is attached as Appendix A to the QSA Qualification Requirements.
QSA Employee	An individual who is employed by a QSA Company and has satisfied and continues to satisfy all QSA Requirements applicable to employees of QSA Companies.
QSA List	The then-current list of QSA Companies published by PCI SSC on the Website.
QSA Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Qualified Security Assessors (QSA)*, as from time to time amended and made available on the Website.
QSA Requirements	With respect to a given QSA Company or QSA Employee, the requirements and obligations thereof pursuant to the QSA Qualification Requirements, the QSA Agreement, each addendum, supplement, or other agreement or attestation entered into between such QSA Company or QSA Employee and PCI SSC, and any and all other policies, procedures, requirements, validation or qualification 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 QSA Company or QSA Employee (as applicable) is then a participant, including but not limited, to all policies, procedures, requirements, standards, obligations of all applicable PCI SSC training programs, quality assurance programs, remediation programs, program guides and other related PCI SSC Program materials, including without limitation those relating to probation, fines, penalties, oversight, remediation, suspension and/or revocation.
Template for Report on Compliance ("ROC Reporting Template")	The mandatory template for completing a Report on Compliance for submission to the Participating Payment Brands and/or acquirers.
Website	The then-current PCI SSC website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.

1.2 Goal

To qualify as a QSA Company or QSA Employee, the candidate(s) must meet or exceed all applicable QSA Requirements, and the QSA Company candidate must execute the QSA Agreement with PCI SSC. Companies that qualify are identified on the QSA List in accordance with the QSA Agreement.

The requirements provided in this document serve as a **qualification baseline** and provide a transparent process for QSA Company and QSA Employee qualification and re-qualification. QSA Companies and QSA Employees must adhere to all applicable requirements provided in this document and must provide all required provisions described in this document.

1.3 Qualification Process Overview

The qualification process consists of two parts: (1) qualification of the security company itself, and (2) qualification of the company's employee(s) who will be performing and/or managing on-site PCI DSS Assessments.

To initiate the qualification process, the security company must sign the QSA Agreement in unmodified form and submit it to PCI SSC along with the company's executed QSA Company Application (See Appendix C). Additionally, a QSA Employee Application (See Appendix D) must be completed by each company employee seeking qualification and submitted to PCI SSC.

1.4 Document Structure

This document is structured as follows.

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

Section 2: QSA 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: QSA Capability Requirements reviews the information and documentation necessary to demonstrate the security company's service expertise, as well as that of its employees.

Section 4: QSA Company Administrative Requirements describes standards for operating as a QSA Company, including background checks, adherence to PCI SSC procedures, quality assurance, and protection of confidential and sensitive information.

Section 5: QSA Ongoing Qualification outlines the annual re-qualification process.

Section 6. Assessor Quality Management describes PCI SSC's assessor quality management process, including remediation and revocation.

Appendices: The appendices to the QSA Qualification Requirements include the QSA Agreement (Appendix A), insurance requirements (Appendix B), and QSA Company (Appendix C) and QSA Employee (Appendix D) application forms.

1.5 Related Publications

This document should be reviewed in conjunction with other relevant PCI SSC publications, including but not limited to the current publically available versions of the following, each available on the Website:

- *PCI DSS*
- *ROC Reporting Template*
- *PCI SSC Code of Professional Responsibility*

1.6 QSA Company Application Process

This document describes the information that must be provided to PCI SSC as part of the application and qualification process, as well as ongoing requirements for QSA Companies and QSA Employees. Each outlined requirement is followed by the information ("Provision") that must be submitted to document how the security company and employees meet or exceed the stated requirements.

To facilitate preparation of the application package, refer to Appendix C: "QSA Company Application" and Appendix D, "QSA Employee Application." All application materials and the signed QSA Agreement must be submitted in English. The QSA Agreement is binding in English even if the QSA Agreement was translated and reviewed in another language. All other documentation provided by the QSA Company (or candidate) in a language other than English must be accompanied by a certified English translation (examples include business licenses and insurance certificates).

Note: *QSA Companies are authorized to perform PCI DSS Assessments and QSA-related duties only in the geographic region(s) or country(s) in which they have been qualified to perform services. Under no circumstances may QSAs perform PCI DSS Assessments—or act as a QSA in any capacity—outside of the qualified region(s). If QSA-related tasks must be performed outside of the qualified region it may be necessary to engage a QSA within that region to perform the related tasks.*

Applications must indicate all geographic region(s) for which the QSA Company candidate is applying. See the Website – *PCI SSC Programs Fee Schedule*. All application packages must include a signed QSA Agreement and all required documentation. Applicants must send their completed application packages by mail to the following address (e-mail submissions will not be accepted):

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

Note*: PCI SSC reserves the right to reject any application from any applicant (company or employee) that PCI SSC determines has committed, within three (3) years prior to the application date, any conduct that may be considered a "Violation" (defined for purposes of Section 6.3 below or the QSA Agreement) if committed by a QSA Company or QSA Employee. The period of ineligibility will be a minimum of one (1) year, as determined by PCI SSC in a reasonable and non-discriminatory manner.*

1.7 Additional Information Requests

In an effort to maintain the integrity of the QSA Program, PCI SSC may request from time to time that QSA Companies and/or QSA Employees submit additional information or materials in order to demonstrate adherence to applicable requirements, as part of the applicable qualification or re-qualification process, or as part of the QSA Program approval or quality assurance process, including but not limited to in connection with remediation, revocation, or appeals. All such information and materials must be submitted in accordance with the corresponding PCI SSC request, in English or with a certified English translation, within three (3) weeks of the corresponding PCI SSC request or as otherwise requested by PCI SSC.

2 QSA Company Business Requirements

This section describes the minimum business requirements for QSA Companies, and related information that must be provided to PCI SSC by each QSA Company and candidate QSA Company regarding its business legitimacy, independence, and required insurance coverage.

2.1 Business Legitimacy

2.1.1 Requirement

The QSA Company must be recognized as a legal entity.

2.1.2 Provisions

The following information must be provided to PCI SSC:

- Copy of current QSA Company (or candidate QSA Company) formation document or equivalent approved by PCI SSC (the "Business License"), including year of incorporation, and location(s) of offices (Refer to the Documents Library on the Website – *Business License Requirements* for more information)
- Written statements describing all past or present allegations or convictions of any fraudulent or criminal activity involving the QSA Company, QSA Company candidate or any principal thereof, QSA Employee, and the status and resolution
- Written statements describing any past or present appeals or revocations of any qualification issued by PCI SSC to the QSA Company (or any predecessor entity or, unless prohibited by applicable law, any QSA Employee of any of the foregoing), and the current status and any resolution thereof

2.2 Independence

2.2.1 Requirement

The QSA 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 SSC Assessments.

The QSA Company must have a code-of-conduct policy, and provide the policy to PCI SSC upon request. The QSA Company's code-of-conduct policy must support—and never contradict—the *PCI SSC Code of Professional Responsibility.*

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

- The QSA Company will not undertake to perform any PCI SSC Assessment of any entity that it controls, is controlled by, is under common control with, or in which it holds any investment.

Note: *QSA Employees are permitted to be employed by only one QSA Company at any given time.*

- The QSA Company must not (and will not) have offered, been offered, been provided, or have accepted any gift, gratuity, service, or other inducement to any employee of PCI SSC

or to any customer, in order to enter into the QSA Agreement or any agreement with a customer, or to provide QSA Company-related services.

- The QSA Company must fully disclose in the Report on Compliance if it assesses any customer that uses any security-related device or security-related application developed or manufactured by the QSA Company, or to which the QSA Company owns the rights, or that the QSA Company has configured or manages, including but not limited to the following:
  - Application or network firewalls
  - Intrusion detection/prevention systems
  - Database or other storage solutions
  - Encryption solutions
  - Security audit log solutions
  - File integrity monitoring solutions
  - Anti-virus solutions
  - Vulnerability scanning services or solutions
- When recommending remediation actions that include one of its own solutions or products, the QSA Company must also recommend other market options that exist.
- The QSA Company must have separation of duties controls in place to ensure QSA Employees conducting PCI SSC Assessments are independent and not subject to any conflict of interest.
- The QSA Company will not use its status as a "listed QSA" to market services unnecessary to bring QSA Company clients into compliance with the PCI DSS or any other PCI SSC Standard.
- The QSA Company must not misrepresent any requirement of the PCI DSS or any other PCI SSC Standard in connection with its promotion or sales of services to its clients, or state or imply that the PCI DSS or any other PCI SSC Standard requires usage of the QSA Company's products or services.
- The QSA Company must notify its QSA Employees of the independence requirements provided for in this document, as well as QSA Company's independence policy, at least annually.

2.2.2 Provisions

The QSA Company (or candidate QSA Company) must describe its practices to maintain and assure QSA Employee and QSA Company independence with respect to all PCI SSC Assessments, including but not limited to practices, organizational structure, separation of duties, and employee education in place to prevent conflicts of interest. The description must address each requirement listed in Section 2.2.1.

2.3 Insurance Coverage

2.3.1 Requirement

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

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

2.3.2 Provisions

The QSA Company (or candidate QSA Company) must provide a proof-of-coverage statement to PCI SSC to demonstrate that insurance coverage matches PCI SSC requirements and locally set insurance coverage requirements. If the QSA Company subcontracts or assigns any portion of the QSA Company services (requires prior written consent from PCI SSC—see Section 3.2.1), the QSA Company must also provide to PCI SSC proof-of-coverage statements covering all subcontractors, demonstrating that insurance matching applicable insurance coverage requirements (see Appendix B) for all such subcontractors is purchased and maintained.

2.4 QSA Company Fees

2.4.1 Requirement

Each QSA Company applicant must pay an application processing fee, and a regional qualification fee for each geographic region or country in which the QSA Company applicant intends to perform PCI DSS Assessments. The application processing fee is credited toward the regional qualification fee(s). All fees are invoiced by PCI SSC and must be paid to PCI SSC according to the instructions accompanying the invoice.

QSA Company fees Include:

- Regional qualification fees (vary by country or region)
- Annual regional re-qualification fees for subsequent years (also vary by country or region)
- Annual QSA Employee training fee for each QSA Employee (or candidate)

Note: *All QSA Company fees are specified on the Website in the PCI SSC Programs Fee Schedule and are subject to change.*

2.5 QSA Agreement

2.5.1 Requirement

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

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

3 QSA Capability Requirements

This section describes the minimum capability requirements for QSA Companies and QSA Employees, as well as the related documentation that all QSA Companies and QSA Employees must provide to PCI SSC in order to demonstrate requisite technical security audit expertise, work history, and industry experience.

3.1 QSA Company – Services and Experience

3.1.1 Requirement

The QSA Company must possess technical security assessment experience similar or related to the PCI DSS Assessment.

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

3.1.2 Provisions

The following information must be provided to PCI SSC:

- Description of the applicant QSA Company's experience and knowledge with information security audit engagements, preferably related to payment systems, equal to at least one year or three separate audits
- Description of the applicant QSA Company's relevant areas of specialization within information security (for example, network security, database and application security, and incident response), demonstrating at least one area of specialization
- Evidence of a dedicated security practice, such as:
    - The total number of employees on staff and the number of those performing security assessments
- Brief description of other core business offerings
- Description of size and types of market segments in which the applicant QSA Company tends to focus, such as Fortune 500, financial industry, insurance industry, or small-to-medium sized businesses
- List of languages supported by the applicant QSA Company
- Two client references from security engagements performed by the applicant QSA Company within the last 12 months

3.2 QSA Employee – Skills and Experience

Each QSA Company employee performing or managing PCI DSS Assessments must be qualified by PCI SSC as a QSA Employee; only QSA Employees qualified by PCI SSC can conduct PCI DSS Assessments. QSA Employees are responsible for the following:

- Performing the PCI DSS Assessment
- Being on-site for the duration of the PCI DSS Assessment
- Reviewing the work product that supports the PCI DSS Assessment procedures
- Ensuring adherence to the then-current PCI DSS
- Validating the scope of the PCI DSS Assessment
- Selecting systems and system components where sampling is employed
- Evaluating compensating controls
- Producing the final Report on Compliance (ROC)

3.2.1 Requirement

Each QSA Employee performing or managing PCI SSC Assessments must satisfy the following requirements:

- Pass background checks required per Section 4.2.
- Possess sufficient information security knowledge and experience to conduct technically complex security assessments.
- Possess a minimum of one year of experience in each of the following information security disciplines (experience may be acquired concurrently—for example, if the role involved experience in multiple disciplines at the same time):
  - Application security
  - Information systems security
  - Network security
- Possess a minimum of one year of experience in each of the following audit/ assessment disciplines (experience may be acquired concurrently, for example, if the role involved experience in multiple disciplines at the same time):
  - IT security auditing
  - Information security risk assessment or risk management

- Possess at least one of the following accredited, industry-recognized professional certifications (possessing one certification from each list is recommended, but not currently required):

  List A – Information Security

  - (ISC)[2] Certified Information System Security Professional (CISSP)
  - ISACA Certified Information Security Manager (CISM)
  - Certified ISO 27001 Lead Implementer [1]

  List B – Audit

  - ISACA Certified Information Systems Auditor (CISA)
  - GIAC Systems and Network Auditor (GSNA)
  - Certified ISO 27001, Lead Auditor, Internal Auditor [1]
  - IRCA ISMS Auditor or higher (e.g., Auditor/Lead Auditor, Principal Auditor)

    Note: *"Provisional" auditor designations do not meet the requirement.*

  - IIA Certified Internal Auditor (CIA)

  Note: *The requirement to possess at least one industry-recognized certification is effective as of January 1, 2016 for new QSA Employees.*

  For QSA Employees qualified and added to the search tool prior to January 1, 2016, this requirement is effective July 1, 2016 (for example, upon annual requalification after June 30, 2016).

- Possess knowledge about the PCI DSS and all applicable documents on the PCI SSC Website.
- Attend annual QSA Employee training provided by PCI SSC, and legitimately pass, of his or her own accord without any unauthorized assistance, all examinations conducted as part of training. If a QSA Employee fails to pass any exam in connection with such training, the QSA Employee must no longer lead or manage any PCI SSC Assessment until successfully passing the exam.
- Adhere to the PCI SSC Code of Professional Responsibility.
- Be an employee of the QSA Company (meaning this work cannot be subcontracted to non-employees) unless PCI SSC has given prior written consent for each subcontracted worker.

---

[1] ISO27001 certifications will be accepted as meeting the requirement *only* when certifications are issued by an *accredited* certification body (for example, ANSI-ASQ National Accreditation Board (ANAB) and United Kingdom Accreditation Service (UKAS)). Certified ISO 27001 courses should be accredited to the ISO/IEC 17024 standard. It is the responsibility of the QSA/candidate to ensure that the certifying body is accredited, and to provide evidence of accreditation to PCI SSC.

To find out if your country has an accreditation body, visit the International Accreditation Forum (IAF) website at www.iaf.nu and use the *IAF MLA signatories* list to identify an accreditation body in your country or region.

To find a certification body visit the International Organization for Standardization certification information page; the section titled *Choosing a certification body* will explain how to find a certification body.

Verification of company's certification should be addressed to the certification organization in question. You may also wish to contact the ISO member in your country or the country concerned, as they may have a national database of certified companies.

Note: *Approved subcontractors shall not be permitted to include a company logo other than that of the responsible QSA Company or any reference to another company in the Report on Compliance or attestation documents while performing work on behalf of the QSA Company.*

If a QSA Company wishes to hire another company that is not an active QSA Company to perform any portion of the QSA Company services, such hiring is considered to be subcontracting and requires prior written consent by PCI SSC for each subcontracted worker. The QSA Company must also provide to PCI SSC proof-of-coverage statements covering all such subcontractors to demonstrate that insurance satisfying applicable insurance coverage requirements (see Appendix B) has been purchased and is maintained for all such subcontractors.

3.2.2 Provisions

This section is intended to draw out specific experience regarding candidate QSA Employees. Examples (including timeframes) of how each QSA Employee candidate's work experience meets the QSA Qualification Requirements must be provided for each QSA Employee candidate.

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

- A record of working experience and responsibilities outlined in Section 3.2.1 above, by completing and submitting Appendix D for each candidate QSA Employee, and;
- Résumé or Curriculum Vitae (CV) of each candidate QSA Employee.

3.3 Code of Professional Responsibility

3.3.1 Requirement

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

4 QSA Administrative Requirements

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

4.1 Contact Person

4.1.1 Requirement

The QSA 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 (see Appendix C):

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

4.2 Background Checks

4.2.1 Requirement

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

Minor offenses–for example, misdemeanors or non-US equivalents–are allowed; but major offenses–for example, felonies or non-US equivalents–automatically disqualify a candidate from qualifying as a QSA Employee. Upon request, each QSA Company must provide to PCI SSC the background check history for each QSA Employee (or candidate QSA Employee), to the extent legally permitted within the applicable jurisdiction.

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

4.2.2 Provisions

The QSA Company (or candidate QSA Company) must provide PCI SSC with responses to each of the following (see *Appendix C*):

- Attestation that its policies and hiring procedures include performing background checks: Examples of background checks include previous employment history, criminal record, credit history, and reference checks.
- A written statement that it successfully completed such background checks for each candidate QSA Employee.

- A summary description of current QSA personnel background check policies and procedures, which must require and include the following:
  - Verification of aliases (when applicable)
  - Comprehensive country and (if applicable) state level review of records of any criminal activity such as felony (or non-US equivalent) convictions or outstanding warrants, within the past five years minimum
  - Annual background checks consistent with this section for each of its QSA Employees for any change in criminal records, arrests or convictions

4.3 Internal Quality Assurance

For each PCI DSS Assessment, the resulting *Report on Compliance* (ROC) must follow the most current *ROC Reporting Template* available on the Website. The ROC must be accompanied by an Attestation of Compliance (AOC) in the form then available in the Documents Library on the Website, signed by a duly authorized officer of the QSA Company, which summarizes whether the entity that was assessed is in compliance or not in compliance with the PCI DSS, and any related findings.

4.3.1 Requirement

- The QSA Company must adhere to all QSA Program quality assurance requirements described in this document or otherwise established by PCI SSC from time to time.
- The QSA Company must have a quality assurance (QA) program, documented in its Quality Assurance manual.
- The QSA Company must maintain and adhere to a documented quality assurance process and manual, which includes all of the following:
  - Company name
  - List of PCI SSC Programs in which the QSA Company participates
  - A resource planning policy and process for PCI DSS Assessments which includes: onboarding requirements for QSA Employees, résumés and current skill sets for QSA Employees, and a process for ongoing training, monitoring, and evaluation of QSA Employees to ensure their skill sets stay current and relevant for PCI DSS Assessments
  - Descriptions of all job functions and responsibilities within the QSA Company relating to its status and obligations as a QSA Company
  - Identification of QA manual process owner
  - Approval and sign-off processes for ROCs and PCI DSS Assessments
  - Requirements for independent quality review of QSA Company and QSA Employee work product
  - Requirements for handling and retention of workpapers and other PCI DSS Assessment Results and Related Materials (defined in the QSA Agreement; see also

Section 4.5 for specific requirements for Workpaper Retention Policy requirements and specifications)

- QA process flow
- Distribution and availability of the QA manual
- Evidence of annual review by the QA manual process owner
- Coverage of all activities relevant to the particular PCI SSC Program, and references to the corresponding PCI SSC Qualification Requirements for that program, and to other applicable PCI SSC Program documentation for information concerning other PCI SSC Program-specific requirements
- Requirement for all QSA Employees to regularly monitor the Website for updates, guidance and new publications relating to the QSA Program

- The QSA Company must have qualified personnel (independent of the assessing and/or authoring QSA Employee) conduct a quality assurance review of assessment procedures performed, supporting documentation workpapers retained in accordance with QSA Company's Workpaper Retention Policy, information documented in the ROC related to the appropriate selection of system components, sampling procedures, compensating controls, remediation recommendations, proper use of payment definitions, consistent findings, and thorough documentation of results.
- The QSA Company must inform each client of the QSA Feedback Form (available on the Website) upon commencement of each PCI DSS Assessment.
- PCI SSC, at its sole discretion, reserves the right to conduct audits of the QSA Company at any time and further reserves the right to conduct site visits at the expense of the QSA Company.
- Upon request, the QSA Company (or applicant) must provide a complete copy of the quality assurance manual to PCI SSC.
- The PCI DSS Assessment must be conducted on-site at the client's facilities.

4.3.2 Provisions

The applicant QSA Company must provide a completed version of Appendix C to PCI SSC.

4.4 Protection of Confidential and Sensitive Information

4.4.1 Requirement

The QSA Company must have and adhere to a documented process for protection of confidential and sensitive information. This must include adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect confidential and sensitive information against any threats or unauthorized access during storage, processing, and/or communicating of this information.

The QSA Company must maintain the privacy and confidentiality of information obtained in the course of performing its duties and obligations as a QSA Company, unless (and to the extent) disclosure is required by legal authority.

4.4.2 Provisions

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

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

4.5 Evidence (Assessment Workpaper) Retention

4.5.1 Requirement

- Assessment Results and Related Materials (defined in the QSA Agreement), including but not limited to PCI DSS Assessment workpapers and related materials, represent the evidence generated and/or gathered by a QSA Company to support the contents of each ROC. Retention of Assessment Results and Related Materials is required and the Assessment Results and Related Materials relating to a given PCI DSS Assessment should represent all steps of the PCI DSS Assessment from end-to-end. Such Assessment Results and Related Materials may include screen captures, config files, interview notes, and a variety of other materials and information (and typically will include all of the foregoing). The QSA Company must maintain and adhere to a documented retention policy regarding all Assessment Results and Related Materials (a "Workpaper Retention Policy"), which includes, minimally, the following: Formal assignment of an employee responsible for ensuring the continued accuracy of the Workpaper Retention Policy and that each QSA Employee (a) complies with the Workpaper Retention Policy and (b) signs an appropriate confidentiality agreement with the QSA Company (as contemplated by Section 4.4 above).

- A blank copy of the QSA Company's Workpaper Retention Policy agreement that each QSA Employee is required to sign, included as part of the policy, which includes agreement to conform at all times with the Workpaper Retention Policy and the QSA Qualification Requirements.
- A requirement that all Assessment Results and Related Materials must be classified as confidential and handled accordingly, with detailed instructions describing how QSA Employees are to comply with this requirement. If the classification and handling of confidential information is addressed in other confidential and sensitive data protection handling policies of the QSA Company, this should be clearly noted within the Workpaper Retention Policy.
- A requirement that Assessment Results and Related Materials must be retained for at least three (3) years and must include all digital and hard copy evidence created and/or obtained by or on behalf of the QSA Company during each PCI DSS Assessment—including but not limited to: documentation reviewed (policies, processes, procedures, network and dataflow diagrams), case logs, meeting agendas and notes, evidence of onsite and offsite activities (including interview notes), screenshots, config files, results of any tests performed, and any other relevant information created and/or obtained.
- Requirements ensuring that the QSA Company has confirmed that all Assessment Results and Related Materials relating to a given PCI DSS Assessment has in fact been retained in accordance with the procedures defined in the Workpaper Retention Policy, prior to releasing the final ROC for that PCI DSS Assessment.
- All Assessment Results and Related Materials must be made available to PCI SSC and/or its Affiliates upon request for a minimum of three (3) years after completion of the applicable PCI DSS Assessment.
- The QSA Company must provide a copy of the Workpaper Retention Policy and related procedures to PCI SSC upon request, including copies of any other policies and procedures referenced within any of the foregoing documents, such as general confidential and sensitive data protection handling policies for the QSA Company.

4.5.2 Provisions

The applicant QSA Company must provide a completed version of Appendix C to PCI SSC.

4.6 Security Incident Response

This section describes obligations for QSA Companies where breach of cardholder data in a customer's environment has or is suspected to have occurred.

4.6.1 Requirement

The QSA Company must have and adhere to a documented process for notifying the applicable customer when the QSA Company or any employee, contractor or other personnel thereof, during or in connection with the performance of any PCI SSC Assessment or other QSA Program-related services, becomes aware of an actual or suspected breach of cardholder data within that customer's environment (each an "Incident"). Such process must require, and provide instruction for, notifying the customer in writing of the Incident and related findings, and informing the

customer of its obligations to notify the Participating Payment Brands in accordance with each Participating Payment Brands' notification requirements.

The customer notification must be documented and retained in accordance with the QSA Company's evidence-retention policy, along with a summary of the Incident and what actions were taken in connection with the Incident and corresponding discovery and/or notification. QSA Companies and QSA Employees are required to be familiar with the obligations for reporting Incidents to each of the Participating Payment Brands.

No QSA Company or QSA Employee shall take any action after an Incident that is reasonably likely to diminish the integrity of, or otherwise interfere with or negatively affect the ability of a PFI to perform, any PFI Investigation (see the *PCI Forensic Investigator (PFI) Program Guide* for additional details).

Failure to provide such written notification to the customer or otherwise comply with any of the above (or any other) QSA Qualification Requirements constitutes a "Violation" (see Section 6.3 below) and may result in remediation, revocation, and/or termination of the QSA Agreement.

4.6.2 Provisions

The applicant QSA Company must attest (see Appendix C) that it has an internal Incident-response plan, including but not limited to:

- Instructions and procedures for notifying customers of Incidents discovered during or in connection with the performance of any PCI SSC Assessment or other QSA Program-related services, and documenting those Incidents and related information in accordance with Section 4.6.1.
- Retention requirement for all Incident-related documentation, notices and reports, with the same protections as those noted for work-paper retention in the QSA Company's evidence-retention policy and procedures.

5 QSA List and Annual Re-Qualification

This section describes what happens after initial qualification, and activities related to annual re-qualification.

5.1 QSA List

Once a company has met applicable QSA Qualification Requirements, PCI SSC will add the QSA Company to the QSA List on the Website.

Once an individual has met applicable QSA Requirements, PCI SSC will add the QSA Employee to the applicable QSA Employee search tool on the Website.

Only those QSA Companies and QSA Employees on the QSA List or in such search tool (as applicable) are recognized by PCI SSC to perform PCI DSS Assessments.

If, at any time, a QSA Company and/or QSA Employee does not meet the applicable QSA Requirements (including without limitation, payment or documentation requirements), PCI SSC reserves the right to immediately remove the QSA Company/Employee from the respective list(s) or tool(s) on the Website, regardless of Remediation or Revocation. PCI SSC will notify the QSA Company of the removal in accordance with the QSA Agreement, typically via registered or overnight mail and/or e-mail. Refer to Sections 6.2 and 6.3 below for additional information relating to Remediation and Revocation.

5.2 Annual Re-Qualification

5.2.1 Requirements

All QSA Companies must be re-qualified, regionally, by PCI SSC on an annual basis. The annual re-qualification date is based upon the QSA Company's *original qualification date* (on a per-region basis). Re-qualification requires payment of annual training and re-qualification fees, and continued compliance with applicable QSA Requirements.

Additionally, each QSA Employee must be re-qualified by PCI SSC on an annual basis. The annual re-qualification date is based upon the QSA Employee's *previous qualification date*. Re-qualification requires proof of CPEs as noted in Section 5.2.2, proof of training successfully completed, payment of annual training and re-qualification fees, and continued compliance with applicable QSA Requirements.

Negative feedback from QSA Company clients (merchants, service providers, etc.), PCI SSC, Participating Payment Brands, or others may impact QSA Company and/or QSA Employee eligibility for re-qualification.

5.2.2 Provisions

The following must be provided to PCI SSC during the annual re-qualification process:

QSA Companies

- Payment of annual fee for each region qualified

Note: *PCI SSC may from time to time request that QSA Companies and/or QSA 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.*

QSA Employees

- Proof of information systems audit training within the last 12 months in accordance with the current version of the PCI SSC CPE Maintenance Guide
- Maintaining professional certification(s) as required per Section 3.2 QSA Employee – Skills and Experience. PCI SSC reserves the right to request proof of current professional certifications at any time
- Payment of annual re-qualification fees in accordance with the Website – *PCI SSC Programs Fee Schedule*

6 Assessor Quality Management Program

The PCI SSC's Assessor Quality Management (AQM) team exists to monitor and review assessor work in order to provide reasonable assurance that assessors maintain a baseline standard of quality.

6.1 QSA Audit Process

The purpose of the ongoing QSA audit process is to confirm that each QSA Company is maintaining documented quality processes in accordance with this document and the QSA Company's internal quality assurance program, as well as to gain assurance that assessor work is at a level consistent with the baseline objectives of the PCI DSS and supporting PCI SSC documentation. PCI SSC reserves the right to audit a QSA Company at any time, and further reserves the right to conduct site visits, at the expense of the QSA Company.

Once selected for audit by AQM, the QSA Company will be notified, typically via PCI SSC's secure assessor web portal for the QSA Program (the "Portal"). The notification will specify the Assessment Results and Related Materials the QSA Company is expected to provide over the course of the audit, which may include but is not limited to internal QA manuals, documented processes such as the Workpaper Retention Policy, ROCs redacted in accordance with PCI SSC policy, and workpapers.

The AQM team will review the ROCs, supporting documentation and the QSA Company's internal QA manual to determine whether the organization's internal QA processes are sufficiently documented in line with the above requirements and that they are being followed.

6.2 QSA Quality Remediation Process

QSA Companies that do not meet all applicable quality assurance standards set by PCI SSC may be offered the option to participate in PCI SSC's QSA Company Quality Remediation program ("Remediation") with respect to any PCI SSC Program qualification. Without limiting the generality of the foregoing, PCI SSC may offer Remediation in connection with any quality assurance audit, any Violation (defined below) or any other PCI SSC Program-related quality concerns, including but not limited to unsatisfactory feedback from QSA Company customers or Participating Payment Brands. When a QSA Company qualifies for Remediation, the QSA Company will be notified in accordance with the QSA Agreement, typically via registered or overnight mail and/or e-mail. Once the QSA Company signs the agreement to participate ("Remediation Agreement") and pays the fee(s) required in the notification, the applicable listing on the QSA List will be annotated with "In Remediation" and the listing will display the QSA Company's details in red text. Refer to the Website – *PCI SSC Programs Fee Schedule* for details of all applicable fees.

At the time of notification that the QSA Company qualifies for Remediation, AQM will provide the QSA Company with information on the requirements and procedures of the Remediation process and what it entails. Once AQM has gained sufficient assurance of quality improvement and the requirements of the Remediation Agreement have been fulfilled, Remediation ends, and the QSA Company's listing on the Website returns to "In Good Standing" in black text. QSA Companies that fail to satisfy Remediation requirements may be revoked, and QSA Companies electing not to participate in Remediation when eligible will be revoked.

Note: *The* Remediation Statement *on the Website affirms the Council's position on Remediation, and any external queries about a QSA Company's status will be directed to the QSA Company in question.*

QSA Companies in remediation may continue to perform PCI SSC Assessments for which they are qualified by PCI SSC unless otherwise instructed by PCI SSC in connection with the Remediation process.

6.3 QSA Revocation Process

Each event below is an example of a "Violation" (defined in the QSA Agreement), and accordingly, regardless of prior warning or Remediation, may result in revocation of QSA Company and/or QSA Employee qualification (and/or other PCI SSC Program qualifications). This list is not exhaustive. Among other things, any qualification under any PCI SSC Program may be revoked if PCI SSC determines that either the QSA Company or any of its QSA Employees has breached any provision of the QSA Agreement or otherwise failed to satisfy any applicable QSA Requirement (each also a Violation), including but not limited to.

- Failure to meet applicable PCI SSC Program quality standards or comply with applicable QSA Requirements
- Failure to pay applicable PCI SSC Program fees
- Failure to meet applicable PCI SSC Program training requirements (annual or otherwise)
- Failure to meet applicable PCI SSC Program continuing education requirements
- Failure to provide quality services, based on customer feedback or evaluation by PCI SSC or its affiliates
- Failure to maintain applicable PCI SSC Program insurance requirements
- Failure to comply with or validate compliance in accordance with applicable Program Qualification Requirements (defined in the QSA Agreement), PCI SSC Standards or program guides, or the terms of the QSA Agreement or supplements or addenda thereto
- Failure to maintain physical, electronic, or procedural safeguards to protect confidential or sensitive information
- Failure to report unauthorized access to any system storing confidential or sensitive information
- Engaging in unprofessional or unethical business conduct, including without limitation, plagiarism or other improper use of third-party work product in ROCs or other PCI SSC Assessment reports
- Failure to comply with any provision or obligation regarding non-disclosure or use of confidential information or materials
- Cheating on any exam in connection with PCI SSC Program training; submitting exam work in connection with PCI SSC Program training that is not the work of the individual candidate taking the exam; theft of or unauthorized access to PCI SSC Program exam content; use of an alternate, stand-in or proxy during any PCI SSC Program exam; use of any prohibited or unauthorized materials, notes or computer programs during any such exam; or providing or communicating in any way any unauthorized information to another person, device or other resource during any PCI SSC Program exam
- Providing false or intentionally incomplete or misleading information to the Council in any application or other materials
- Failure to be in Good Standing (as defined in the QSA Agreement) as a QSA Company or to be in Good Standing (as defined in the applicable Program Qualification Requirements) with

respect to any other PCI SSC qualification then held by such QSA Company or QSA Employee (as applicable), in each case including but not limited to failure to successfully complete applicable quality assurance audits and/or comply with all applicable requirements, policies, and procedures of PCI SSC's quality assurance, remediation, and oversight programs and initiatives as established or imposed from time to time by PCI SSC in its sole discretion

- Failure to promptly notify PCI SSC of any event described above that occurred within three (3) years of the QSA Company's or QSA Employee's initial qualification date

Each Violation constitutes a breach of the QSA Agreement and the applicable addendum or supplement for each applicable PCI SSC Program, and a failure to comply with applicable QSA Requirements, and may result in revocation of QSA Company and/or QSA Employee qualification, revocation of any other PCI SSC Program qualification, and/or termination of the *QSA Agreement* and/or any such addendum or supplement.

If the decision is made to revoke any PCI SSC Program qualification (including but not limited to QSA Company and/or QSA Employee qualification), notification will be provided in accordance with the QSA Agreement and will include information regarding the appeal process.

Appeals must be submitted within 30 days from the date of the notification to the QSA Program Manager by postal mail to the following address (e-mail submissions will not be accepted):

PCI SSC
401 Edgewater Place, Suite 600
Wakefield, MA 01880, USA

In connection with revocation, the following will occur:

- The QSA Company and/or QSA Employee (as applicable) name will be removed from the relevant QSA List and/or search tool (as applicable).
- PCI SSC may notify third parties.
- A company and/or individual (as applicable) the Qualification of which has been revoked may reapply at any time; provided however, that (i) if revoked in connection with Remediation, an election not to participate in Remediation when offered, or due to failure to satisfy applicable quality assurance standards set by PCI SSC, such company and/or individual shall be ineligible to re-apply to the QSA Program for a period of two (2) years; and (ii) acceptance of qualification applications after revocation is determined at the Council's discretion in a reasonable and nondiscriminatory manner, in light of the relevant facts and circumstances, including but not limited to the nature and severity of the violation, occurrence of repeat violations, and the applicant's demonstrated ability to comply with remediation requirements (if applicable).

Note: *When reading Sections 5 or 6 of this document in connection with any PCI SSC Program (other than the QSA Program) for which qualification as a QSA Company or QSA Employee is required (e.g., the PA-DSS Program), unless otherwise expressly provided in the applicable documentation for such other program, references in Sections 5 and 6 to terms specific to the QSA Program (e.g., QSA Company, QSA Employee, QSA Requirement, and PCI DSS Assessment) should be read to include the corresponding terms of such other PCI SSC Program. For example, for purposes of the PA-DSS Program, the term QSA Employee as it appears in this Section 6 should be read to include the term PA-QSA Employee as well.*

Appendix A. Qualified Security Assessor (QSA) Agreement

A.1 Introduction

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

A.2 General Information

Applicant					
Company Name:					
Business Address:		City:			
State/Province:		Country:		Postal Code:	
Regions Applying For (see the Website - *PCI SSC Programs Fee Schedule*):					
Language(s) to be displayed on Listing:					
Primary Contact					
Name:		Job Title:			
Direct Telephone Number:		E-mail:			
Location:		Fax:			
Secondary Contact					
Name:		Job Title:			
Direct Telephone Number:		E-mail:			
Location:		Fax:			
Applicant QSA Company Officer					
Applicant Officer Name:		Job Title:			
Applicant's Officer Signature ↑		*Date* ↑			
PCI SSC					
Name:					
Job Title:					
PCI SSC Signature ↑		*Date* ↑			

A.3 Terms and Conditions

A.3.1 QSA Services

Subject to the terms and conditions of this Agreement, while QSA is in Good Standing (defined in Section A.5.1(a) below) as a QSA Company or in compliance with Remediation, PCI SSC hereby approves QSA to perform, in accordance with this Agreement and the QSA Qualification Requirements (defined below), onsite reviews of the member Financial Institutions of Participating Payment Brands ("Financial Institutions"), issuers of Participating Payment Brand payment cards ("Issuers"), merchants authorized to accept Participating Payment Brand cards in payment for goods or services ("Merchants"), acquirers of Merchant accounts ("Acquirers") and data processing entities performing services for a Financial Institution, Issuer, Merchant or Acquirer ("Processors", and each Processor, Acquirer, Issuer, Merchant or Financial Institution, a "QSA Company client"), to determine QSA Company clients' compliance with the PCI DSS as part of the QSA Program. For purposes of this Agreement: (i) the onsite reviews described above that are conducted by QSA are referred to herein as "PCI DSS Assessments"; (ii) the PCI DSS Assessments, collectively with all related services provided by QSA to PCI SSC, QSA Company clients or others in connection with this Agreement and the QSA Program or any other PCI SSC Program, are referred to herein as the "Services"; (iii) "QSA Qualification Requirements" means the most current version of (or successor document to) the *Payment Card Industry (PCI) Qualification Requirements for Qualified Security Assessors (QSA)* document as available through the Website, as may be amended from time to time in PCI SSC's discretion, including without limitation, any and all additional supplements or addenda thereto which are applicable to QSA as a result of its participation in the QSA Program and related qualified security assessor initiatives operated by PCI SSC (each of which initiatives is hereby deemed to be included within the meaning of the term "QSA Program" for purposes of this Agreement); (iv) "Member" means an entity that is then formally admitted as (or an affiliate of) a member of PCI SSC in accordance with its governing documents (status as a PCI SSC "Participating Organization" does not establish that an entity is a "Member"); (v) "Participating Payment Brand" means a payment card brand (or affiliate thereof) that is then a Member and owner of PCI SSC; and (vi) all capitalized terms used in this Agreement without definition shall have the meanings ascribed to them in the QSA Qualification Requirements. The QSA Qualification Requirements are hereby incorporated into this Agreement, and QSA acknowledges and agrees that it has reviewed the current version of the QSA Qualification Requirements available on the Website.

QSA acknowledges that data security practices exist within a rapidly changing environment and agrees to monitor the Website at least weekly for changes to the PCI DSS and/or the QSA Qualification Requirements. QSA will incorporate all such changes into all PCI DSS Assessments initiated on or after the effective date of such changes. QSA acknowledges and agrees that any ROC regarding a PCI DSS Assessment that is not conducted in accordance with the PCI DSS as in effect at the initiation date of such PCI DSS Assessment may be rejected.

A.3.2 Performance of Services

QSA warrants, represents and agrees that it will only perform PCI SSC Assessments for which is has been qualified by PCI SSC, and that it will perform each such PCI SSC Assessment in strict compliance with the applicable PCI SSC Standard(s) as in effect as of the commencement date of such PCI SSC Assessment. Without limiting the foregoing, QSA will include in each ROC an Attestation of Compliance in the form available through the Website signed by a duly authorized officer of QSA, in which QSA certifies without qualification that (a) in performing the applicable

PCI DSS Assessment, QSA followed the requirements and procedures of the PCI DSS without deviation and (b) application of such requirements and procedures did not indicate any conditions of non-compliance with the PCI DSS other than those expressly noted in the ROC.

A.3.3 QSA Service Staffing

QSA shall ensure that a QSA Employee that is fully qualified in accordance with all applicable provisions of the relevant *Program Qualification Requirements* (defined below) supervises all aspects of each engagement to perform Services, including without limitation, being present onsite for the duration of each PCI SSC Assessment, reviewing the work product that supports QSA's PCI SSC Assessment procedures, and ensuring adherence to the applicable *Program Qualification Requirements* and PCI SSC Standards. Employees performing the following tasks must also be qualified as QSA Employees: scoping decisions, selection of systems and system components where sampling is employed (in accordance with the PCI DSS), evaluation of compensating controls and/or final report production and/or review. QSA hereby designates the individual identified as the "Primary Contact" in Section A.2 above as QSA's primary point of contact and "Primary Contact" for purposes of the QSA Program and this Agreement. QSA may change its Primary Contact at any time upon written notice to PCI SSC, and hereby represents that each Primary Contact shall have authority to execute any and all decisions on QSA's behalf concerning QSA Program matters.

A.3.4 QSA Requirements

QSA agrees to comply with all QSA Requirements, including without limitation, QSA's responsibilities and obligations pursuant to this Agreement, all quality assurance and Remediation requirements, and all requirements applicable to QSA Companies pursuant to the QSA Qualification Requirements and the then-current versions of (or successor documents to) the qualification and/or validation requirements published by PCI SSC with respect to each PCI SSC Program that requires qualification as a QSA Company as a prerequisite and in which QSA is a participant (each a "Related PCI SSC Program"), as from time to time amended and made available on the Website (collectively, "*Program Qualification Requirements*"). Without limiting the foregoing, QSA agrees to comply with all requirements of, make all provisions provided for in, and ensure that its QSA Employees comply with all applicable *Program Qualification Requirements*, agrees to comply with all such requirements regarding background checks, and warrants that it has obtained all required consents to such background checks from each employee designated by QSA to PCI SSC to perform Services hereunder. QSA warrants that, to the best of QSA's ability to determine, all information provided to PCI SSC in connection with this Agreement and QSA's participation in any PCI SSC Program is and shall be accurate and complete as of the date such information is provided. In the event of any change as a result of which any such information is no longer accurate or complete (including but not limited to any change in QSA's circumstances or compliance with applicable QSA Requirements), QSA shall QSA shall promptly (and in any event within thirty (30) days after such change) notify PCI SSC of such change and provide such information as may be necessary to ensure that the information PCI SSC has received is then accurate and complete. QSA acknowledges that PCI SSC from time to time may require QSA to provide a representative and/or QSA Employees to attend any mandatory training programs in connection with each PCI SSC Program in which QSA is then a participant, which may require the payment of attendance and other fees by QSA.

A.4 Fees

QSA agrees to pay all applicable fees imposed by PCI SSC in connection with QSA's and its QSA Employees' participation in each PCI SSC Program in which QSA is a participant (collectively, "Fees"), in each case as and in the manner provided for in the applicable *Program Qualification Requirements*, the *PCI SSC Programs Fee Schedule* on the Website and/or the other applicable PCI SSC Program documentation. Such Fees may include, without limitation, initial processing fees, regional qualification fees, regional re-qualification fees, training fees, fees in connection with quality assurance and/or remediation, fees to cover administrative costs, re-listing, penalties and other costs, and other fees. QSA agrees to pay all such Fees as and when required by PCI SSC and that all Fees are nonrefundable (regardless of whether QSA's application is approved, QSA has been removed from the QSA List, this Agreement or any Addendum (defined in Section A.9.2 below) hereto has been terminated, or otherwise).

QSA acknowledges that PCI SSC may review and modify its Fees at any time and from time to time. Whenever a change in Fees occurs, PCI SSC shall notify QSA in accordance with the terms of Section A.10.1. Such change(s) will be effective immediately after the date of such notification. However, should QSA not agree with such change(s), QSA shall have the right to terminate this Agreement (or, if such change only applies to a Related PCI SSC Program, the corresponding Addendum (defined in Section A.9.2 below) for such Related PCI SSC Program) upon written notice to PCI SSC in accordance with the provisions of Section A.10.1 at any time within 30 days after such notification from PCI SSC. Except to the extent otherwise expressly provided in the QSA Qualification Requirements or other applicable PCI SSC Program documentation, all fees payable to PCI SSC in connection with any PCI SSC Program must be paid in US dollars (USD), by check, by credit card or by wire transfer to a PCI SSC bank account specified for such purpose by PCI SSC. QSA acknowledges and agrees that such Fees do not include any taxes, such as value added taxes (VAT), sales, excise, gross receipts and withholding taxes, universal service fund fee, or any similar tax or other government imposed fees or surcharges which may be applicable thereto. QSA 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, QSA will pay such additional amounts as may be necessary, such that PCI SSC receives the amount it would have received had no withholding been imposed.

A.5 Advertising and Promotion; Intellectual Property

A.5.1 QSA List and QSA Use of PCI Materials and Marks

(a) So long as QSA is qualified by PCI SSC as a QSA Company, PCI SSC may, at its sole discretion, display the identification of QSA, together with related information regarding QSA's status as a QSA Company, in such publicly available list of QSA Companies as PCI SSC may maintain and/or distribute from time to time, whether on the Website or otherwise (the "QSA List"), along with information identifying QSA and corresponding qualification status information (including without limitation, good standing, remediation and/or revocation status). QSA shall provide all requested information necessary to ensure to PCI SSC's satisfaction that the identification and information relating to QSA on the QSA List is accurate. Without limiting the rights of PCI SSC set forth in the first sentence of this Section or elsewhere, PCI SSC expressly reserves the right to remove QSA from the QSA List at any time during which QSA is not in Good Standing as a QSA Company. QSA shall be deemed to be in "Good Standing" as a QSA Company as long as this Agreement is in full force and effect, QSA has

been approved as a QSA Company and such approval has not been revoked and QSA is not in breach of any of the terms or conditions of this Agreement (including without limitation, any term or provision regarding compliance with the QSA Qualification Requirements or payment).

(b) In advertising or promoting its Services, so long as QSA is in Good Standing as a Qualified Security Assessor, QSA may make reference to the fact that QSA is listed in the QSA List, provided that it may do so only during such times as QSA actually appears in the QSA List.

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

A.5.2 Uses of QSA Name and Designated Marks

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

A.5.3 No Other Rights Granted

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

A.5.4 Intellectual Property Rights

(a) All Intellectual Property Rights, title and interest in and the PCI SSC Programs, the PCI DSS and all other PCI Materials, all materials QSA 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 A.6, so long as QSA is in Good Standing as a QSA Company or in compliance with Remediation, QSA 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 QSA's internal review purposes or as otherwise expressly permitted in this Agreement or pursuant to a separate written consent or agreement between PCI SSC and QSA in each instance. For purposes of this Agreement, "Intellectual Property Rights" shall mean all present and future patents, trademarks, service marks, design rights, database rights (whether registrable or unregistrable, and whether registered or not), applications for any of the foregoing, copyright, know-how, trade secrets, and all other industrial or intellectual property rights or obligations whether registrable or unregistrable and whether registered or not in any country.

(b) All right, title and interest in and to the Intellectual Property Rights in all materials generated by or on behalf of PCI SSC with respect to QSA are and at all times shall remain the property of PCI SSC. Subject to the provisions of Section A.6, QSA may use and disclose such materials solely for the purposes expressly permitted by this Agreement. QSA shall not revise, abridge, modify or alter any such materials.

(c) QSA 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 QSA Program or any of the PCI Materials.

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

A.6 Confidentiality

A.6.1 Definition of Confidential Information

As used in this Agreement, "Confidential Information" means (i) all terms of this Agreement; (ii) any and all information designated in this Agreement as Confidential Information; (iii) any and all originals or copies of, any information that either party has identified in writing as confidential at the time of disclosure; and (iv) any and all Personal Information, proprietary information, merchant information, technical information or data, assessment reports, trade secrets or know-how, information concerning either party's past, current, or planned products, services, fees, finances, member institutions, Acquirers, Issuers, concepts, methodologies, research, experiments, inventions, processes, formulas, designs, drawings, business activities, markets,

plans, customers, equipment, card plastics or plates, software, source code, hardware configurations or other information disclosed by either party or any Member, or their respective directors, officers, employees, agents, representatives, independent contractors or attorneys, in each case, in connection with any PCI SSC Program or activity in which QSA is a participant and in whatever form embodied (e.g., oral, written, electronic, on tape or disk, or by drawings or inspection of parts or equipment or otherwise), including without limitation, any and all other information that reasonably should be understood to be confidential. "Personal Information" means any and all Participating Payment Brand payment card account numbers, Participating Payment Brand transaction information, IP addresses or other PCI SSC, Member or third party information relating to a natural person, where the natural person could be identified from such information. Without limiting the foregoing, Personal Information further includes any information related to any Participating Payment Brand accountholder that is associated with or organized or retrievable by an identifier unique to that accountholder, including accountholder names, addresses, or account numbers.

A.6.2 General Restrictions

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

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

A.6.3 QSA Company Client Data

To the extent any data or other information obtained by QSA relating to any QSA Company client in the course of providing Services thereto may be subject to any confidentiality restrictions between QSA and such QSA Company client, QSA shall provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such QSA Company client in writing) that (i) QSA may disclose each ROC, Attestation of Compliance and other related or similar reports or information generated or gathered by QSA in connection with its performance of the Services to PCI SSC and/or Participating Payment Brands, as requested by the QSA Company client, (ii) to the extent any Participating Payment Brand obtains such reports

or information in accordance with the preceding clause A6.3(i), such Participating Payment Brand may disclose (a) such reports or information on an as needed basis to other Participating Payment Brands and to such Participating Payment Brands' respective Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies and (b) that such Participating Payment Brand has received a ROC, report and other related information with respect to such QSA Company client (identified by name) and whether the ROC or report was satisfactory, and (iii) QSA may disclose such information as necessary to comply with its obligations and requirements pursuant to Section A.10.2(b) below. Accordingly, notwithstanding anything to the contrary in Section A.6.2(a) above, to the extent requested by a QSA Company client, PCI SSC may disclose Confidential Information relating to such QSA Company client and obtained by PCI SSC in connection with this Agreement to Participating Payment Brands in accordance with this Section A.6.3, and such Participating Payment Brands may in turn disclose such information to their respective member Financial Institutions and other Participating Payment Brands. QSA hereby consents to such disclosure by PCI SSC and its Participating Payment Brands. As between any Member, on the one hand, and QSA or any QSA Company client, on the other hand, the confidentiality of ROCs and any other information provided to Members by QSA or any QSA Company client 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 QSA or such QSA Company client (as applicable), on the other hand.

A.6.4 Personal Information

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

A.6.5 Return

Within fourteen (14) days after notice of termination of this Agreement or demand by PCI SSC, QSA promptly shall return to PCI SSC all property and Confidential Information of PCI SSC and of all third parties to the extent provided or made available by PCI SSC; provided, however, that QSA 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 QSA's workpapers as a result of providing services to a QSA Company client; and QSA shall continue to maintain the confidentiality of all such retained Confidential Information in accordance with this Agreement. If agreed by PCI SSC, QSA may instead destroy all such materials and information and provide a certificate of destruction to PCI SSC, with sufficient detail regarding the items destroyed, destruction date, and assurance that all copies of such information and materials also were destroyed.

A.6.6 Remedies

In the event of a breach of Section A.6.2 by the Receiving Party, the Receiving Party acknowledges that the Disclosing Party will likely suffer irreparable damage that cannot be fully remedied by monetary damages. Therefore, in addition to any remedy that the Disclosing Party may possess pursuant to applicable law, the Disclosing Party retains the right to seek and obtain injunctive relief against any such breach in any court of competent jurisdiction. In the event any such breach results in a claim by any third party, the Receiving Party shall indemnify, defend and hold harmless the Disclosing Party from any claims, damages, interest, attorney's fees, penalties, costs and expenses arising out of such third-party claim(s).

A.7 Indemnification and Limitation of Liability

A.7.1 Indemnification

QSA shall defend, indemnify, and hold harmless PCI SSC and its Members, and their respective subsidiaries, and all affiliates, subsidiaries, directors, officers, employees, agents, representatives, independent contractors, attorneys, successors, and assigns of any of the foregoing (collectively, including without limitation, PCI SSC and its Members, "Indemnified Parties") from and against any and all claims, losses, liabilities, damages, suits, actions, government proceedings, taxes, penalties or interest, associated auditing and legal expenses and other costs (including without limitation, reasonable attorney's fees and related costs) that arise or result from any claim by any third party with respect to QSA's (i) breach of its agreements, representations or warranties contained in this Agreement; (ii) participation in any PCI SSC Program or use of any PCI Materials or PCI SSC Program-related information (a) in violation of this Agreement or (b) in violation of any applicable law, rule or regulation; (iii) non-performance of Services for any QSA Company client that has engaged QSA to perform Services, including without limitation claims asserted by QSA Company clients or Members; (iv) negligence or willful misconduct in connection with any PCI SSC Program, this Agreement or QSA's performance of Services, except to the extent arising out of negligence or willful misconduct of an Indemnified Party; or (v) breach, violation, infringement or misappropriation of any third-party Intellectual Property Right. All indemnities provided for under this Agreement shall be paid by QSA as incurred by the Indemnified Party. This indemnification shall be binding upon QSA and its executors, heirs, successors and assigns. Nothing in this Agreement shall be construed to impose any indemnification obligation on QSA to the extent the corresponding claim or liability arises solely from a defect in the PCI Materials provided by an Indemnified Party and such PCI

Materials are used by QSA without modification and in accordance with all then applicable publicly available updates, guidance, and best practices provided by PCI SSC.

A.7.2 Indemnification Procedure

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

A.7.3 No Warranties; Limitation of Liability

(a) PCI SSC PROVIDES THE *PCI DSS*, ALL OTHER PCI SSC STANDARDS, THE QSA PROGRAM, ALL OTHER PCI SSC PROGRAMS, THE QSA QUALIFICATION REQUIREMENTS, ALL OTHER PROGRAM QUALIFICATION REQUIREMENTS, THE WEBSITE AND ALL RELATED AND OTHER MATERIALS PROVIDED OR OTHERWISE MADE ACCESSIBLE BY PCI SSC IN CONNECTION WITH ANY PCI SSC PROGRAM (THE FOREGOING, COLLECTIVELY, THE "PCI MATERIALS") ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND. QSA ASSUMES THE ENTIRE RISK AS TO RESULTS AND PERFORMANCE ARISING OUT OF ITS USE OF ANY OF THE PCI MATERIALS.

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

(c) In particular, without limiting the foregoing, QSA acknowledges and agrees that the accuracy, completeness, sequence or timeliness of the PCI Materials or any portion thereof cannot be guaranteed. In addition, PCI SSC makes no representation or warranty whatsoever, expressed or implied, and assumes no liability, and shall not be liable in any respect to QSA regarding (i) any delay or loss of use of any of the PCI Materials, or (ii) system performance and effects on or damages to software or hardware in connection with any use of the PCI Materials.

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

(e) PCI SSC shall be liable vis-à-vis QSA only for any direct damage incurred by QSA 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 QSA to PCI SSC under Section A.4.

(f) Except as otherwise expressly provided in this Agreement, neither PCI SSC nor any Participating Payment Brand shall be liable vis-à-vis QSA for any other damage incurred by QSA under this Agreement or in connection with any PCI SSC Program, including but not limited to, loss of business, revenue, goodwill, anticipated savings or other commercial or economic loss of any kind arising in any way out of the use of any PCI SSC Program (regardless of whether such damages are reasonably foreseeable or PCI SSC has been advised of the possibility of such damages), or for any loss that results from force majeure.

A.7.4 Insurance

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

A.8 Independence; Representations and Warranties

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

A.9 Term and Termination

A.9.1 Term

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

A.9.2 Termination by QSA

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

A.9.3 Termination by PCI SSC

PCI SSC may terminate this Agreement and/or any Addendum effective as of the end of the then-current Term by providing QSA with written notice of its intent to terminate or not to renew this Agreement (or such Addendum, as applicable) at least sixty (60) days prior to the end of the then-current Term. Additionally, PCI SSC may terminate this Agreement and/or any Addendum: (i) with written notice upon QSA's voluntary or involuntary bankruptcy, receivership, reorganization dissolution or liquidation under state or federal law that is not otherwise dismissed within thirty (30) days; (ii) with written notice upon QSA's breach of any representation or warranty under this Agreement or such Addendum; (iii) with fifteen (15) days' prior written notice following QSA's breach of any other term or provision of this Agreement or the applicable Addendum (including without limitation, QSA's failure to comply with any of the QSA Requirements), provided such breach remains uncured when such 15-day period has elapsed; (iv) in accordance with Section A.9.5 below; (v) if PCI SSC ceases to operate the QSA Program, whether with or without

replacing it with any other program; or (vi) in accordance with the terms of the applicable Addendum.

A.9.4 Effect of Termination

Upon any termination or expiration of this Agreement: (i) QSA will be removed from the QSA List and each Addendum shall immediately and automatically terminate (subject to the survival of any terms or provisions thereof which expressly survive termination or expiration thereof); (ii) QSA shall immediately cease all advertising and promotion of its Qualifications, it status as a QSA Company, and its listing(s) on the QSA List, and ensure that it and its employees do not state or imply that any employee of QSA is a "QSA Employee," a "QSA" or otherwise qualified by PCI SSC under any Program for which QSA Company Qualification is required; (iii) QSA shall immediately cease soliciting for and performing all Services (including but not limited to processing of ROCs), provided that QSA shall complete any and all Services contracted with QSA Company clients prior to such expiration or the notice of termination if and to the extent instructed by PCI SSC in writing; (iv) to the extent QSA is instructed to complete any Services pursuant to preceding clause (iii), QSA will deliver all corresponding outstanding ROCs and other PCI SSC Assessment reports within the time contracted with the QSA Company client, (v) QSA shall remain responsible for all of the obligations, representations and warranties hereunder with respect to all ROCs and other PCI SSC Assessment reports submitted by QSA to PCI SSC or any other person or entity; (vi) QSA shall return or destroy all PCI SSC and third party property and Confidential Information in accordance with the terms of Section A.6; (vii) if requested by PCI SSC, QSA shall obtain (at QSA's sole cost and expense) the services of a replacement QSA Company acceptable to PCI SSC for purposes of completing those Services for which QSA was engaged prior to such expiration or the notice of termination but which QSA has not been instructed to complete pursuant to Section (iii) above; (viii) QSA shall, within fifteen (15) days of such expiration or the notice of termination, in a manner acceptable to PCI SSC, notify those of its QSA Company clients with which QSA is then engaged to perform any PCI SSC Assessment or other Services of such expiration or termination; (ix) if requested by PCI SSC, QSA shall within fifteen (15) days of such request, identify to PCI SSC in writing all QSA Company clients with which QSA was engaged to perform Services immediately prior to such expiration or notice of termination and the status of such Services for each; and (x) notwithstanding anything to the contrary in this Agreement, PCI SSC may notify any of its Members and any acquirers, QSA Company clients or others of such expiration or termination and the reason(s) therefor. The provisions of Sections A.5.4, A.6, A.7, A.9.4 and A.10 of this Agreement, and the terms of each Addendum which by their terms survive termination of such Addendum, shall survive the expiration or termination of this Agreement for any or no reason.

A.9.5 Revocation

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

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

(c) All Revocation appeal proceedings will be conducted in accordance with such procedures as PCI SSC may establish from time to time for the applicable PCI SSC Program, PCI SSC will review all relevant evidence submitted by QSA and each complainant (if any) in connection with therewith, and PCI SSC shall determine whether termination of any Qualification provided to QSA by PCI SSC (including without limitation, Qualification as a QSA Company) is warranted or, in the alternative, no action, or specified remedial actions shall be required. All determinations of PCI SSC regarding Revocation and any related termination or appeals shall be final and binding upon QSA. If PCI SSC determines that termination is warranted, then effective immediately and automatically upon such determination, such Qualification and this Agreement and/or the applicable Addendum shall terminate. If PCI SSC determines that such termination is not warranted, the Revocation shall be lifted, the applicable Qualification shall be reinstated, and the listing of QSA that was removed from the QSA List as a result of such Revocation shall be reinstated. If PCI SSC determines that remedial action is required, PCI SSC shall notify QSA and may establish a date by which such remedial action must be completed; provided, however, that unless otherwise agreed by PCI SSC in writing the Revocation shall not be lifted, and QSA shall not be reinstated on the QSA List, unless and until such time as QSA has completed such remedial action; and provided, further, that if QSA fails to complete any required remedial actions by the date (if any) established by PCI SSC for completion thereof, PCI SSC may terminate the applicable Qualification and this Agreement and/or the applicable Addendum, effective immediately as of or any time after such date.

A.10 General Terms

A.10.1 Notices

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

A.10.2 Audit and Financial Statements

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

(b) Notwithstanding anything to the contrary in Section A.6 of this Agreement, in order to assist in ensuring the reliability and accuracy of QSA's PCI SSC Assessments, QSA hereby agrees to comply with all quality assurance procedures and requirements established or imposed by PCI SSC from time to time in connection with each PCI SSC Program in which QSA is a participant (including but not limited to conditions and requirements imposed in connection with remediation, revocation or any other Qualification status) and that, within 15 days of any written request by PCI SSC, QSA hereby agrees to provide to PCI SSC such Assessment Results and Related Materials (defined below) as PCI SSC may reasonably request with respect to any QSA Company client for which QSA has performed a PCI SSC Assessment. Each agreement between QSA and each of its QSA Company clients (each a "Client Agreement") shall include such provisions as may be necessary or appropriate, or otherwise required by PCI SSC, to ensure that QSA has all rights, licenses and other permissions necessary for QSA to comply with its obligations and requirements pursuant to this Agreement, with no conditions, qualifications or other terms (whether in such Client

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

A.10.3 Governing Law; Severability

Any dispute in any way arising out of or in connection with the interpretation or performance of this Agreement, which cannot be amicably settled within thirty (30) days of the written notice of the dispute given to the other party by exercising the best efforts and good faith of the parties, shall be finally settled by the courts of Delaware (United States of America) in accordance with Delaware law without resort to its conflict of laws provisions. Each of the parties irrevocably submits to the nonexclusive jurisdiction of the United States District Courts for the State of Delaware and the local courts of the State of Delaware and waives any objection to venue in said courts. Should any individual provision of this Agreement be or become void, invalid or unenforceable, the validity of the remainder of this Agreement shall not be affected thereby and shall remain in full force and effect, in so far as the primary purpose of this Agreement is not frustrated.

A.10.4 Entire Agreement; Modification; Waivers

The parties agree that this Agreement, including the QSA Qualification Requirements and any other documents, addenda, supplements, amendments, appendices, exhibits, schedules or other materials incorporated herein by reference (each of which is hereby incorporated into and made a part of this Agreement by this reference), is the exclusive statement of the agreement between the parties with respect to the subject matter hereof, which supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the parties with respect to such subject matter (including without limitation, if applicable, each prior *Qualified Security Assessor (QSA) Agreement* between QSA and PCI SSC). This Agreement may be

modified, altered or amended only (i) by written instrument duly executed by both parties or (ii) by PCI SSC upon thirty (30) days' written notice to QSA, provided, however, that if QSA does not agree with such unilateral modification, alteration or amendment, QSA shall have the right, exercisable at any time within the aforementioned thirty (30) day period, to terminate this Agreement upon written notice of its intention to so terminate to PCI SSC. Any such unilateral modification, alteration or amendment will be effective as of the end of such 30-day period unless the Agreement is earlier terminated by QSA pursuant to the preceding sentence. The waiver or failure of either party to exercise in any respect any right provided for in this Agreement shall not be deemed a waiver of any further right under this Agreement.

A.10.5 Assignment

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

A.10.6 Independent Contractors

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

A.10.7 Remedies

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

A.10.8 Counterparts

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

A.10.9 Conflict

In the event of any express conflict or inconsistency between the terms and provisions of this Agreement and terms and provisions of the QSA Qualification Requirements, this Agreement shall control. In the event of any express conflict or inconsistency between the terms and provisions of this Agreement and the terms and provisions of any Addendum or the *Program Qualification Requirements* or policies of PCI SSC with respect to any Related PCI SSC Program in which QSA is a then participant, the conflicting or inconsistent terms and provisions of such Addendum, *Program Qualification Requirements* or policy shall control, but only to the extent necessary to resolve such conflict or inconsistency with respect to QSA's participation in such Related PCI SSC Program. Any and all disputes or disagreements regarding any such conflict or inconsistency shall be resolved by PCI SSC in its sole but reasonable discretion, and all determinations of PCI SSC in this regard shall be final and binding.

A.10.10 No Third-Party Beneficiaries

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

[remainder of page intentionally left blank]

Appendix B. Insurance Coverage

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

- WORKERS' COMPENSATION: Statutory Workers Compensation as required by applicable law and
- EMPLOYER'S LIABILITY with a limit of $1,000,000
- 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. PCI SSC to be added as "Additional Insured." The policy Coverage Territory must include the entire Region(s) in which the QSA Company has qualified to operate.
- COMMERCIAL AUTOMOBILE INSURANCE including owned, leased, hired, or non-owned autos subject to minimum limits of $1,000,000 per accident
- 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 QSA Company's client against the QSA Company for theft committed by the QSA Company's Employees. The minimum limit shall be $1,000,000 each loss and annual aggregate. The policy Coverage Territory must include the entire Region(s) in which the QSA Company is qualified to operate.
- TECHNOLOGY ERRORS & OMISSIONS, CYBER-RISK and PRIVACY LIABILITY INSURANCE covering liabilities for financial loss resulting or arising from acts, errors or omissions in rendering computer or information technology Services, or from data damage/destruction/corruption, including without limitation, failure to protect privacy, unauthorized access, unauthorized use, virus transmission, denial of service and loss of income from network security failures in connection with the Services provided under this agreement with a minimum limit of two million dollars ($2,000,000) each claim and annual aggregate. The policy Coverage Territory must include the entire Region(s) in which the QSA Company is qualified to operate.

If any of the above insurance is written on a claims-made basis, then Security Assessor shall maintain such insurance for five (5) years after the termination of this agreement. The limits shown in the appendix may be written in other currencies, but should be the equivalent of the limits in US dollars shown here.

Without limiting Security Assessor'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 Security Assessor's performance of the Services under this agreement. The insurers shall agree that the Security Assessor's insurance is primary and any insurance maintained by CPS SSC shall be excess and non-contributing to the Security Assessor's insurance.

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

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

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

Appendix C. QSA Company Application

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

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

☐ The Company acknowledges and agrees that in order to participate as a QSA Company in the QSA Program, it must satisfy all of the requirements specified in the QSA Qualification Requirements and supporting documents

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

QSA Company Business Requirements – Section 2
(Continued)
Independence – 2.2.2 Provisions

☐ The Company hereby acknowledges and agrees that it must adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing PCI SSC Assessments.

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

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

☐ Below or attached hereto are (a) a description of the Company's practices for maintaining and assuring assessor independence, including but not limited to, the Company's practices, organizational structures, separation of duties, rules, and employee education in place to prevent conflicts of interest, and (b) copies of all written Company policies relating to any of the foregoing.

☐ The Company hereby:

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

QSA Company Business Requirements – Section 2
(Continued)
Insurance Coverage – 2.3.2 Provisions
☐ The Company agrees that at all times while its QSA Agreement is in effect, Company will maintain sufficient insurance, insurers, coverage, exclusions, and deductibles that PCI SSC reasonably requests to adequately insure the Company for its obligations and liabilities under the QSA Agreement, including without limitation the Company's indemnification obligations.
☐ The Company hereby acknowledges and agrees to adhere to all requirements for insurance coverage required by PCI SSC, including without limitation the requirements in Appendix B, "Insurance Coverage," which includes details of required insurance coverage.
☐ The Company hereby certifies to PCI SSC that, along with this application, the Company is providing to PCI SSC a proof-of-coverage statement demonstrating that its insurance coverage matches locally set insurance coverage requirements.
☐ The Company hereby agrees not to subcontract or assign any portion of the QSA services without first (a) obtaining the prior written consent of PCI SSC (see Section 3.2.1) and (b) providing to PCI SSC proof-of-coverage statements covering all such subcontractors and demonstrating that such insurance satisfies all applicable PCI SSC insurance coverage requirements (see Appendix B).
☐ A copy of the Company's bound insurance coverage is attached to this application.
Fees – 2.4.1 Requirements
☐ The Company acknowledges that it will be charged an application processing fee, annual regional qualification fees for each geographic region or country in which the Company intends to perform PCI DSS Assessments, and annual fees for each QSA Employee's PCI SSC training.
☐ The Company agrees to pay all such fees upon invoice from PCI SSC (or as part of the QSA Employee training registration process, if applicable), and that any such fees invoiced by PCI SSC will be made payable to PCI SSC according to instructions provided on the corresponding invoice.
QSA Agreement – 2.5.1 Requirements
☐ The Company acknowledges and agrees that along with its completed application package it is providing to PCI SSC a QSA Agreement between PCI SSC and the Company, in unmodified form, signed by a duly authorized officer of the Company.
PCI SSC Code of Professional Responsibility – 3.3.1 Requirements
☐ The Company acknowledges and agrees that it has read and understands the PCI SSC Code of Professional Responsibility, and hereby agrees to advocate, continuously adhere to, and support the terms and provisions thereof.

QSA Capability Requirements – Section 3
QSA Company Skills and Experience – 3.1.2 Provisions
☐ The Company represents and warrants that it currently possesses (and at all times while it is a QSA Company will continue to possess) technical security assessment experience similar or related to PCI DSS Assessments, and that it has (and must have) a dedicated security practice that includes staff with specific job functions that support the security practice.
☐ Included immediately below are descriptions of the Company's experience and knowledge with information security audit engagements (including but not limited to any related to payment systems), equal to at least one year or three separate audits:

QSA Capability Requirements – Section 3		
(Continued)		
Engagement 1:	Years:	Months:
Description of security audit/engagement:		
Engagement 2 (if applicable):	Years:	Months:
Description of security audit/engagement:		
Engagement 3 (if applicable):	Years:	Months:
Description of security audit/engagement:		

☐ Immediately below is a description of the Company's relevant areas of specialization within information security (for example, network security, database and application security, and incident response), demonstrating at least one area of specialization:

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

Provide two client references from security engagements within the last 12 months:			
Client:		From (date):	To (date):
Contact name:		Job title:	
Contact phone number:		E-mail address:	
Client:		From (date):	To (date):
Contact name:		Job title:	
Contact phone number:		E-mail address:	

QSA Administrative Requirements – Section 4
☐ The Company hereby acknowledges and agrees to the administrative requirements for QSA Companies set forth in the QSA Qualification Requirements, including company contacts, background checks, adherence to PCI DSS procedures, quality assurance, and protection of confidential and sensitive information.
Background Checks – 4.2.2 Provisions
☐ The Company agrees that its policies and hiring procedures must include performing background checks and satisfying the provisions in Section 4.2.2 (to the extent legally permitted within the applicable jurisdiction) when hiring each applicant QSA Employee.
☐ The Company hereby attests that its policies and hiring procedures include performing background checks in full accordance with Section 4.2.
☐ The Company hereby attests that it successfully completes background checks for each candidate QSA Employee in accordance with the provisions of Section 4.2.2
Below is a summary description of the Company's personnel background check policies:
The Company's personnel background check policies and procedures include the following (*to the extent legally permitted within the applicable jurisdiction*): ☐ Verification of aliases (when applicable) ☐ Reviewing records of any criminal activity, such as felony (or non-US equivalent) convictions or outstanding warrants ☐ Annually review records of any criminal activity, such as felony (or non-US equivalent) convictions or outstanding warrants ☐ Minor offenses (for example, misdemeanors or non-US equivalents) are allowed, but major offenses (for example, felonies or non-US equivalents) automatically disqualify an employee from serving as a QSA Employee
☐ The Company understands and agrees that, upon request, it must provide to PCI SSC the background check history for each of its QSA Employees, to the extent legally permitted within the applicable jurisdiction.
Internal Quality Assurance – 4.3.2 Provisions
☐ The Company acknowledges and agrees that it must adhere to all quality assurance requirements described in the QSA Qualification Requirements and supporting documentation, must have a quality assurance program, documented in its Quality Assurance manual, and must maintain and adhere to a documented quality assurance process and manual that includes all items described in Section 4.3.1 of the QSA Qualification Requirements.
☐ The Company acknowledges and agrees that its internal quality assurance reviews must be performed by qualified personnel (independent of the assessing and/or authoring QSA Employee) and must cover assessment procedures performed, supporting documentation, information documented in the ROC related to the appropriate selection of system components, sampling procedures, compensating controls, remediation recommendations, proper use of payment definitions, consistent findings, and thorough documentation of results.

QSA Administrative Requirements – Section 4
(Continued)
The Company acknowledges and agrees that as a QSA Company, it must at its sole cost and expense:
☐ At all times maintain and adhere to the internal quality assurance requirements as described in Section 4.3.1 of the QSA Qualification Requirements.
☐ Provide to PCI SSC, upon request and from time to time, a complete copy of the Company's quality assurance manual, in accordance with the QSA Qualification Requirements and supporting documentation.
☐ Permit PCI SSC, upon request from time to time, to conduct audits of the Company and/or to conduct site visits.
☐ Inform each Company PCI SSC Assessment client of the *QSA Feedback Form* (available on the Website), upon commencement of the PCI DSS Assessment for that client.
☐ Conduct all PCI DSS Assessments on-site at the applicable client's facilities.
Protection of Confidential and Sensitive Information – 4.4.2 Provisions
☐ The Company currently has and agrees to adhere to a documented process for protection of confidential and sensitive information, which includes adequate physical, electronic, and procedural safeguards consistent with industry-accepted practices to protect confidential and sensitive information against any threats or unauthorized access during storage, processing, and/or communicating of this information.
☐ The Company must maintain the privacy and confidentiality of information obtained in the course of performing its duties under the QSA Agreement, unless (and to the extent) disclosure is expressly permitted thereunder.
☐ The Company's confidential and sensitive data protection handling policies and practices include all physical, electronic, and procedural safeguards described in Section 4.4 of the QSA Qualification Requirements.
☐ The Company agrees to provide PCI SSC a blank copy of the confidentiality agreement that it requires each QSA to sign (include a blank copy of such confidentiality agreement with this application).
Evidence (Workpaper) Retention – 4.5.2 Provisions
☐ The Company has an evidence-retention policy and procedures per Section 4.5.1 of the QSA Qualification Requirements and agrees to retain all records created and/or obtained during each PCI DSS Assessment for a minimum of three (3) years.
☐ The Company has and agrees to adhere to a documented process for securely maintaining digital and/or hard copies of all case logs, Assessment Results, workpapers, notes, and other information created and/or obtained by the Company during each PCI DSS Assessment.
☐ The Company agrees to make the foregoing materials and information available to PCI SSC upon request for a minimum of three (3) years.
☐ The Company agrees to provide a copy of the foregoing evidence-retention policy and procedures to PCI SSC upon request.
Security Incident Response – 4.6.2 Provisions
☐ The Company has a security incident-response plan and procedures per Section 4.6 of the QSA Qualification Requirements and agrees to retain all records created and/or obtained in connection with the discovery and response regarding the applicable Incident for a minimum of three (3) years.
☐ The Company's security incident-response plan includes instructions and procedures for reporting and documenting evidence of each Incident.

Signature

By signing below, the undersigned hereby:

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

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

Legal Name of Applicant QSA Company			
Officer:		Title:	
By:			
Duly authorized officer signature ↑		*Date* ↑	

Appendix D. QSA Employee Application

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

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

QSA Employee Skills, Experience and Education			
Provide examples of the Candidate's work and/or description of experience in the following areas of expertise (requires at least one year in each area):			
Examples of work and/or description of experience in **network security** (for example, administration of firewalls, intrusion prevention systems, etc.):			
From (date):	To (date):	Total time: Years	Months
Examples of work and/or description of experience in **application security:**			
From (date):	To (date):	Total time: Years	Months
Examples of work and/or description of experience in **systems integration and security:**			
From (date):	To (date):	Total time: Years	Months
Examples of work and/or description of experience in **auditing information systems and processes:**			
From (date):	To (date):	Total time: Years	Months
Examples of work and/or description of experience in **information security risk assessment or risk management:**			
From (date):	To (date):	Total time: Years	Months

Candidate Professional Certifications (check all that apply):			
☐	(ISC)^2 CISSP	Certification number:	Expiry date:
☐	ISACA CISM	Certification number:	Expiry date:
☐	ISACA CISA	Certification number:	Expiry date:
☐	SANS GIAC/GSNA	Certification number:	Expiry date:
☐	IRCA Auditor	Certification number:	Expiry date:
☐	IIA CIA	Certification number:	Expiry date:
☐	ISO 27001, Lead Auditor/Implementer, Internal Auditor	Certification number: Accredited certification body:	Date achieved:

Signature

By signing below, I hereby acknowledge and agree that:

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

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

(c) I have read and understand the PCI SSC Code of Professional Responsibility, and will advocate, continuously adhere to and support the terms and provisions thereof.

Candidate:		Title:	
Candidate signature ↑		*Date* ↑	