Payment Card Industry (PCI)
Data Security Standard
Validation Requirements

For Qualified Security Assessors (QSA)

Version 1.2

October 2008

Document Changes

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

Table of Contents

1 Introduction

In response to requests from merchants for a unified set of payment account data security requirements, members of the payment card industry ("PCI") adopted the PCI Data Security Standard ("PCI DSS"), a set of requirements for cardholder data protection across the entire industry, maintained by the PCI Security Standards Council, LLC ("PCI SSC"), the current version of which is available on the PCI SSC web site at http://www.pcisecuritystandards.org (the"Website"). Organizations that are authorized to validate an entity's adherence to PCI DSS requirements are referred to as "Qualified Security Assessors" or "QSAs". Validation of these requirements by independent and qualified security companies is important to the effectiveness of PCI DSS. The quality, reliability, and consistency of a QSA's work provide confidence that cardholder data are adequately protected.

Key to the success of the PCI DSS is merchant and service provider compliance. When implemented appropriately, PCI DSS requirements provide a well-aimed defense against data exposure and compromise. As a result, on-site PCI DSS assessments performed by Qualified Security Assessors ("Assessments") have become increasingly critical in today's environment. The proficiency with which a QSA conducts an Assessment can have a tremendous impact on the consistent and proper application of PCI measures and controls. The current version of these *Payment Card Industry (PCI) Data Security Standard Validation Requirements for Qualified Security Assessors* (the *"QSA Validation Requirements"*), as available through the Website, describes the necessary qualifications a QSA must have to be recognized by the PCI SSC to perform Assessments.

Members of the payment card industry also adopted the Payment Application Data Security Standard (the "PA-DSS"), a set of requirements derived from and closely related to the PCI DSS, but intended to illustrate for payment software vendors what is required for their payment software applications to facilitate and not prevent their customers' PCI DSS compliance. The PA-DSS is also maintained by PCI SSC and is available as part of the *Payment Application Data Security Standard and Audit Procedures* (*"PA-DSS Security Audit Procedures"*) through the Website. Each QSA organization that chooses to additionally qualify to become a Payment Application Qualified Security Assessor (defined below) must satisfy the requirements set forth in the most current version of the *Payment Card Industry (PCI) Data Security Standard QSA Validation Requirements—Supplement for Payment Application Qualified Security Assessors (PA-QSA)* (available through the Website), in addition to continuing to satisfy all general requirements for QSAs.

1.1 Terminology

Throughout these *QSA Validation Requirements*, the following terms shall have the following meanings:

"Payment Application Qualified Security Assessor" or "PA-QSA" means a QSA company that provides services to payment application vendors in order to validate such vendors' payment applications as adhering to the requirements of the PA-DSS and that has satisfied and continues to satisfy all requirements applicable to PA-QSAs, as described in the *QSA Validation Requirements—Supplement for Payment Application Qualified Security Assessors (PA-QSA)*.

"PA-DSS Assessment" means assessment of vendor payment applications in accordance with the *PA-DSS Security Audit Procedures* in order to establish vendor compliance with the PA-DSS.

"Principal QSA" and "Associate QSA" are used to refer to those QSA companies that have satisfied additional qualification requirements where needed to support PCI DSS adoption in certain global markets, as described in further detail in *QSA Validation Requirements—Supplement for Principal-Associate Qualified Security Assessors.*

"QSA Agreement" refers to the *PCI Qualified Security Assessor (QSA) Agreement* attached as Appendix A to the *QSA Validation Requirements*.

"QSA employee" refers to an individual who is employed by a QSA company and who has satisfied and continues to satisfy all QSA Requirements applicable to those of the QSA's employees who will conduct Assessments, as described in further detail herein.

"Qualified Security Assessor" or "QSA" refers to a company that has satisfied and continues to satisfy all requirements set forth in these *QSA Validation Requirements*.

All capitalized terms used in these *QSA Validation Requirements* without definition shall have the meanings specified in the *QSA Agreement*.

1.2 Goal

To qualify as a QSA by PCI SSC, a company must meet or exceed the requirements described in the *QSA Validation Requirements* and execute the QSA Agreement (see Appendix A) with PCI SSC and comply with its terms.

The requirements defined in the *QSA Validation Requirements* serve as a **validation baseline** for PCI SSC and provide a transparent process for QSA qualification and re-qualification across the payment industry.

1.3 Qualification Process Overview

The QSA qualification process has potentially three parts: the first involves the qualification of the security company itself. The second relates to the qualification of the company's employee(s) who will be performing and/or managing the on-site PCI DSS Assessments. The third (and optional) part relates to qualification of Principle and Associate QSAs where needed to support global market needs. (See *QSA Validation Requirements—Supplement for Principal-Associate Qualified Security Assessors.*)

Those QSA organizations that choose to additionally qualify to become a Payment Application QSA (PA-QSA) must also complete the requirements specified in PCI DSS QSA Validation Requirements—Supplement for Payment Application Qualified Security Assessors (PA-QSA).

All QSAs and PA-QSAs will be identified on PCI SSC's list of QSAs on the Website (the "QSA List") in accordance with the QSA Agreement. If a company is not on the QSA List, its work product is not recognized by PCI SSC. All QSAs must re-qualify annually.

QSA Validation Requirements are incorporated into the QSA Agreement. To initiate the qualification process, the security company must sign the QSA Agreement in unmodified form and submit it to PCI SSC.

1.4 Document Structure

QSA Validation Requirements define the requirements a security company must meet to become a QSA. The document is structured in five sections as follows.

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

Section 2: QSA 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. QSA fees and agreements are also covered.

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 Administrative Requirements focuses on the logistics of doing business as a PCI DSS QSA, including background checks, adherence to PCI DSS procedures, quality assurance, and protection of confidential and sensitive information.

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

Appendices: The appendices to the *QSA Validation Requirements* include the QSA Agreement and several helpful checklists, feedback forms, and detailed fee requirements.

1.5 Related Publications

The *QSA Validation Requirements* should be used in conjunction with the following other PCI SSC publications, each available through the Website:

PCI DSS

- *Payment Card Industry (PCI) Data Security Standard Security Audit Procedures ("PCI DSS Security Audit Procedures")*
- *PA-DSS Security Audit Procedures*

QSA Validation Requirements for Principal and Associate QSAs and PA-QSAs can be found in the following two documents, also available through the Website:

- *QSA Validation Requirements—Supplement for Principal-Associate Qualified Security Assessors*
- *QSA Validation Requirements—Supplement for Payment Application Qualified Security Assessors (PA-QSA)*

1.6 QSA Application Process

In addition to outlining the requirements that a PCI QSA must meet to perform on-site PCI DSS Assessments, the *QSA Validation Requirements* describe the information that must be provided to PCI SSC as part of the application process. Each outlined requirement is followed by the information that must be submitted to document that the security company meets or exceeds the stated requirements.

To facilitate preparation of the application package, refer to Appendix B: QSA – New Application Process Checklist. 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 in a language other than English must be accompanied by a certified English translation (examples include business licenses and insurance certificates).

Applications must indicate which geographic region(s)—see Appendix D – QSA Fees for list of region(s) or country(s)—the QSA is applying for, and include all relevant application fees for each applicable region or country.

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

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

E-mail submissions will not be accepted.

Important Note: PCI SSC reserves the right to reject any application from any applicant (company or individual) that PCI SSC determines has committed, within two (2) years prior to the application date, any conduct that would have been considered a "Violation" (defined in Section 5.2 below) 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, in light of the circumstances.

1.7 Requests

PCI SSC, in an effort to maintain the integrity of the QSA program, may request from time to time demonstrated adherence to the requirements listed in this document. The QSA is responsible to respond to such a PCI SSC request with the documented evidence no later than three (3) weeks from receipt of written notice.

2 QSA Business Requirements

This section describes the minimum business requirements and related information that must be provided to PCI SSC (for Principal and/or Associate QSA requirements, see *QSA Validation Requirements—Supplement for Principal-Associate Qualified Security Assessors*, and for PA-QSA requirements, see *QSA Validation Requirements—Supplement for Payment Application Qualified Security Assessors (PA-QSA)*). Subsections include information about the company's business legitimacy, independence, and required insurance coverage.

2.1 Business Legitimacy

2.1.1 Requirement

The QSA must be recognized as a legal entity.

2.1.2 Provisions

The following information must be provided to PCI SSC:

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

2.2 Independence

2.2.1 Requirement

The QSA must adhere to professional and business ethics, perform all duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing Assessments.

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

The QSA must adhere to all independence requirements in this section, as required by PCI SSC, including without limitation, the following (collectively, the "Specified Independence Requirements").

- The QSA will not undertake to perform Assessments of entities that it controls or with which it is under common control or in which it holds any investment.
- The QSA has not offered or provided (and will not offer or provide) any gift, gratuity, service, or other inducement to any employee of PCI SSC or any QSA subject or agency involved in retaining the QSA to enter into the QSA Agreement or to provide QSA-related services.
- The QSA must fully disclose in the Report on Compliance if they assess customers who use any security-related devices or security-related applications that have been developed or manufactured by the QSA, or to which the QSA owns the rights, or that the QSA has configured or manages, including the following:
  - Application or Network Firewalls
  - Intrusion Detection/Prevention Systems

- Database or other Encryption Solutions
- Security Audit Log Solutions
- File Integrity Monitoring Solutions
- Anti-virus solutions

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

2.2.2 Provisions

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

- The QSA customer uses products or applications developed or manufactured by the QSA company.
- The QSA customer uses products or applications managed or configured by the QSA company.
- The description must include details with respect to compliance with the Specified Independence Requirements called out in Section 2.1 above.

2.3 Insurance Coverage

2.3.1 Requirement

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

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

2.3.2 Provisions

The QSA must provide a proof of coverage statement to PCI SSC to demonstrate that insurance coverage matches locally set insurance coverage requirements. If the QSA subcontracts or assigns any portion of the QSA services (only with prior written consent from PCI SSC—see Section 3.2.1), the QSA must also provide to PCI SSC proof of coverage statements from all subcontractors to demonstrate that subcontractors purchase and maintain insurance to match insurance coverage requirements.

2.4 QSA Fees

2.4.1 Requirement

Each QSA applicant must provide to PCI SSC an initial processing fee per geographic region or country in which the QSA applicant intends to perform Assessments (see Appendix D – QSA Fees). These fees are credited toward the qualification fee (see below) if a company is qualified as a QSA. The initial processing fee check should be made payable to PCI SSC and mailed with the completed QSA application package. See Section 1.6 of this document for the mailing address. Once a company is approved for qualification as a QSA, the following fees may also apply.

- The qualification fee, which must be paid in full within 30 days of notification. This fee may vary by location, as specified in Appendix D, QSA Fees.
- An annual QSA re-qualification fee for subsequent years, also summarized by location in Appendix D, QSA Fees.
- A training fee for each QSA employee to be qualified, for training sponsored by PCI SSC. This is an annual fee. See Appendix D, QSA Fees.

Note:
All fees are subject to change.

Additional fees apply for PA-QSA qualification and Principal-Associate QSA qualification; these are outlined in *QSA Validation Requirements—Supplement for Payment Application Qualified Security Assessors (PA-QSA),* Appendix E, and *QSA Validation Requirements—Supplement for Principal-Associate Qualified Security Assessors,* Appendix D, respectively.

2.5 QSA Agreements

2.5.1 Requirement

PCI SSC requires that all agreements between PCI SSC and the QSA (including the QSA Agreement) be signed by a duly authorized officer of the QSA, submitted in unmodified form to PCI SSC, and mailed with the completed QSA application package.

The QSA Agreement requires that all QSAs and employees of the QSA comply with the requirements outlined in the *QSA Validation Requirements*.

There are various agreements, depending on what QSA programs your company is applying for. Initially to become a QSA, your company must submit the QSA Agreement.

Once the QSA Agreement and associated documentation is submitted, to be qualified for additional programs, please submit the appropriate optional agreement (s) along with the completed application package(s), as follows:

- *PCI SSC Agreement for Principal-Associate QSAs*
- *Principal-Associate QSA Agreement*
- *PA-QSA Agreement*

See *QSA Validation Requirements—Supplement for Payment Application Qualified Security Assessors (PA-QSA)* or *QSA Validation Requirements—Supplement for Principal-Associate Qualified Security Assessors* as appropriate more information and for agreements and checklists.

3 QSA Capability Requirements

This section describes the minimum QSA capability requirements and related documentation the QSA must provide to PCI SSC. The QSA must demonstrate security audit expertise, work history, and industry experience.

3.1 QSA Company - Services and Experience

3.1.1 Requirement

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

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

3.1.2 Provisions

The following information must be provided to PCI SSC:

- The QSA'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 QSA'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 number of all employees and the number of employees performing security assessments; and
  - For the number of employees performing security assessments, the percentage of time dedicated to such assessments
- Brief description of core business offerings
- Description of size and types of market segments in which the QSA tends to focus, such as Fortune 500, financial industry, insurance industry, or small-to-medium sized businesses
- List of languages supported by the QSA
- Two client references from security engagements within the last 12 months

3.2 QSA Staff – Skills and Experience

Each QSA 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 Assessment
- Reviewing the work product that supports the audit procedures
- Ensuring adherence to the *PCI DSS Security Audit Procedures*
- Scoping decisions
- Selecting systems and system components where sampling is employed
- Evaluating compensating controls
- Producing the final report

3.2.1 Requirement

The QSA employee(s) performing or managing PCI DSS Assessments must:

- Have sufficient information security knowledge and experience to conduct technically complex security assessments
- Possess industry-recognized security certification(s) or equivalent work experience
- Be knowledgeable about the PCI DSS and the PCI DSS Security Audit Procedures
- Attend annual 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 so pass any exam in connection with such training, the QSA employee must no longer lead or manage a PCI DSS assessment until successfully passing the exam on a future attempt
- Be employees of the QSA (meaning this work cannot be subcontracted to non-employees) unless PCI SSC has given prior written consent for each subcontracted worker.

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

3.2.2 Provisions

The following information must be provided to PCI SSC for each individual to be qualified:

- Education (subject, level, institute) equal to bachelor's degree or professional certificate
- Area(s) of expertise (Network Security, Application Security and Consultancy, System Integration, Auditing, Special Skills), with at least 1 year (total) in three separate areas

- Years of working experience and responsibilities
- Years of working experience related to payment industry and responsibilities
- Résumé
- Minimum of one of the following certifications must be provided to PCI SSC:
  - Copy of Certified Information System Security Professional (CISSP) certificate and ID number
  - Copy of Certified Information Systems Auditor (CISA) certificate and ID number
  - Copy of Certified Information Security Manager (CISM) certificate and ID number

If an employee does not satisfy any of the above education criteria or certificates, he or she must provide a description of a **minimum of five years** of relevant information security experience or proof of other recognized security certifications.

4 QSA Administrative Requirements

This section describes the administrative requirements for QSAs, 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 must provide PCI SSC with a primary and secondary contact and related contact information for each.

4.1.2 Provisions

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

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

4.2 Background Checks

4.2.1 Requirement

The QSA must perform a background check (as described in Subsection 4.2.2) on all QSA employees, if legally permitted within the applicable jurisdiction.

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

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

4.2.2 Provisions

The QSA must provide the following to PCI SSC:

- A written statement that the QSA conducts background checks for each employee prior to submitting employee qualification requests to PCI SSC, and that each employee with respect to which qualification materials have been submitted has successfully passed the background check in accordance with the QSA's policies and procedures (where legally permitted).
- A summary description of current QSA personnel background check policies and procedures, to confirm the procedures include at least (to the extent legally permissible in the applicable jurisdiction):
  - Gathering of current photographs

- Verification of aliases (when applicable)
- Reviewing of records of any criminal activity, arrests or convictions updated annually
- Comparing of fingerprints with national and regional criminal records
- That misdemeanors are allowed, but that felonies automatically disqualify an employee from consideration as a QSA employee

4.3 Adherence to PCI Procedures

4.3.1 Requirements

- For each Assessment, the resulting QSA report must follow the Report on Compliance (ROC) template and instructions, as outlined in the *PCI DSS Security Audit Procedures.*
- The QSA must prepare each ROC based on evidence obtained by following the *PCI DSS Security Audit Procedures.*

4.3.2 Requirements

- The QSA must accompany a ROC with an "Attestation of Compliance" in the form available through http://www.pcisecuritystandards.org, signed by a duly authorized officer of the QSA, that summarizes whether the entity is in compliance or not in compliance with PCI DSS, and any related findings.

4.4 Quality Assurance

4.4.1 Requirements

- The QSA must have implemented a quality assurance program as documented in the quality assurance program manual (as described in Subsection 4.4.2).
- The QSA must provide a QSA Feedback Form to their client at the completion of the audit. See Appendix C, Sample QSA Feedback Form.
- The QSA must adhere to all quality assurance requirements mandated by PCI SSC.
- PCI SSC reserves the right to conduct site visits and audit the QSA at the discretion of the PCI SSC.
- Upon request, the QSA must provide the quality assurance manual to PCI SSC.

4.4.2 Provisions

The QSA must provide the following to PCI SSC:

- A description of the contents of the QSA quality assurance manual, to confirm the procedures fully document the PCI audit processes and the review process for generation of the ROC, including at least the following:

- Reviews of performed audit procedures, supporting documentation, and 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
- A requirement that all QSA employees must adhere to the *PCI DSS Security Audit Procedures*

4.5 Protection of Confidential and Sensitive Information

4.5.1 Requirements

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

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

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

4.5.2 Provisions

The QSA must provide the following:

- A description of the QSA's confidential and sensitive data-protection handling practices, including at a minimum the following physical, electronic, and procedural safeguards:
  - Systems storing customer data do not reside on Internet-accessible systems
  - Protection of systems storing customer data by adequate network and application-layer controls, including a firewall and IDS/IPS
  - The following physical and logical access controls:
    - Restricting access (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 role-based access control
    - Encryption of sensitive customer information when transmitted over the Internet either by e-mail or other means
    - Secure transport and storage of backup media
    - Encryption of customer data on consultants' laptops
- A description of requirements and processes used to ensure employee confidentiality of customer data, including a (blank) copy of confidentiality agreements required to be signed by employees

The QSA must sign the QSA Agreement, which includes a statement that the QSA will adhere to the foregoing requirement.

4.6 Evidence Retention

4.6.1 Requirements

- The QSA must secure (in accordance with 4.5 above) and maintain digital and/or hard copies of case logs, audit results and work papers, notes, and any technical information that was created and/or obtained during the PCI DSS Assessment for a minimum of three (3) years.
- The QSA must adhere to all evidence-retention requirements, as required by PCI SSC.
- This information must be available upon request by PCI SSC and its Affiliates for a minimum of three (3) years.
- The QSA must provide a copy of the evidence-retention policy and procedures to PCI SSC upon request.

4.6.2 Provisions

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

5 QSA Initial Qualification and Annual Re-qualification

This section describes what happens after initial qualification and items related to the annual QSA re-qualification. This section includes: (1) the QSA List, (2) annual maintenance of the QSA qualification, and (3) revocation, if necessary, of a QSA's qualification

5.1 QSA List

Once a company has met all requirements specified in the *QSA Validation Requirements*, PCI SSC will add the QSA to QSA List in accordance with the QSA Agreement. Only those QSAs on the QSA List are authorized by PCI SSC to perform PCI DSS onsite Assessments.

The QSA List and PA-QSA list are posted on the Website.

Those QSAs that have additionally qualified as Associate QSAs (per *QSA Validation Requirements–Supplement for Principal-Associate Qualified Security Assessors)*) will be identified as QSAs on the Website, with the Principal QSA noted as the primary contact.

Those QSAs that have additionally qualified to perform PA-DSS Assessments (per *QSA Validation Requirements–Supplement for Payment Application Qualified Security Assessors (PA-QSA)*) will be identified as PA-QSAs on the Website. Only those QSAs that have also qualified as PA-QSAs are authorized by PCI SSC to perform PA-DSS Assessments.

In the event a company does not meet the requirements specified in the *QSA Validation Requirements*, PCI SSC will notify the company.

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

If a company's appeal is denied, its name will not be placed on the QSA List.

5.2 QSA Re-qualification

5.2.1 Requirements

All QSAs and employees must be re-qualified by PCI SSC on an annual basis, based on the QSA's original qualification date. Re-qualification is based on payment of annual fees, proof of training attended, and satisfactory feedback from the QSA clients (the merchants or service providers that were assessed), from PCI SSC, and from payment brand participants.

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

5.2.2 Provisions

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

- Feedback from QSA clients (entities that were assessed), from PCI SSC, and from payment brand participants (see Appendix C, Sample QSA Feedback Form). Significant or excessive unsatisfactory feedback may be cause for revocation;

- Payment of annual re-qualification fees (see Appendix D, Fees);
- Proof of information systems audit training within the last 12 months to support professional certifications (even if the employee does yet not have professional certifications), of a minimum 20 hours per year and 120 hours over the rolling three-year period. This is in addition to training provided by PCI SSC.

5.3 QSA Revocation Process

Each of the following conditions (each a "Violation") may result in immediate Revocation (as defined in the *QSA Agreement*) of QSA qualification (including removal from the QSA List), subject to reinstatement pending a successful appeal in accordance with the *QSA Agreement*, and/or termination of the *QSA Agreement*:

- The QSA (or any QSA employee thereof) fails to validate compliance in accordance with the *PCI DSS Security Audit procedures* and/or the *PA-DSS Security Audit Procedures*, as applicable.
- The QSA (or any QSA employee thereof) violates any provision or obligation regarding non-disclosure of confidential materials.
- The QSA (or any QSA employee thereof) fails to maintain physical, electronic, and procedural safeguards to protect confidential or sensitive information;
- The QSA (or any QSA employee thereof) fails to report unauthorized access to any system storing confidential or sensitive information.
- The QSA (or any QSA employee thereof) engages in unprofessional or unethical business conduct.
- The QSA (or any QSA employee thereof) fails to provide quality services, based on customer feedback or evaluation by PCI SSC or its affiliates.
- The QSA (or any QSA employee thereof) is determined to have cheated on any exam in connection with QSA or PA-QSA training, including without limitation, submitting work that is not the work of the QSA employee taking the exam, theft of or unauthorized access to an exam, use of an alternate, stand-in or proxy during an exam, use of any prohibited or unauthorized materials, notes or computer programs during an exam and providing or communicating in any way any unauthorized information to another person during an exam.
- The QSA (or any QSA employee thereof) is determined by PCI SSC to have provided false or intentionally incomplete or misleading information to the Council in any application or other materials.
- The QSA (or any QSA employee thereof) failed to promptly notify the Council of any event described above that occured at any time after the date two (2) years before such QSA or QSA employee's qualification by PCI SSC.
- The QSA is otherwise not in Good Standing (as defined in the QSA Agreement).

In the event of any Revocation, the QSAs name will be removed from the QSA List, PCI SSC will notify the QSA of the corresponding Violation, and the QSA will have an opportunity to defend its conduct through an appeal to PCI SSC in accordance with the *QSA Agreement*.

All appeals must be submitted to PCI SSC in writing, addressed to the PCI SSC General Manager and follow all applicable procedures as specified by PCI SSC. PCI SSC will review all relevant evidence submitted by the complainant (if any) and QSA in connection with such appeals and make a decision as to whether termination of QSA qualification is warranted. All decisions of PCI SSC regarding revocation are final.

If a QSA's appeal is denied or the QSA fails to appeal in accordance with the *QSA Agreement*, PCI SSC may immediately terminate the corresponding *QSA Agreement* and notify the participating payment brands and/or acquirers.

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 herein). 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 Appendix D):			
Primary Contact			
Name:	Title:		
Direct Telephone Number:	E-mail:		
Location:	Fax:		
Secondary Contact			
Name:	Title:		
Direct Telephone Number:	E-mail:		
Location:	Fax:		
Applicant's Officer Signature ↑		*Date* ↑	
Applicant Officer Name:	Title:		
PCI SSC			
PCI SSC Signature ↑		*Date* ↑	
Name:			
Title:			
Date:			

A.3 Terms and Conditions

A.3.1 QSA Services

PCI SSC hereby approves QSA to perform, in accordance with this Agreement and the *QSA Validation Requirements* (defined below), onsite reviews of the member Financial Institutions of Members ("Financial Institutions"), issuers of Member payment cards ("Issuers"), merchants authorized to accept Member 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 "Subject"), to determine Subjects' compliance with the Payment Card Industry (PCI) Data Security Standard, as such Standard may be amended from time to time (the "PCI DSS", which is hereby incorporated into this Agreement), the current version of which is available for review on the PCI SSC web site at http://www.pcisecuritystandards.org (the "Website"), as part of the PCI Qualified Security Assessor Program ("QSA Program"). For purposes of this Agreement: (i) "Member" means a then current member of PCI SSC; (ii) the QSA reviews described above are referred to herein as "Assessments"; (iii) the Assessments, collectively with all related services provided by QSA to PCI SSC, Subjects or others in connection with this Agreement and the QSA Program, are referred to herein as the "Services"; (iv) "*QSA Validation Requirements*" means the most current version of (or successor document to) the *Payment Card Industry (PCI) Validation 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); and (v) "QSA Requirements" means the obligations and requirements of QSA pursuant to this Agreement, the *QSA Validation Requirements* and any other agreement, addendum, supplement or other document entered into between PCI SSC and QSA. The QSA Validation Requirements are hereby incorporated into this Agreement, and QSA acknowledges and agrees that it has reviewed the current version of the *QSA Validation 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, the *QSA Validation Requirements* and/or the Payment Card Industry (PCI) Data Security Standard Security Audit Procedures (the "PCI DSS Security Audit Procedures"), also available on the Website and incorporated herein by reference. QSA will incorporate all such changes into all Assessments initiated on or after the effective date of such changes. PCI SSC will not accept any Report of Compliance ("ROC") regarding an Assessment that is not conducted in accordance with the PCI DSS and PCI DSS Security Audit Procedures in effect at the initiation date of such Assessment.

A.3.2 Performance of Services

QSA warrants and represents that it will perform each Assessment in strict compliance with the PCI DSS Security Audit Procedures in effect as of the commencement date of such 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) the PCI DSS Security Audit Procedures were followed without deviation and (b) application of such procedures did not indicate any conditions of non-compliance with the PCI DSS other than those 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 *QSA Validation Requirements* supervises all aspects of each engagement to perform Services, including without limitation, being present onsite for the duration of the Assessment, reviewing the work product that supports the QSA's audit procedures, and ensuring adherence to PCI DSS Security Audit Procedures. Employees performing the following tasks must also be PCI SSC-qualified: scoping decisions, selection of systems and system components where sampling is employed (in accordance with the PCI DSS Security Audit Procedures), evaluation of compensating controls and/or final report production and/or review.

A.3.4 QSA Requirements

QSA agrees to adhere to all QSA Requirements, including without limitation, the requirements stated in this Agreement and all requirements applicable to Qualified Security Assessors (as defined in the *QSA Validation Requirements*) stated in the *QSA Validation Requirements*. Without limiting the foregoing, QSA agrees to comply with all requirements regarding background checks as set forth in the *QSA Validation Requirements* 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. Further, 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 the QSA Program is and shall be accurate and complete as of the date such information is provided. Additionally, QSA acknowledges that PCI SSC may from time to time require QSA to provide a representative to attend any mandatory training programs in connection with the QSA Program, which may require the payment of attendance and other fees.

A.4 Fees

QSA shall pay all fees (collectively, "Fees") as specified in Appendix D of the *QSA Validation Requirements* (the "Fee Schedule"). QSA acknowledges that PCI SSC may review and modify the fees specified in the Fee Schedule at any time and from time to time. Whenever a change in such Fees occurs, PCI SSC shall notify QSA in accordance with the terms of Section A10.1. Such change(s) will be effective thirty (30) days after the date of such notification. However, should QSA not agree with such change(s), QSA shall have the right to terminate this Agreement upon written notice to PCI SSC in accordance with the provisions of Section A10.1 at any time within such 30-day period.

A.4.1 Initial Fee

The applicable regional "Initial Processing Fee" specified in the Fee Schedule will be due and payable upon submission of QSA's executed version of this Agreement to PCI SSC for PCI SSC's approval for each region in which QSA has indicated it will perform Services. This Agreement will not be considered for PCI SSC approval until such Initial Fee payments have been received.

A.4.2 Initial Qualification Fee

The "Qualification Fee" specified in the Fee Schedule will be due and payable within thirty (30) days of notice to QSA that this Agreement has become effective; provided, however, that notwithstanding anything to the contrary in Section A5.1(a) of this Agreement, QSA will not be listed on the QSA List (defined in Section A5.1(a)) until the Qualification Fee is paid in full.

A.4.3 Annual Qualification Fees

Annual Qualification Fees for each Renewal Term (as defined in Section A9.1), as determined by PCI SSC, will be due and payable within thirty (30) days of notice that QSA has been re-qualified for such Renewal Term.

A.4.4 Training Fees

Fees in the amount established by PCI SSC for training of QSA personnel will be due and payable within thirty (30) days after a QSA training session has been scheduled, and in any event, prior to such training session. QSA personnel will not be admitted to training sessions until applicable fees have been paid in full.

A.4.5 Additional Fees

QSA acknowledges that additional Fees may apply, including without limitation, fees to cover administrative costs, re-listing on the QSA List, penalties and other costs, and that QSA will pay all such Fees as and when required.

A.4.6 Nonrefundable Fees

All Fees paid by QSA pursuant to this Agreement are nonrefundable (regardless of whether QSA's application is approved, QSA has been removed from the QSA List, this Agreement has been terminated or otherwise).

A.5 Advertising and Promotion; Intellectual Property

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

(a) So long as QSA is in Good Standing (as defined below) as a Qualified Security Assessor, PCI SSC may, at its sole discretion, display the identification of QSA, together with related information regarding QSA's status as a Qualified Security Assessor, in such publicly available list of Qualified Security Assessors as PCI SSC may maintain and/or distribute from time to time, whether on the Website or otherwise (the "QSA List"). 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. QSA shall be deemed to be in "Good Standing" as a Qualified Security Assessor as long as this Agreement is in full force and effect, QSA has been approved as a QSA 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, all provisions regarding compliance with the *QSA Validation Requirements* and payment). Without limiting the rights of PCI SSC set forth in the first sentence of this Section or in Section A9 below, 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 Qualified Security Assessor.

(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 mark without the prior written consent of PCI SSC in each instance. QSA shall not use any Member mark without the prior written consent of the owner of such mark in each instance. Without limitation of the foregoing, except as 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 or any Member regarding QSA, the Services or related products, or the functionality, quality or

performance of any aspect of any of the foregoing. QSA shall not: (i) make any false, misleading or incomplete statements regarding, or misrepresent the requirements of, PCI SSC, any Member or the PCI DSS, including without limitation, any requirement regarding the implementation of the PCI DSS or the application thereof to any Subject, or (ii) state or imply that the PCI DSS requires usage of QSA's products or services. Except with respect to (A) factual references to the QSA Program or to PCI Materials (defined in Section A7.3) that QSA includes from time to time in its contracts with Subjects and that are required or appropriate in order for QSA to accurately describe the nature of the Services QSA will provide pursuant to such contracts, (B) references permitted pursuant to Section A5.1(b) above and (C) references that PCI SSC has expressly authorized pursuant to a separate written agreement with QSA, QSA may not publish, disseminate or otherwise make available any statements, materials or products (in any form) that refer to the PCI DSS, the PCI Materials or any portion of the foregoing, QSA's listing on the QSA List, PCI SSC, any Member, or any PCI SSC or Member mark, unless such statement, material or product has been reviewed and approved in writing by PCI SSC and, to the extent applicable, such Member, prior to publication or other dissemination, in each instance. Prior review and/or approval of such statements, materials or products by PCI SSC and/or any applicable Member 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 of promotional or other materials or publicity in violation of Section A5 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. To the extent that QSA either uses or makes reference to any Member mark or makes any statement relating to any Member in violation of this Section A5.1, then such Member shall be an express third party beneficiary of this Section and shall have available to it all rights, whether at law or in equity, to enforce the provisions hereof on its own behalf and in its own right directly against QSA.

A.5.2 Uses of QSA Name and Designated Marks

QSA grants PCI SSC and each Member 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 Member shall be required to include any such reference in any materials or publicity regarding the QSA Program. QSA warrants and represents that it has authority to grant to PCI SSC and its Members 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 A5, 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, the PCI DSS Security Audit Procedures or any other PCI Materials.

A.5.4 Intellectual Property Rights

(a) All Intellectual Property Rights, title and interest in and to the QSA Program, the PCI DSS, the 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 A6, so long as QSA is in Good Standing, 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 agreement between PCI SSC and QSA. For purposes of this Agreement, "Intellectual Property Rights" shall mean all present and future patents, trade marks, service marks, design rights, database rights (whether registrable or unregistrable, and whether registered or not), applications for any of the foregoing, copyright, know-how, trade secrets, and all other industrial or intellectual property rights or obligations whether registrable or unregistrable and whether registered or not in any country.

(b) All right, title and interest in and to the Intellectual Property Rights in all materials generated by PCI SSC with respect to QSA are and at all times shall remain the property of PCI SSC. Subject to the provisions of Section A6, 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, all Intellectual Property Rights, title and interest in and to the materials 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 whatever form embodied (e.g., oral, written, electronic, on tape or disk, or by drawings or inspection of parts or equipment or otherwise), including without limitation, any and all other information that reasonably should be understood to be confidential. "Personal Information" means any and all Member payment card account numbers, Member transaction information, IP addresses or other 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 Member 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 and accountants 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 (B) the operation of such party's respective payment card data security compliance programs (if applicable) and (iii) not be disclosed to any third party except as expressly permitted in this Agreement or in writing by the Disclosing Party, and only if such third party is bound by confidentiality obligations applicable to such Confidential Information that are in form and substance similar to the provisions of this Section A6.

(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 Subject Data

To the extent any data or other information obtained by QSA relating to any Subject in the course of providing Services thereto may be subject to any confidentiality restrictions between QSA and such Subject, QSA must provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such Subject in writing) that (i) QSA may disclose each ROC, Attestation of Compliance and other related information to PCI SSC and/or its Members, as requested by the Subject, (ii) to the extent any Member obtains such information in accordance with the preceding clause A6.3(i), such Member may disclose (a) such information on an as needed basis to other Members and to such Members' respective Financial Institutions and Issuers and to relevant governmental, regulatory and law enforcement inspectors, regulators and agencies and (b) that such Member has received a ROC and other related information with respect to such Subject (identified by name) and whether the ROC was satisfactory, and (iii) QSA may disclose such information as necessary to comply with its obligations and requirements pursuant to Section A10.2(b) below. Accordingly, notwithstanding anything to the contrary in Section A6.2(a) above, to the extent requested by a Subject, PCI SSC may disclose Confidential Information relating to such Subject and obtained by PCI SSC in connection with this Agreement to Members in accordance with this Section A6.3, and such Members may in turn disclose such information to their respective member Financial Institutions and other Members. QSA hereby consents to such disclosure by PCI SSC and its Members. The confidentiality of ROCs and any other information provided to Members by QSA or any Subject 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 Subject (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 Subject 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 A9.1) 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 Member guidelines); (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 such cardholders. QSA will make available to PCI SSC and its Members, and will require in its agreements with Subjects that Subjects will make so available, such appropriate reviews and reports to monitor QSA's compliance with the foregoing commitments as PCI SSC or its Members 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, its Members or any Subject 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 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

Upon termination of this Agreement or upon demand, 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 that such requirement shall not apply to electronic copies made as part of QSA's standard computer back up practices. 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 A6.2 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 the QSA Program or use of 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 Subject that has engaged QSA to perform Services, including without limitation claims asserted by Subjects or Members; (iv) negligence or willful misconduct in connection with the QSA Program, this Agreement or its 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 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 any claim or liability arises solely from a defect in the PCI DSS or other materials provided by an Indemnified Party and used by QSA without modification.

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 there from or assume the defense of any Indemnified Party. In any event, PCI SSC and its Members will 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, PCI DSS SECURITY AUDIT PROCEDURES*, QSA PROGRAM, *QSA VALIDATION REQUIREMENTS*, WEBSITE AND ALL RELATED AND OTHER MATERIALS PROVIDED OR OTHERWISE MADE ACCESSIBLE IN CONNECTION WITH THE QSA 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, THE PCI MATERIALS OR ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR THE QSA PROGRAM. PCI SSC SPECIFICALLY DISCLAIMS, AND QSA EXPRESSLY WAIVES, ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO THIS AGREEMENT, THE PCI MATERIALS, ANY MATERIALS OR SERVICES PROVIDED UNDER OR IN CONNECTION WITH THIS AGREEMENT OR THE QSA 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 (WHETHER OR NOT PCI SSC HAS BEEN ADVISED, HAS REASON TO KNOW, OR IS OTHERWISE IN FACT AWARE OF ANY INFORMATION). THE FOREGOING DISCLAIMER IS MADE BY PCI SSC FOR ITSELF AND, WITH RESPECT TO EACH SUCH DISCLAIMER, ON BEHALF OF ITS LICENSORS AND MEMBERS.

(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 and 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 A5 OR A6, 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 A7.

(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 A4.

(f) Notwithstanding Section A7.3(d), PCI SSC shall not be liable vis-à-vis QSA for any other damage incurred by QSA under this Agreement, including but not limited to, loss of business, revenue, goodwill, anticipated savings or other commercial or economic loss of any kind arising in any way out of the use of the QSA 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 Qualified Security Assessors, as applicable, as set forth in Appendix E of the *QSA Validation Requirements*. QSA acknowledges and agrees that if it is a non-U.S. and non-European Union Qualified Security Assessor, 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 Qualified Security Assessors. QSA hereby represents and warrants that it meets all applicable insurance requirements as provided for in this Section A7.4 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 Qualified Security Assessors 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 the *QSA Validation 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 the *QSA Validation 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 A9, 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 re-qualification requirements for each Renewal Term.

A.9.2 Termination by QSA

QSA may terminate this Agreement at any time upon thirty (30) days' written notice to PCI SSC. PCI SSC will remove QSA from the QSA List as soon as practical after receipt of such notice, but in no event later than thirty days after such receipt.

A.9.3 Termination by PCI SSC

PCI SSC may terminate this Agreement effective as of the end of the then current Term by providing QSA with written notice of its intent not to renew this Agreement at least sixty (60) days prior to the end of the then current Term. Additionally, PCI SSC may terminate this Agreement: (i) with written notice upon 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; (iii) with fifteen (15) days' prior written notice following QSA's breach of any term or provision of this Agreement (including without limitation,

QSA's failure to comply with any requirement of the *QSA Validation Requirements*), provided such breach remains uncured when such 15-day period has elapsed; or (iv) in accordance with Section A9.5 below.

A.9.4 Effect of Termination

Upon any termination or expiration of this Agreement: (i) QSA will be removed from the QSA List; (ii) QSA shall immediately cease all advertising and promotion of its status as listed on the QSA List and all references to the PCI DSS and other PCI Materials; (iii) QSA shall immediately cease soliciting for any further Services and shall only complete Services contracted with Subjects prior to the notice of termination; (iv) QSA will deliver all outstanding ROCs within the time contracted with the Subject and shall remain responsible after termination for all of the obligations, representations and warranties hereunder with respect to all ROCs submitted prior to or after termination; (v) QSA shall return or destroy all PCI SSC and third party property and Confidential Information in accordance with the terms of Section A6 and (vi) PCI SSC may notify any of its Members and/or acquirers. The provisions of Sections A5.4, A6, A7, A9.4 and A10 of this Agreement 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 that QSA meets any condition for revocation of QSA qualification as established by PCI SSC from time to time, including without limitation, the conditions described in Section 5.3 of the *QSA Validation Requirements* (each such condition a "Violation"), PCI SSC may, effective immediately upon notice of such Violation to QSA, revoke QSA's qualification as a Qualified Security Assessor, subject to reinstatement pending a successful appeal in accordance with Section A9.5(b) below ("Revocation"). In the event of any Revocation: (i) QSA will be removed from the QSA List, (ii) QSA must comply with Sections A9.4(ii), A9.4(iii) and A9.4(iv) above in the manner otherwise required if this Agreement had been terminated, and (iii) QSA will have a period of thirty (30) days from the date QSA is given notice of the corresponding Violation to submit a written request for appeal to the PCI SSC General Manager. In the event QSA fails to submit such a request within the allotted 30-day period, PCI SSC will deliberate without an appeal and may terminate this Agreement effective immediately as of the end of such period.

(b) All Revocation appeal proceedings will be conducted in accordance with such procedures as PCI SSC may establish from time to time, PCI SSC will review all relevant evidence submitted by the QSA and each complainant (if any) in connection with therewith, and PCI SSC shall determine whether termination of QSA's qualification as a Qualified Security Assessor is warranted or, in the alternative, no action, or specified remedial actions shall be required of QSA. All determinations of PCI SSC regarding Revocation and any related appeals shall be final and binding upon QSA. If PCI SSC determines that termination is warranted, this Agreement shall terminate effective immediately upon such determination. If PCI SSC determines that no action is required of QSA, the Revocation shall be lifted and QSA shall be reinstated on the QSA List. If PCI SSC determines that remedial action is required, PCI SSC may establish a date by which such remedial actions must be completed, provided that the Revocation shall not be lifted, and QSA shall not be reinstated on the QSA List, unless and until such time as QSA has completed such remedial actions; provided 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 this Agreement effective immediately as of 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 personally, by overnight delivery upon written verification of receipt, by facsimile transmission upon electronic acknowledgment of receipt, or by certified or registered mail, return receipt requested, five (5) days after the date of mailing. Notices from PCI SSC to QSA shall be sent to the attention of the Principal 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 Officer 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 A10.1.

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 A6 of this Agreement, in order to assist in ensuring the reliability and accuracy of QSA's Assessments, within 15 days of any written request by PCI SSC or any Member (each a "Requesting Organization"), QSA hereby agrees to provide to such Requesting Organization such Assessment results (including ROCs) as such Requesting Organization may reasonably request with respect to (i) if the Requesting Organization is a Member, any Subject for which QSA has performed an Assessment and that is a Financial Institution of such Member, an Issuer of such Member, a Merchant authorized to accept such Member's payment cards, an Acquirer of accounts of Merchants authorized to accept such Member's payment cards or a Processor performing services for such Member's Financial Institutions, Issuers, Merchants or Acquirers or (ii) if the Requesting Organization is PCI SSC, any Subject for which QSA has performed an Assessment. Each agreement between QSA and its Subjects shall include such provisions as may be required to ensure that QSA has all necessary rights, licenses and other permissions necessary for QSA to comply with its obligations and requirements pursuant to this Agreement. Any failure of QSA to comply with this Section A10.2 shall be deemed breach of QSA's representations and warranties under this Agreement for purposes of Section A9.3, and upon any such failure, PCI SSC may remove QSA's name from the QSA List and/or terminate this Agreement in its sole discretion. Additionally, QSA agrees that all PA-QSA quality assurance procedures established by PCI SSC from time to time shall apply, including without limitation, those relating to probation, fines and penalties, and suspension or revocation.

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 documents and schedules incorporated herein by reference, is the exclusive statement of the agreement between the parties with respect to the QSA Program, which supersedes and merges all prior proposals, understandings and all other agreements, oral or written, between the parties with respect to such subject matter. 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. 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 or delegate its rights and obligations under this Agreement, including by subcontracting, without the prior written consent of PCI SSC, which consent PCI SSC may grant or withhold in its absolute discretion.

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, 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 a conflict between this Agreement and the *QSA Validation Requirements*, this Agreement shall control.

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. Qualified Security Assessor—New Application Process Checklist

This checklist has been provided as a tool to help you organize the PCI DSS Qualified Security Assessor company application information that must be submitted along with your completed/signed Agreement. This checklist is for new applications only; information required for the annual re-qualification process is detailed in Section 5.2. This checklist is a tool only—please review the detailed requirements in this document to ensure completeness of submitted information.

Note:

If your company is applying to become a ***Payment Application Qualified Security Assessor*** *(PA-QSA), additional requirements are documented in* QSA Validation Requirements—Supplement for Payment Application Qualified Security Assessors (PA-QSA). *The requirements contained therein must be met in addition to those documented in this Appendix B.*

Additionally, if your company is applying for a ***Principal-Associate QSA*** *relationship, additional requirements are documented in* QSA Validation Requirements—Supplement for Principal-Associate Qualified Security Assessors*. The requirements contained therein must be met in addition to those documented in this Appendix B.*

QSA Business Requirements

Requirement	Information/documentation Needed
Business Legitimacy	☐ Copy of business license ☐ Year of incorporation ☐ Location(s) of office(s) ☐ Written statement describing any past or present allegations or convictions of any fraudulent or criminal activity involving the security company and its principles
Independence	☐ Description of company's practices to maintain auditor independence. ☐ Company signature on the Qualified Security Assessor (QSA) Agreement
Insurance Coverage	☐ Company signature on the Qualified Security Assessor (QSA) Agreement ☐ Proof of insurance coverage statement that meets PCI SSC requirements (see Appendix E)
QSA Fee	☐ Initial processing fee, payable to PCI SSC.
QSA Agreement	☐ Qualified Security Assessor (QSA) Agreement signed by company officer

QSA Capability Requirements

Requirement	Information/documentation Needed
Company Services and Experience	☐ High level description of the security company's experience and knowledge with information security and payment system audit engagements ☐ High level description of the security company's relevant areas of specialization within information security ☐ Description of a dedicated security practice, including the total number of employees, the number of information security employees on staff, and the percentage of their time dedicated to performing security assessments ☐ Description of core business offerings ☐ A description of industries and size of companies with which the security company has worked ☐ List of languages supported by the security company ☐ Two client references from recent security engagements
Company Employee Skills and Experience	Provide the following for each employee to be qualified: ☐ Education (subject, degrees, institutions) ☐ Area(s) of expertise ☐ Years of working experience and responsibilities ☐ Years of working experience related to payment industry and role (if any) ☐ Résumé or CV ☐ Copy of CISSP – Certified Information System Security Professional certification and ID number, or ☐ Copy of CISA – Certified Information Systems Auditor certification and ID number, or ☐ Copy of CISM – Certified Information Security Manager and ID number, or ☐ A description of a minimum of five years' information security experience

QSA Administrative Requirements

Requirement	Information/documentation Needed	
Contact Person—Primary and Secondary	☐ Name ☐ Title ☐ Address	☐ Phone ☐ Fax ☐ E-mail
Background Checks	☐ A statement that QSA conducts background checks for each employee prior to submitting employee qualification requests to PCI SSC, and that each employee for which qualification materials have been submitted has successfully completed the background check in accordance with the QSA's policies and procedures ☐ Company signature on the Qualified Security Assessor (QSA) Agreement ☐ A description of the current QSA company personnel background check policies and procedures	
Adherence to PCI DSS Procedures and Attestation of Compliance	☐ Company signature on the Qualified Security Assessor (QSA) Agreement	
Quality Assurance	☐ A description of the quality assurance procedure that will be used for the ROC and signed “Attestation of Compliance” ☐ Company signature on the Qualified Security Assessor (QSA) Agreement	
Protection of Confidential and Sensitive Information	☐ A description of the security company’s sensitive data protection handling practices, including physical, electronic, and procedural safeguards. Includes requirements and processes used to ensure employee confidentiality of customer data ☐ Blank copy of confidentiality agreements required to be signed by employees ☐ Company signature on the Qualified Security Assessor (QSA) Agreement	
Evidence Retention	☐ Description of the security company’s evidence-retention policy and procedures ☐ Company signature on the Qualified Security Assessor (QSA) Agreement	

Appendix C. Sample QSA Feedback Form

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

Information collected from the Feedback Form will be held in strict confidence and used for the sole purpose of improving the quality of service provided by the QSA.

This form can be obtained directly from the QSA during the audit, or can be found online in a useable format at www.pcisecuritystandards.org. The client, not the QSA, should submit this form to PCI SSC. Please send this completed form to PCI SSC at: compliance@pcisecuritystandards.org.

QSA Feedback Form

	Client (merchant or service provider)			**Qualified Security Assessor Company (QSA)**	
Name					
Contact					
Title					
Telephone					
E-mail					
	Location of Assessment			**QSA employee who performed Assessment**	
Street				Name	
City				Title	
State/ Province				ID Number	
Country		Postal Code		Telephone	
				E-mail	

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

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

Question	Select One	Comments
1. During the initial PCI engagement, the QSA explained the objectives, timing, and review process, and address your questions and concerns.	***1-5***	
2. The QSA employee(s) understood your business and technical environment, as well as the cardholder data environment.	***1-5***	
3. The QSA employee(s) had sufficient security and technical skills to effectively perform this assessment.	***1-5***	
4. The QSA sufficiently understood the PCI Data Security Standard and the PCI DSS Security Audit Procedures.	***1-5***	
5. The QSA effectively minimized interruptions to operations and schedules.	***1-5***	
6. The QSA provided an accurate estimate for time and resources needed.	***1-5***	
7. The QSA provided an accurate estimate for report delivery.	***1-5***	
8. The QSA did not attempt to market their own products or services for your company to attain PCI compliance.	***1-5***	
9. The QSA did not imply that use of a specific brand of commercial product or service was necessary to achieve compliance.	***1-5***	
10. In situations where remediation was required, the QSA presented product and/or solution options that were not exclusive to their own product set.	***1-5***	
11. The QSA used secure transmission to send any confidential reports or data.	***1-5***	
12. The QSA demonstrated courtesy, professionalism, and a constructive and positive approach.	***1-5***	
13. There was sufficient opportunity for you to provide explanations and responses during the audit.	***1-5***	
14. During the review wrap-up, the QSA clearly communicated findings and expected next steps.	***1-5***	
15. If applicable, the QSA provided sufficient follow-up during your company's remediation efforts, until eventual compliance was achieved.	***1-5***	
Please provide any additional comments here about the QSA, your audit, or the PCI DSS documents.		

QSA Feedback Form for Payment Brands and Others

	QSA Client (merchant or service provider)	Qualified Security Assessor (QSA) Company
Company Name		
	Payment Brand Reviewer	**QSA employee who performed Assessment**
Name		
Title		Employee ID number:
Telephone		
E-mail		

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

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

Question	Select One	Comments
1. The QSA clearly understood how to notify your payment brand about compliance and non-compliance issues, and the status of merchants and service providers.	***1-5***	
2. The QSA Client had a positive and professional experience with the QSA.	***1-5***	
3. The QSA demonstrated sufficient understanding of the PCI Data Security Standard and the PCI DSS Security Audit Procedures.	***1-5***	
4. The QSA appropriately documented the results related to their findings.	***1-5***	
5. From your understanding, the QSA appropriately scoped the cardholder data environment.	***1-5***	
6. The QSA evaluated all compensating controls were appropriate and all risks relevant to the original requirements were addressed.	***1-5***	

Appendix D. QSA Fees

QSA fees are set according to location. QSAs are qualified to serve specific markets and pay fees according to those markets of service. QSAs may service multiple markets. If so, they pay separate fees for each market served.

All fee checks should be made payable to PCI SSC and mailed with the completed QSA application package. See Section 1.6 of this document for the mailing address.

Additional fees apply to QSAs who qualify as PA-QSAs or Principal or Associate QSAs.

The most current program fees are available at https://www.pcisecuritystandards.org/fees

Appendix E. Insurance Coverage

This is the expected insurance clause and coverage for all QSA companies, except for in those locations where such insurance coverage is not available or provided. The limits shown in this appendix may be written in other currencies, but should be the equivalent of the limits in US dollars shown here.

Note:
For QSAs to conduct work outside their home countries, the following is an additional insurance coverage requirement: The insurance provider must respond to claims on a global basis (and particularly respond to claims brought in the U.S. if applicable.

Note:
Most insurance is not automatically written to respond to claims outside of the country and many specifically exclude claims from the U.S.

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

Prior to the commencement of the Services under this agreement, the 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."
- 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 employee dishonesty, robbery, fraud, theft, forgery, alteration, mysterious disappearance and destruction. The minimum limit shall be $1,000,000 each loss and annual aggregate.
- TECHNOLOGY ERRORS & OMISSIONS, CYBER-RISK and PRIVACY LIABILITY INSURANCE covering liabilities for financial loss resulting or arising from acts, errors or omissions in rendering computer or information technology Services, or from data damage/destruction/corruption, including without limitation, failure to protect privacy, unauthorized access, unauthorized use, virus transmission, denial of service and loss of income from network security failures in connection with the Services provided under this agreement with a minimum limit of two million dollars ($2,000,000) each claim and annual aggregate.

If any of the above insurance is written on a claims-made basis, then Security Assessor shall maintain such insurance for five (5) years after the termination of this agreement.

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.