Payment Card Industry (PCI)
Data Security Standard

QSA Validation Requirements

Supplement for Payment Application Qualified Security Assessors (PA-QSA)

Version 1.2
April 2008

Table of Contents

1 Introduction

In addition to creating the PCI DSS, members of the payment card industry (“PCI”) have 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 applications to facilitate and not prevent their customers’ PCI DSS compliance. The PA-DSS is maintained by PCI SSC and is available through the Website (defined below) as part of the *Payment Application Data Security Standard and Audit Procedures* (*“PA-DSS Security Audit Procedures”*).

This *Supplement for Payment Application Qualified Security Assessors (PA-QSA)* (the "PA-QSA Supplement") supplements the *QSA Validation Requirements* (defined below) for each QSA company that intends to qualify as a Payment Application Qualified Security Assessor (defined below), and describes the minimum capability requirements, laboratory requirements, and related documentation that a QSA must satisfy and provide to PCI SSC in order to qualify to perform PA-DSS Assessments (defined below).

1.1 Terminology

Note that throughout this PA-QSA Supplement, 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 additional PA-QSA Requirements (as defined in the PA-QSA Addendum).

"PA-QSA Addendum" refers to the *Addendum to Qualified Security Assessor (QSA) Agreement for Payment Application QSAs* attached as Appendix A to the *PA-QSA Supplement*.

"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.

“PA-QSA employee” refers to an individual employed by a PA-QSA who has satisfied and continues to satisfy all PA-QSA Requirements applicable to employees of PA-QSAs who will conduct PA-QSA Assessments, as described in further detail herein.

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

"QSA Validation Requirements" refers to the then current version of the *Payment Card Industry (PCI) Data Security Standard Validation Requirements For Qualified Security Assessors (QSA)* as amended from time to time and made available on the PCI SSC web site at http://www.pcisecuritystandards.org (the "Website").

All capitalized terms used in this PA-QSA Supplement without definition shall have the meanings specified in the *QSA Validation Requirements* or the *QSA Agreement*, as applicable.

1.2 Goal

In order to qualify and remain in good standing as a PA-QSA, a QSA must meet or exceed, and then continue to satisfy, all of the requirements set forth in this PA-QSA Supplement, as well as the general requirements for all QSAs as set forth in the *QSA Validation Requirements* and the *QSA Agreement* (all such general QSA requirements, collectively, "QSA Requirements"), and execute the *PA-QSA Addendum* in the form attached hereto as Appendix A.

Together, the QSA Requirements and the PA-QSA Requirements are intended to serve as a validation baseline for PA-QSAs, and provide a transparent process for PA-QSA qualification and re-qualification across the payment industry.

1.3 Qualification Process Overview

The PA-QSA qualification process first involves the qualification of the QSA company itself as a PA-QSA company, followed by qualification of the QSA company's employee(s) who will be performing and/or managing the PA-DSS assessments.

Companies that qualify as PA-QSAs will be identified as such on the Website in accordance with the *PA-QSA Addendum* for a period of one (1) year from the date of such qualification. If a company is not so identified, its work product as a PA-QSA is not recognized by PCI SSC. All PA-QSAs must re-qualify annually.

To initiate the PA-QSA qualification process, the QSA must sign the *PA-QSA Addendum* in unmodified form and submit it to PCI SSC as part of its completed PA-QSA application package.

1.4 Document Structure

The PA-QSA Supplement is structured in five sections as follows.

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

Section 2: PA-QSA Business Requirements covers minimum additional business requirements that must be demonstrated to PCI SSC by the PA-QSA. This section outlines information and items that must be provided to prove business stability, independence, and insurance coverage. PA-QSA fees and agreements are also covered.

Note:

All requirements set forth in QSA Validation Requirements *must be met by organizations wishing to qualify as PA-QSAs.*

Section 3: PA-QSA Capability Requirements reviews the information and documentation necessary to demonstrate the PA-QSA's service expertise, as well as that of its employees.

Section 4: PA-QSA Administrative Requirements focuses on the logistics of doing business as a PA-QSA, including adherence to PCI DSS procedures, quality assurance, and protection of confidential and sensitive information.

Appendices: The appendices to the PA-QSA Supplement include the PA-QSA Addendum and several helpful checklists, feedback forms, and detailed fee requirements.

1.5 Related Publications

The PA-QSA Supplement is intended for use with the current version of the *QSA Validation Requirements,* which should be used in conjunction with the current versions of the following other PCI SSC publications, each as available through the Website:

- *PCI DSS*,
- *QSA Validation Requirements,*
- *Payment Card Industry (PCI) Data Security Standard Security Audit Procedures*, and
- *PA-DSS Security Audit Procedures*.

1.6 PA-QSA Application Process

In addition to outlining the requirements that a PA-QSA must meet to perform PA-DSS Assessments, this PA-QSA Supplement describes the information that must be provided to PCI SSC as part of the PA-QSA 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 C: PA-QSA Application Process Checklist. All application materials and the signed PA-QSA Addendum must be submitted in English. The PA-QSA Addendum is binding in English even if the PA-QSA Addendum was translated and reviewed in another language. All other documentation provided by the PA-QSA in a language other than English must be accompanied by a certified English translation (examples include business licenses and insurance certificates).

All PA-QSA application packages must include a signed PA-QSA Addendum 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.

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 PA-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 Payment Application QSA Business Requirements

2.1 *Business Legitimacy*

PA-QSAs must meet all business legitimacy requirements as set forth in the *QSA Validation Requirements.*

2.2 *Independence*

PA-QSAs must meet all independence requirements as set forth in the *QSA Validation Requirements.*

2.3 *Insurance Coverage*

PA-QSAs must meet all insurance coverage requirements as set forth in the *QSA Validation Requirements.*

2.4 *PA-QSA Fees*

2.4.1 Requirement

For PA-QSA qualification, each PA-QSA applicant must provide to PCI SSC a processing fee per geographic region or country in which the PA-QSA applicant intends to perform PA-DSS Assessments (see Appendix E: PA-QSA Fees). These fees are credited toward the qualification fee (see below) if a company is qualified as a PA-QSA. The initial processing fee check should be made payable to PCI SSC and mailed with the completed PA-QSA application package. See Section 1.6 of the PA-QSA Supplement for the mailing address. Once a company is approved for qualification as a PA-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 E.

Note:

All fees are subject to change.

- An annual PA-QSA re-qualification fee for subsequent years, also summarized by location in Appendix E*.*
- A training fee for each PA-QSA employee to be qualified, for training sponsored by PCI SSC. This is an annual fee. See Appendix E.

2.5 *PA-QSA Agreements*

2.5.1 Requirement

As described in further detail in the *QSA Validation Requirements*, each QSA must have executed and submitted the QSA Agreement to qualify as a QSA.

Once qualified as a QSA, there are various other agreements and/or addenda a QSA must execute and submit to PCI SSC, depending on the QSA programs in which the QSA wishes to participate. Please refer to the *QSA Validation Requirements* for information about other agreements that may be needed, depending on what QSA programs your company is applying for.

In order to participate in the PA-QSA program, PCI SSC requires that the PA-QSA Addendum be signed in unmodified form by a duly authorized officer of the QSA and then submitted by mail to PCI SSC with the completed PA-QSA application package.

The PA-QSA Addendum requires that all PA-QSAs comply with this PA-QSA Supplement and all additional PA-QSA Requirements.

3 Payment Application QSA Capability Requirements

3.1 PA-QSA Company – Services and Experience

3.1.1 Requirements

- The PA-QSA must fulfill all QSA Requirements, as defined in the QSA Agreement.
- The PA-QSA must fulfill all PA-QSA Requirements and comply with all terms and provisions of the PA-QSA's QSA Agreement, PA-QSA Addendum and any other agreements executed with PCI SSC.
- The PA-QSA must have performed at least two PCI DSS assessments.
- The PA-QSA must possess substantial application security knowledge and experience performing application and/or code reviews, as determined in the sole discretion of PCI SSC.
- The PA-QSA must have demonstrated competence in cryptographic techniques, to include cryptographic algorithms, key management and rotation processes, and secure key storage, as determined in the sole discretion of PCI SSC.
- The PA-QSA must have demonstrated competence in using penetration-testing methodologies, to include use of forensic tools/methods, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes.

3.1.2 Provisions

The following information must be provided to PCI SSC, in addition to the QSA company information required in Section 3.1 of this PA-QSA Supplement:

- For the PA-QSA, a description of both relevant experience with application security and application and code reviews, preferably related to payment applications and including a description of methodology used to perform such reviews equal to at least one year or three separate application security engagements.
- A description of dates and clients for two previous PCI DSS assessments performed by the PA-QSA.
- Description of the PA-QSA's relevant areas of specialization within application security, and code reviews (for example, use of OWASP or other secure coding guidelines, web vulnerability assessment, application penetration testing, or designing or implementing cryptography systems), demonstrating at least one area of specialization.
- Description of experience with cryptographic techniques, including cryptographic algorithms, key management and rotation processes, and secure key storage, demonstrating at least one area of specialization.
- Description of experience using penetration testing methodologies, to include use of forensic tools/methods, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes.

- Two client references from application security engagements within the last 12 months.

3.2 *PA-QSA Staff - Skills and Experience*

Each PA-QSA employee performing or managing PA-DSS Assessments must be qualified by PCI SSC as *both* a QSA and a PA-QSA employee; only PA-QSA employees qualified by PCI SSC can conduct PA-DSS Assessments. PA-QSA employees are responsible for the following:

- Performing the PA-DSS Assessments.
- Verifying that the laboratory used to test the client's application meets requirements defined in Appendix B: Confirmation of PA-QSA's General Testing Laboratory Capabilities.
- Verifying the work product addresses all audit procedure steps and supports the compliance status of the application.
- Strictly following the *PA-DSS Security Audit Procedures*.
- Producing the final report.

3.2.1 Requirements

The PA-QSA employee(s) performing or managing PA-DSS assessments must also:

- Be a QSA employee and fulfill all requirements specified in Section 2.2 of the *QSA Validation Requirements*.
- Have performed at least two PCI DSS Assessments.
- Have substantial application security knowledge and experience conducting application and code reviews, and/or demonstrated competence in cryptographic techniques, for example experience coding per OWASP or other secure coding guidelines, performing web vulnerability assessments, performing application penetration testing, experience using penetration testing methodologies, to include use of forensic tools/methods, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes, and/or experience in cryptographic techniques such as cryptographic algorithms, key management and rotation processes, and secure key storage, as determined in the sole discretion of PCI SSC.
- Be knowledgeable about the *PA-DSS Security Audit Procedures*, as determined in the sole discretion of PCI SSC.
- 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 PA-QSA employee fails to pass any exam in connection with such training, the PA-QSA employee must no longer lead or manage a PA-DSS assessment until successfully passing the exam on a future attempt.
- Be employees of the PA-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 PA-QSA or any reference to another company in the *Report of Validation* or attestation documents while performing work on behalf of the PA-QSA.

3.2.2 Provisions

The following information must be provided to PCI SSC for each individual to be qualified as a PA-QSA, in addition to the QSA Staff information required in Section 2.2:

- A description of dates and clients for two previous PCI DSS assessments performed by the potential PA-QSA individual.
- Description of area(s) of expertise within application security, code reviews and cryptography (for example, use of OWASP or other secure coding guidelines, web vulnerability assessment, application penetration testing, experience using penetration testing methodologies, to include use of forensic tools/methods, ability to exploit OWASP vulnerabilities, and ability to execute arbitrary code to test processes, and/or designing or implementing cryptography systems) with at least one year (total) in three separate areas.

3.3 PA-QSA Testing Laboratory

3.3.1 Requirement

The PA-QSA must complete Appendix B as part of the PA-QSA application process, to confirm that the PA-QSA:

a) Maintains a testing laboratory meeting all requirements specified in Appendix B.

b) Has documented processes to verify that a software vendor's laboratory meets the requirements specified in Appendix B, whenever it is necessary to use a software vendor's testing laboratory rather than the PA-QSA's testing laboratory.

In addition, PA-QSA must review and confirm testing laboratory configurations as part of each PA-DSS review and complete *PA-DSS Security Audit Procedures* Appendix B: Confirmation of Testing Laboratory Configuration Specific to the PA-DSS Assessment.

3.3.2 Provisions

- Description of documented processes used to verify that a vendor's laboratory meets the requirements specified in Appendix B, whenever it is necessary to use a vendor's testing laboratory rather than the PA-QSA's testing laboratory.
- Completed Appendix B.

3.4 Mock Assessment

3.4.1 Requirement

PCI SSC reserves the right to require successful completion of a mock assessment annually, after at least one employee has successfully completed PA-QSA training and passed the examination, or to use a mock assessment as a tool to validate the PA-QSA's quality assurance program.

4 Payment Application QSA Administrative Requirements

4.1 *Contact Person*

4.1.1 Requirement

The PA-QSA must provide PCI SSC with primary and secondary contacts (and related contact information) for both:

- Persons responsible for PA-DSS Assessments.
- Persons responsible for oversight of quality assurance of PA-DSS Assessments.

4.1.2 Provisions

The following contact information must be provided to PCI SSC, for each primary and secondary contact mentioned above:

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

4.2 *Background Checks*

- PA-QSAs must meet all background check requirements as specified in the *QSA Validation Requirements.*

4.3 *Adherence to PCI Procedures*

4.3.1 Requirements

- For each PA-DSS Assessment, the resulting PA-QSA report must follow the PA-DSS Report on Validation ("PA-DSS ROV") template and instructions, as outlined in the *PA-DSS Security Audit Procedures*.

- The PA-QSA must prepare each PA-DSS ROV based on evidence obtained by following the *PA-DSS Security Audit Procedures*.

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

4.4 *Quality Assurance*

4.4.1 Requirements

- The PA-QSA must fulfill all QSA requirements for quality assurance as defined in Section 4.4 of the *QSA Validation Requirements*.
- The PA-QSA must have implemented a quality assurance program that includes PA-DSS reports, as documented in their company's quality assurance program manual (as described in Subsection 4.4.2 of the PA-QSA Supplement as well as subsection 4.4.2 of the *QSA Validation Requirements*).
- The PA-QSA must provide a PA-QSA Feedback Form to their client at the completion of the audit. See Appendix D: Sample PA-QSA Feedback Form.
- The PA-QSA must adhere to all PA-QSA quality assurance requirements mandated by PCI SSC, including but not limited to the following:
    - Report review processes
    - Warning letters
    - Probation
    - Fines and penalties
    - Suspension and any reinstatement processes
- PCI SSC reserves the right to conduct site visits and audit the PA-QSA at the discretion of the PCI SSC.
- Upon request, the PA-QSA must provide the quality assurance manual to PCI SSC.

4.4.2 Provisions

The PA-QSA must provide the following to PCI SSC:

- The description of the responsibilities of the PA-DSS quality assurance person that lists, at a minimum, the following responsibilities:
    - Oversight of quality assurance for all PA-QSA reports.
    - Review and approval of all PA-DSS reports prior to submission to PCI SSC.
    - Sole responsibility for submitting PA-DSS reports to PCI SSC.
    - A description of the contents of the PA-QSA quality assurance manual to confirm the procedures include PA-DSS audit and report review processes.
    - A requirement that all PA-QSA employees must adhere to the *PA-DSS Security Audit Procedures*.

4.5 Protection of Confidential and Sensitive Information

PA-QSAs must adhere to all requirements to protect sensitive and confidential information, as required by PCI SSC.

4.6 Evidence Retention

PA-QSAs must meet all evidence retention requirements as set forth in the *QSA Validation Requirements*.

4.7 PA-QSA Recognition of Client's Validation Status

4.7.1 Requirements

The PA-QSA must not provide any formal recognition of PA-DSS validation status to a client until PCI SSC has notified the PA-QSA and vendor as follows:

- PCI SSC has issued an acceptance letter to both PA-QSA and software vendor; and
- PCI SSC has included the software vendor and specific application on the published list of validated payment applications.

4.7.2 Provisions

The PA-QSA must provide the following:

- A statement that the PA-QSA will not recognize a client's validation status until PCI SSC has notified PA-QSA and vendor via an acceptance letter and inclusion of the application on the list of validated applications.

5 PA-QSA Initial Qualification and Annual Re-qualification

For information about what happens after initial qualification and items related to the annual PA-QSA re-qualification, please refer to Section 5 of the *QSA Validation Requirements*, which includes: (1) the QSA List, (2) annual maintenance of the QSA qualification, and (3) revocation, if necessary, of a QSA's qualification.

Appendix A. Addendum to Qualified Security Assessor (QSA) Agreement for Payment Application QSAs

A.1 Introduction

This Addendum to Qualified Security Assessor (QSA) Agreement for Payment Application QSAs (the "Addendum") is entered into by and between PCI Security Standards Council, LLC ("PCI SSC") and the undersigned Payment Application QSA Applicant ("QSA") as of the date of PCI SSC's approval hereof (the "Addendum Effective Date"), as evidenced by its signature below, for purposes of adding and modifying certain terms of the Qualified Security Assessor (QSA) Agreement between PCI SSC and QSA dated as of the QSA Agreement Date below, as in effect as of the Addendum Effective Date (the "Agreement"). Capitalized terms appearing in this Addendum shall have the meanings ascribed to them herein for all purposes of this Addendum and the Agreement, and if not defined in this Addendum, shall have the meanings ascribed to them in the Agreement.

In consideration of the mutual covenants herein set forth, the sufficiency of which is acknowledged, QSA and PCI SSC agree as follows.

A.2 General Information

Applicant			
Applicant Name:			
Company Name:			
QSA Agreement Date:			
Location/Address:			
State/Province:	Country:	Postal Code:	
Regions Applying For (see Appendix D):			
Applicant's Signature			
Applicant's Officer Signature ↑		*Date ↑*	
Applicant Officer Name:	Title:		

For PCI SSC Use Only:		
Application Date:		
Application Approved:		
PCI SSC Officer Signature ↑		
PCI SSC Officer Name:	Title:	

A.3 Terms and Conditions

A.3.1 Definitions

A.1.1.1 Terms in Addendum

For purposes of this Addendum, the following terms shall have the following meanings:

(a) "PA-DSS" means the PCI DSS Payment Application Data Security Standard, as such Standard may be amended from time to time in PCI SSC's discretion, the current version of which is available for review on the Website. The PA-DSS is hereby incorporated into this Addendum.

(b) "PA-DSS Assessments" means QSA's reviews of Payment Applications in accordance with the PA-QSA Requirements and the PA-DSS as part of the PA QSA Program.

(c) "PA-DSS Security Audit Procedures" means the Payment Application Data Security Standard and Audit Procedures, as amended from time to time in PCI SSC's discretion, the current version of which is available for review on the Website.

(d) "Payment Application Qualified Security Assessor" or "PA-QSA" means a QSA company in Good Standing that performs PA-DSS Assessments of 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 PA-QSA Requirements.

(e) "Payment Applications" means software applications that store, process, or transmit payment cardholder data as part of payment authorization or settlement.

(f) "PA-QSA Program" means PCI SSC's Payment Application Qualified Security Assessor Program.

(g) "PA-QSA Requirements" means all obligations and requirements of QSA pursuant to this Addendum, the PA-QSA Supplement and any other agreement, addendum, supplement or other document entered into between PCI SSC and QSA in connection with the PA-QSA Program.

(h) "PA-QSA Services" means PA-DSS Assessments and all related services provided by QSA to PCI SSC and Vendors in connection with this Addendum and the PA-QSA Program.

(i) "PA-QSA Supplement" means the then current version of the Supplement for Payment Application Qualified Security Assessors (PA-QSA), as amended from time to time in PCI SSC's discretion, the current version of which is available for review on the Website.

(j) "Vendors" means software vendors who develop, and then sell, distribute, or license Payment Applications to third parties.

A.1.1.2 Terms in Agreement

While this Addendum is in effect, the following terms appearing in the Agreement are hereby amended as follows for purposes of the Agreement:

(a) The term "Services" shall include the PA-QSA Services.

(b) The term "QSA Requirements" shall include the PA-QSA Requirements.

(c) The term “Subjects” shall include Vendors.

(d) The terms "Report of Compliance", "ROC" and "Attestation of Compliance" shall, where applicable, include the terms "Report of Validation", "ROV" and "Attestation of Validation", respectively, as those terms are used in the PA-QSA Supplement.

A.3.2 PA QSA Services

Subject to the terms and conditions of the Agreement, PCI SSC hereby approves QSA to conduct PA-DSS Assessments of Payment Applications for Vendors in order to validate compliance of such Payment Applications with the PA-DSS. Notwithstanding the foregoing, QSA agrees that it shall not recognize any Vendor's validation status until PCI SSC has notified QSA and Vendor via an acceptance letter and inclusion of the Vendor's Payment Application on PCI SSC's published list of validated Payment Applications.

QSA agrees to monitor the Website at least weekly for changes to the PA-DSS, the PA-QSA Supplement and/or the PA-DSS Security Audit Procedures. QSA will incorporate all such changes into all PA-DSS Assessments initiated on or after the effective date of such changes. QSA acknowledges that PCI SSC will not accept any Report of Validation ("ROV") regarding a PA-DSS Assessment that is not conducted in accordance with the PA-DSS and PA-DSS Security Audit Procedures in effect at the initiation date of such PA-DSS Assessment.

A.3.3 Performance of PA-QSA Services

(a) QSA warrants and represents that it will perform each PA-DSS Assessment in strict compliance with the PA-DSS Security Audit Procedures in effect as of the commencement date of such PA-DSS Assessment. Without limiting the foregoing, QSA will include in each ROV an Attestation of Validation in the form available through the Website signed by a duly authorized officer of QSA, in which QSA certifies without qualification that (a) the PA-DSS Security Audit Procedures were followed without deviation and (b) application of such procedures did not indicate any conditions of non-compliance with the PA-DSS other than those noted in the ROV.

(b) QSA acknowledges and agrees that PCI SSC, in an effort to maintain the integrity of the QSA Program, may request from time to time demonstrated adherence to the requirements set forth in the PA-QSA Supplement. Each such request shall be in writing and QSA shall respond thereto with documented evidence of such adherence in form and substance acceptable to PCI SSC no later than three (3) weeks from QSA's receipt of such written request.

A.3.4 PA-QSA Service Staffing

QSA shall ensure that a PA-QSA employee that is fully qualified in accordance with all applicable provisions of the PA-QSA Supplement supervises all aspects of each engagement to perform PA-QSA Services in accordance with the PA-QSA Supplement and the PA-DSS Security Audit Procedures.

A.3.5 PA-QSA Requirements

QSA agrees to adhere to all PA-QSA Requirements, and in connection therewith, to comply with all requirements and make all provisions as set forth in the PA-QSA Supplement, including without limitation, all Business Requirements, Capability Requirements, and Administrative Requirements, as set forth in Sections 2, 3 and 4 of the Supplement, and all requirements with respect to PA-QSA employees (as defined in the Supplement). Further, QSA warrants that, to the best of QSA's ability to determine, all information provided to PCI SSC in connection with this Addendum and QSA's participation in the PA-QSA Program is and shall be accurate and complete as of the date such information is provided. 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 PA-QSA Program, which may require the payment of attendance and other fees.

A.4 PA-QSA Fees

QSA shall pay all fees (collectively, "PA-QSA Fees") as specified in Appendix E of the PA-QSA Supplement (the "PA-QSA Fee Schedule"), in accordance with Section 2.4 of the PA-QSA Supplement. QSA acknowledges that PCI SSC may review and modify such fees at any time and from time to time, provided that PCI SSC shall notify QSA of such change and such change will be effective thirty (30) days after the date of such notification. Should QSA not agree with any such change, QSA may terminate this Addendum upon written notice to PCI SSC at any time within such 30-day period.

A.5 QSA List; Promotional References; Restrictions

(a) So long as QSA is in PA-QSA Good Standing (as defined below), PCI SSC may, at its sole discretion, identify QSA as a PA-QSA on the QSA List or in such other publicly available list of PA-QSAs as PCI SSC may maintain and/or distribute from time to time, whether on the Website or otherwise (for purposes of the Agreement, such other list (if any) shall be deemed to be part of the QSA List). QSA shall be deemed to be in "PA-QSA Good Standing" as long as QSA is in Good Standing as a Qualified Security Assessor, this Addendum is in full force and effect, QSA has been approved as a PA-QSA and such approval has not been revoked and QSA is in compliance with all PA-QSA Requirements.

(b) So long as QSA is in PA-QSA Good Standing and is identified in the QSA List as a PA-QSA, Section A5.1(b) of the Agreement is hereby amended to the extent necessary to permit QSA to make reference to such PA-QSA listing in advertising or promoting its PA-QSA Services, in addition to the references already permitted by Section A5.1(b) of the Agreement.

(c) QSA shall not: (i) make any false, misleading or incomplete statements regarding, or misrepresent the requirements of the PA-DSS, including without limitation, any requirement regarding the implementation of the PCI DSS or the application thereof to any Vendor, or (ii) state or imply that the PA-DSS requires usage of QSA's products or services.

A.6 Vendor Data; Quality Assurance

(a) To the extent any data or other information obtained by QSA relating to any Vendor in the course of providing PA-QSA Services thereto may be subject to any confidentiality restrictions between QSA and such Vendor, QSA must provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such Vendor in writing) that (i) QSA may disclose each ROV, Attestation of Validation and other related information to PCI SSC and/or its Members, as requested by the Vendor, (ii) to the extent any Member obtains such information in accordance with the preceding clause A6(a)(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 ROV and other related information with respect to such Vendor (identified by name) and whether the ROV was satisfactory, and (iii) QSA may disclose such information as necessary to comply with its obligations and requirements pursuant to Section A10.2(b) of the Agreement. Accordingly, notwithstanding anything to the contrary in Section A6.2(a) of the Agreement, to the extent requested by a Vendor, PCI SSC may disclose Confidential Information relating to such Vendor and obtained by PCI SSC in connection with this Addendum to Members in accordance with this Section A6(a), 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 ROVs and any other information provided to Members by QSA or any Vendor is outside the scope of the 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 Vendor (as applicable), on the other hand.

(b) Notwithstanding anything to the contrary in Section A6 of the Agreement or in this Addendum, in order to assist in ensuring the reliability and accuracy of PA-DSS 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 with such PA-DSS Assessment results (including ROVs) as such Requesting Organization may reasonably request with respect to (i) if the Requesting Organization is a Member, any Vendor for which QSA has performed a PA-DSS Assessment to the extent such Vendor has provided a Payment Application to 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 Vendor for which QSA has performed a PA-DSS Assessment. Each agreement between QSA and its Vendors 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 A6(b) shall be deemed breach of QSA's representations and warranties under the Agreement for purposes of Section A9.3 thereof, and upon any such failure, PCI SSC may remove QSA's name from the QSA List and/or terminate the 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.7 Term and Termination

A.7.1 Term

This Addendum shall become effective as of the Addendum Effective Date and, unless earlier terminated in accordance with this Section A7, shall continue for an initial term of one (1) year, and thereafter shall renew for additional subsequent terms of one year, subject to

QSA's successful completion of qualification and re-qualification requirements for each such one-year term (each a "Contract Year"). This Addendum shall immediately terminate upon termination of the Agreement.

A.7.2 Termination by QSA

QSA may terminate this Addendum upon thirty (30) days' written notice to PCI SSC.

A.7.3 Termination by PCI SSC

PCI SSC may terminate this Addendum effective as of the end of any Contract Year by providing QSA with written notice of its intent not to renew this Addendum at least sixty (60) days prior to the end of the then current Contract Year. Additionally, PCI SSC may immediately terminate this Addendum (i) with written notice upon QSA's breach of any representation or warranty under this Addendum; or (ii) with fifteen (15) days' prior written notice following QSA's breach of any term or provision of this Addendum (including without limitation, QSA's failure to comply with any requirement of the PA-QSA Supplement), provided such breach remains uncured when such 15-day period has elapsed.

A.7.4 Effect of Termination

Upon any termination or expiration of this Addendum: (i) QSA will no longer be identified as a PA-QSA on the QSA List; (ii) QSA shall immediately cease all advertising and promotion of its status as a PA-QSA and all references to the PA-DSS and other PCI Materials; (iii) QSA shall immediately cease soliciting for any further PA-QSA Services and shall only complete PA-QSA Services contracted with Vendors prior to the notice of termination; (iv) QSA will deliver all outstanding ROVs within the time contracted with the Vendor and shall remain responsible after termination for all of the obligations, representations and warranties hereunder with respect to all ROVs submitted prior to or after termination; (v) QSA shall return or destroy, in accordance with the terms of Section A6 of the Agreement, all PCI SSC and third party property and Confidential Information obtained in connection with this Addendum and the performance of PA-QSA Services; and (vi) PCI SSC may notify any of its Members and/or acquirers. The provisions of this Section A7.4 shall survive the expiration or termination of this Addendum for any or no reason.

A.8 General Terms

While this Addendum is in effect, the terms and conditions set forth herein shall be deemed incorporated into and a part of the Agreement. This Addendum 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. Except as expressly modified by this Addendum, the Agreement shall remain in full force and effect in accordance with its terms.

Appendix B. Confirmation of PA-QSA's General Testing Laboratory Capabilities

The PA-QSA Testing Laboratory must have the following capabilities, and the PA-QSA must confirm the testing laboratory capabilities via this checklist, which must be completed and submitted by the PA-QSA along with all other required documentation in the PA-QSA's application package:

Requirement		Confirmation of General Lab Capabilities
1	**Install software per vendor's installation instructions provided to merchant.** The common installation of the payment application product on all platforms listed in the PA-DSS report, installed per the vendor's installation manual provided to merchant.	□
2	**Install and test all software versions listed in PA-DSS report.**	□
	▪ Install all common implementations (including region/country specific versions) of the payment application to be tested.	□
	▪ Test all application versions and platforms.	□
	▪ Test all application functionalities.	□
3	**Install, and verify application functions with, all PCI DSS required security devices.**	□
	▪ Implementation of all security devices required by PCI DSS, including: firewalls, Network Address Translators (NAT), Port Address Translators (PAT), anti-virus software and encryption.	□
	▪ Test application(s) with all security devices required by PCI DSS.	□
4	**Install and/or configure, and verify application functions with, all PCI DSS required settings.**	□
	▪ Implementation of PCI DSS compliant system settings, patches, etc. for operating systems, system software, and applications used by application.	□
	▪ Test application(s) with of PCI DSS compliant system settings, etc.	□
5	**Simulate real-world use of the application.**	□
	▪ The laboratory simulates the "real world" use of the payment application, including all systems and applications where the payment application is implemented. For example, a standard implementation of a payment application might include a client/server environment within a retail storefront with a POS machine, and back office or corporate network. The laboratory must simulate the total implementation.	□
	▪ Only test card numbers are used for the simulation/testing—live PANs are not used for testing. These test cards can usually be obtained from the vendor or a processor or acquirer.	□

Requirement		Confirmation of General Lab Capabilities
	▪ The application's authorization and/or settlement functions were run and output examined per Item 6 below.	□
	▪ Map and determine all output produced by the application in every possible scenario, whether temporary, permanent, error processing, debugging mode, log files, etc.	□
	▪ Simulate and validate all functions of the software, to include generation of all error conditions and log entries using both simulated "live" data and invalid data.	□
	▪ Detail the test architecture and environment in the PA-DSS Report.	□
6	**Provide capabilities for, and test using, the following penetration testing methodologies:**	
	▪ **Use of forensic tools/methods[2]:** Search all output identified for evidence of sensitive authentication data using commercial tools, scripts, etc., per PA-DSS Requirement 1.1.1–1.1.3.	□
	▪ **Attempt to exploit QWASP vulnerabilities:** Attempt to exploit the application(s) per PA-DSS Requirement 5.1.1–5.1.10.	□
	▪ **Attempt to execute arbitrary code during the application update process:** Run the update process with arbitrary code per PA-DSS requirement 7.2.b.	□
7	**Use vendor's lab ONLY after verifying all requirements are met** *If use of the application vendor's lab is necessary (e.g., the PA-QSA does not have the mainframe, AS400, or Tandem the application runs on), the PA-QSA can either (1) use equipment on loan from the vendor or (2) use the vendor's lab facilities, provided that this is detailed in the report together with the location of the tests. For either option, the PA-QSA should verify that the vendor's equipment and lab meet the following requirements:*	
	▪ The PA-QSA verifies that the vendor's lab meets all above requirements specified in this document and documents the details in the report	□
	▪ All testing is executed by the PA-QSA (the vendor cannot run tests against their own application)	□
	▪ All testing is either (1) performed while on-site at the vendor's premises, or (2) performed remotely via a network connection using a secure link (e.g., VPN).	□

[2] Forensic tool or method: A tool or method for uncovering, analyzing and presenting forensic data, which provides a robust way to authenticate, search, and recover computer evidence rapidly and thoroughly. In the case of forensic tools or methods used by PA-QSAs, these tools or methods should accurately locate any sensitive authentication data written by the payment application. These tools may be commercial, open-source, or developed in-house by the PA-QSA.

Requirement		Lab Capabilities and Processes Verified
8	**Maintain an effective quality assurance (QA) process**	□
	▪ The QA process verifies that all platforms identified in the PA-DSS report were included in testing	□
	▪ The QA process verifies that all PA-DSS requirements were tested against	□
	▪ The QA process verifies that PA-QSA laboratory configurations and processes meet requirements and were accurately documented in the report.	□
	▪ The QA process verifies that the report accurately presents the results of testing.	□

Appendix C. PA-QSA – Application Process Checklist

This checklist has been provided as a tool to help you organize the Payment Application Qualified Security Assessor (PA-QSA) application information that must be submitted along with your completed/signed Agreement. This checklist is for new PA-QSA applications only. This checklist is a tool only—please review the detailed requirements in this document to ensure completeness of submitted information.

PA-QSA Business Requirements[3]

Requirement	Information/documentation Needed
Business Legitimacy	Not applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Validation Requirements* Appendix B: Qualified Security Assessor – New Application Process Checklist.
Independence	Not applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Validation Requirements* Appendix B: Qualified Security Assessor – New Application Process Checklist.
Insurance Coverage	Not Applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Validation Requirements* Appendix B: Qualified Security Assessor – New Application Process Checklist.
PA-QSA Fee	□ Initial PA-QSA processing fee, payable to PCI SSC
PA-QSA Addendum	□ PA-QSA Addendum signed by company officer

[3] This checklist is for **PA-QSAs** and details the documentation needed to substantiate the PA-QSA's qualifications to perform PA-DSS Assessments. It is also required that PA-QSAs are qualified as QSAs as well, and all PA-QSA documentation must be accompanied by QSA documentation (or that QSA documentation must be previously submitted to PCI SSC), as stated in the *Validation Requirements for Qualified Security Assessors* document, Appendix B.

PA-QSA Capability Requirements[3]

Requirement	Information/documentation Needed
PA-QSA Company Services and Experience	Meet the following PA-QSA Company requirements, in addition to all QSA requirements specified in *Validation Requirements for Qualified Security Assessors.* □ Description of both relevant experience with and areas of specialization within application security and application and code reviews, preferably related to payment applications and including a description of methodology used to perform such reviews. □ Description of dates and clients for two previous PCI DSS assessments performed by company □ Description of cryptographic techniques, including cryptographic algorithms, key management and rotation processes, and secure key storage □ Two client references from recent application security assessments
PA-QSA Company Employee Skills and Experience	Meet the following for each PA-QSA employee to be qualified, in addition to all QSA requirements specified in *Validation Requirements for Qualified Security Assessors.* For each individual applying as a PA-QSA, provide a description of: □ Dates and clients for two previously completed PCI DSS assessments □ Areas of expertise in application security, application and code reviews, and/or cryptographic techniques

[3] This checklist is for **PA-QSAs** and details the documentation needed to substantiate the PA-QSA's qualifications to perform PA-DSS Assessments. It is also required that PA-QSAs are qualified as QSAs as well, and all PA-QSA documentation must be accompanied by QSA documentation (or that QSA documentation must be previously submitted to PCI SSC), as stated in the *Validation Requirements for Qualified Security Assessors* document, Appendix B.

PA-QSA Administrative Requirements[3]

Requirement	Information/documentation Needed
PA-QSA Testing Laboratory	□ Description of PA-QSA Testing Laboratory, using Appendix B as a template □ Inclusion of completed Appendix B: Checklist for PA-QSA Testing Laboratory and Laboratory Processes □ Description of documented processes used by PA-QSA to verify vendor's testing laboratory meets requirements specified in Appendix B, if use of vendor's testing is necessary
PA-QSA Contact Person—Primary and Secondary	□ Name □ Title □ Address □ Phone □ Fax □ E-mail
Background Checks	□ For each PA-QSA employee to be qualified, statement that employee successfully completed the background check in accordance with the QSA's policies and procedures □ Company signature on the PA-QSA Addendum
Adherence to PCI DSS Procedures and Attestation of Validation	□ Company signature on the PA-QSA Addendum
Quality Assurance	□ A description of the quality assurance procedure that will be used for PA-DSS Assessments □ A description of the responsibilities of the PA-DSS Quality Assurance contact, including at least the following: ▪ Oversight of quality assurance for all PA-DSS reports ▪ Review and approval of all PA-DSS reports prior to submission to PCI SSC ▪ Sole responsibility for submitting PA-DSS reports to PCI SSC □ Company signature on the PA-QSA Addendum
Responsibility for QA Oversight—Primary and Secondary	□ Name □ Title □ Address □ Phone □ Fax □ E-mail
Protection of Confidential and Sensitive Information	Not applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Validation Requirements*, Appendix B – Qualified Security Assessor – New Application Process Checklist.

(continued on next page)

PA-QSA Administrative Requirements[3] *(continued)*

Requirement	Information/documentation Needed
Evidence Retention	Not applicable for PA-QSA documentation; however, this information should either: a) Already have been submitted as part original QSA application, or b) For new QSAs also applying to be a PA-QSA, included as part of QSA application per *QSA Validation Requirements*, Appendix B – Qualified Security Assessor – New Application Process Checklist.
Recognition of Client's Validation Status	□ A statement that PA-QSA will not recognize a client's validation status until PCI SSC has notified PA-QSA and vendor via an acceptance letter and inclusion of the application on the list of validated applications □ Company signature on the PA-QSA Addendum

[3] This checklist is for **PA-QSAs** and details the documentation needed to substantiate the PA-QSA's qualifications to perform PA-DSS Assessments. It is also required that PA-QSAs are qualified as QSAs as well, and all PA-QSA documentation must be accompanied by QSA documentation (or that QSA documentation must be previously submitted to PCI SSC), as stated in the *Validation Requirements for Qualified Security Assessors* document, Appendix B.

Appendix D. Sample PA-QSA Feedback Form

This form is used to review PA-QSAs and their work product, and is intended to be completed by the client, after a PCI PA-DSS Assessment audit. While the primary audience of this form are the clients of PA-DSS Assessments (software vendors or distributors), there are several questions at the end, under “PA-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 PA-QSA.

This form can be obtained directly from the PA-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.

PA-QSA Feedback Form

	Client (software vendor)			*Payment Application Qualified Security Assessor Company (PA-QSA)*	
Name					
Contact					
Title					
Telephone					
E-mail					
	Location of Assessment			*PA-QSA employee(s) who performed Assessment*	
Street				Name	
City		Country		ID number	
State/ Province		Postal Code		Telephone	
				E-mail	

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

Statement	**Select One**	**Comments**
1. During the initial engagement, the PA-QSA explained the objectives, timing, and review process, and addressed your questions and concerns.	***1-5***	
2. The PA-QSA employee(s) understood your business and technical environment, as well as the cardholder data environment.	***1-5***	

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

Statement	Select One	Comments
3. The PA-QSA employee(s) had sufficient security and technical skills to effectively perform this assessment.	***1-5***	
4. The PA-QSA sufficiently understood the Payment Application Data Security Standard and Audit Procedures.	***1-5***	
5. The PA-QSA effectively minimized interruptions to operations and schedules.	***1-5***	
6. The PA-QSA provided an accurate estimate for time and resources needed.	***1-5***	
7. The PA-QSA provided an accurate estimate for report delivery.	***1-5***	
8. The PA-QSA did not attempt to market products or services for your company to attain PA-DSS compliance.	***1-5***	
9. The PA-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 PA-QSA presented product and/or solution options that were not exclusive to their own product set.	***1-5***	
11. The PA-QSA used secure transmission to send any confidential reports or data.	***1-5***	
12. The PA-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 assessment.	***1-5***	
14. During the review wrap-up, the PA-QSA clearly communicated findings and expected next steps.	***1-5***	
15. The PA-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 PA-QSA, your assessment experience, or the PA-DSS documents.		

PA-QSA Feedback Form for Payment Brands and Others

	PA-QSA Client (merchant or service provider reviewed)	**Payment Application Qualified Security Assessor Company (PA-QSA)**	
Company Name			
	Payment Brand Reviewer	**PA-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 PA-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 Client had a positive and professional experience with the PA-QSA.	***1-5***	
3. The PA-QSA demonstrated sufficient understanding of the PCI Payment Application Data Security Standard Security Audit Procedures.	***1-5***	
4. The PA-QSA appropriately documented the results related to their findings.	***1-5***	
5. From your understanding, the PA-QSA appropriately scoped the payment application's role cardholder data environment.	***1-5***	

Appendix E. PA-QSA Fees

This table shows the PA-QSA fees. Like QSAs, PA-QSAs are qualified to serve specific markets and pay fees according to those markets of service, or 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 PA-QSA application package. See Section 1.6 of this document for the mailing address.

Region	**Initial Processing Fee***	**Qualification Fee**	**Annual Re-qualification Fee**	**Training Fee per individual**
Asia Pacific	500 USD	2,000 USD	1,000 USD	500 USD
Canada	500 USD	5,000 USD	2,500 USD	1250 USD
Central Europe, Middle East, and Africa	500 USD	2,000 USD	1,000 USD	500 USD
Europe	500 USD	5,000 USD	2,500 USD	1250 USD
Latin America and the Caribbean	500 USD	2,000 USD	1,000 USD	500 USD
USA	500 USD	5,000 USD	2,500 USD	1250 USD

* The Initial Processing Fee will be credited toward the Qualification Fee when a company is qualified as a PA-QSA.