
# Payment Card Industry (PCI) Data Security Standard

# QSA Validation Requirements

## Supplement for PCI Forensic Investigators (PFIs)

Version 2.0
November 2012

## Document Changes

| Date | Version | Description |
|---|---|---|
| November 2012 | 2.0 | Amendments to support remote forensic investigations and minor administrative revisions |

.

# Table of Contents

# 1 Introduction

This document supplements and should be read in conjunction with the *PFI Program Guide* (defined in Section 1.1 below) and the *QSA Validation Requirements* (defined in Section 1.1 below), as well as the other documents referenced in Section 1.3 below. Capitalized and other terms used but not otherwise defined herein shall be defined as provided in Section 1.1 below.

### Background

To help ensure the security of Cardholder Data, applicable payment card industry rules require merchants, service providers, financial institutions and other entities that process, store or transmit Cardholder Data to comply with the relevant PCI Standards. Compliance with the PCI DSS is assessed either by companies qualified to do so by PCI SSC (including but not limited to "QSAs") or by the merchant, service provider, financial institution, or other entity itself.

In the event of an actual or suspected attack, compromise or vulnerability affecting payment card transactions or Cardholder Data, forensic investigation may be required. Forensic investigation of this kind can be challenging and complex, requiring forensic investigators with highly specialized skills and proven staff and experience, capable of rapid response.

Prior to the PFI Program, Participating Payment Brands maintained separate requirements for forensic investigators for such events, and the process of selecting or being approved as an investigator could be complicated and cumbersome, especially when the Security Issue in question affected multiple Participating Payment Brands.

The PFI Program represents a streamlining of requirements for forensic investigators, and is intended to help simplify and expedite procedures and requirements for being approved as, and engaging with, forensic investigators.

### PFI Program

In an effort to help ensure that each PFI and PFI employee possesses the requisite knowledge, skills, experience and capacity to perform PFI Investigations in a proficient manner in accordance with industry expectations, each PFI and each PFI employee (including Core Forensic Investigators and Lead Investigators) is required at all times to satisfy all applicable PFI Validation Requirements, and must demonstrate the same as part of initial PFI approval and annually thereafter.

***IMPORTANT NOTE:***

*Approval as a PFI or PFI employee requires that the company or employee in question at all times be a PCI SSC-approved QSA or QSA employee, as applicable. Accordingly, approval as a PFI or PFI employee will immediately and automatically terminate if the underlying QSA qualification is revoked, cancelled, withdrawn or terminated.*

Once approved, and thereafter while in Good Standing, a PFI is eligible to perform PFI Investigations of Security Issues where the PFI has determined (in good faith, prior to initiating the PFI Investigation) that the associated data loss originated in a PFI Region for which that PFI is then approved in accordance with the PFI Program.

This Supplement for PCI Forensic Investigators is intended for candidate and existing PFIs and PFI employees, as well as Approving Organizations, and sets forth the additional requirements that must be satisfied by a given QSA and its employees in order to be approved as a PFI, PFI employee, Core Forensic Investigator or Lead Investigator (as applicable) under the PCI SSC PFI Program.

Interested entities must meet or exceed all applicable PFI Validation Requirements in order to be approved as PFIs and maintain their approval.

## 1.1 Terminology

The terms set forth in this Section 1.1, when used in this document, shall have the meanings set forth in this Section 1.1. When used in the *PFI Supplement,* terms defined in *the PFI Program Guide* or *QSA Validation Requirements* and not defined in the *PFI Supplement* shall have the meanings ascribed to them in the *PFI Program Guide* or *QSA Validation Requirements,* as applicable.

| Term | Meaning |
|---|---|
| Approving Organization | PCI SSC, or such other organization as PCI SSC may from time to time designate to review and approve entities as PFIs for purposes of participation in the PFI Program. |
| ASV Assessment | An information security vulnerability assessment performed by a PCI SSC- approved Approved Scanning Vendor in accordance with the *PCI SSC Validation Requirements for Approved Scanning Vendors (ASV)* or successor document thereto. |
| Cardholder Data | Defined in the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* |
| Compromised Entity | A merchant, service provider, financial institution, or other entity that: (a) processes, stores or transmits Cardholder Data; (b) is required to comply with any PCI Standard; and (c) is, at the time in question, required pursuant to Industry Rules to undergo a PFI Investigation of a specific Security Issue. |
| Core Forensic Investigator | A PFI employee who satisfies all of the requirements set forth in Section 3.3.3 hereof. |
| Good Standing | (a) With respect to a given PFI, that the PFI is in Good Standing as a QSA (as described in the QSA Validation Requirements), the PFI's PFI approval has not been revoked, terminated, suspended, cancelled, or withdrawn, the PFI is in compliance with all PFI company requirements, and the PFI is not in breach of any of the terms, conditions, requirements, obligations, policies, or procedures of the PFI Program Guide, the PFI Program, the PFI's QSA Agreement or PFI Addendum, or any other agreement with PCI SSC; and<br>(b) With respect to a given PFI employee, that the PFI employee is in compliance with all PFI employee requirements. |
| Industry Rules | Applicable payment card industry rules and requirements of acquirers, issuers and/or Participating Payment Brands. |
| Lead Investigator | With respect to a given PFI Investigation, a Core Forensic Investigator designated by the applicable PFI to lead that PFI Investigation. |

| Term | Meaning |
|---|---|
| P2PE Standard | The then-current versions of (or successor documents to) the *Payment Card Industry (PCI) Point-to-Point Encryption Solution Requirements and Testing Procedures*, any and all appendices, exhibits, schedules, and attachments to any of the foregoing and all materials incorporated therein, in each case, as from time to time amended and made available on the Website. |
| PA-DSS | The then-current version of the *Payment Card Industry (PCI) Payment Application Data Security Standard Requirements and Security Assessment Procedures* (or successor document thereto), as made publicly available by PCI SSC. |
| PA-QSA or Payment Application Qualified Security Assessor | 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-QSA Assessment | A PA-DSS assessment performed by a PA-QSA. |
| Participating Payment Brand | A payment card brand that, as of the time in question, is also then a formally admitted member of PCI SSC (or affiliate thereof). The Participating Payment Brands as of the release of this version of this document were American Express Travel Related Services Company, Inc, DFS Services LLC, JCB Advanced Technologies, Inc, MasterCard International Incorporated, Visa International Service Association (or respective affiliates). |
| PCI DSS | The then-current version of the *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures* (or successor document thereto), as made publicly available by PCI SSC. |
| PCI SSC | PCI Security Standards Council, LLC, a Delaware limited liability company. |
| PCI Standards | The security standards published and managed by PCI SSC, including without limitation, the PCI DSS and the PA-DSS. |
| PFI | A company, organization or other legal entity that has been approved as a PFI by an Approving Organization and is in compliance with all PFI company requirements. |
| PFI Addendum | An addendum to the QSA Agreement in the form attached hereto as *Appendix B* |
| PFI company requirements | The requirements applicable to PFIs and the provisions required of PFIs as set out in the PFI Supplement and PFI Program Guide, and such additional requirements as PCI SSC may establish for PFIs from time to time in connection with the PFI Program. |

| Term | Meaning |
|---|---|
| PFI employee | A full-time employee of a PFI who has been approved as a PFI employee by the Approving Organization and is in compliance with all PFI employee requirements. |
| PFI employee requirements | The specific requirements applicable to PFI employees as set out in Section 3.3.1 below, and such additional requirements as PCI SSC may establish for PFI employees from time to time in connection with the PFI Program. |
| PFI Guidelines | The *Forensic Investigation Guidelines* attached as *Appendix A* to the *PFI Program Guide*. |
| PFI Investigation | The forensic investigation of a Security Issue for a Compromised Entity pursuant to applicable Industry Rules. |
| PFI Program | The PCI Forensic Investigator Program as managed by PCI SSC and as further described herein and in the PFI Program Guide. |
| PFI Program Guide | The then-current version of the *Payment Card Industry (PCI) PCI Forensic Investigator (PFI) Program Guide* (or successor document thereto), as made publicly available by PCI SSC. |
| PFI Region | With respect to a given PFI, a geographical region (as identified in *Appendix B* hereto) (a) for which the PFI has paid all applicable regional approval and renewal fees in accordance with the then applicable PFI Program requirements and (b) with respect to which PCI SSC has approved the PFI to perform PFI Investigations. |
| PFI Reports | Reports based on evidence obtained by following the PFI guidelines. See Section 4.3.1 below. |
| PFI Supplement | The then-current version of this *Payment Card Industry (PCI) Data Security Standard, QSA Validation Requirements, Supplement for PCI Forensic Investigators (PFIs)* (or successor document thereto), as made publicly available by PCI SSC. |
| PFI Validation Requirements | Collectively, the PFI company requirements and the PFI employee requirements. |
| Qualified Integrators and Resellers or "QIRs" | Refers to a company that has satisfied and continues to satisfy all requirements set forth in QIR Qualification Requirements, and is thereby qualified by PCI SSC to implement, configure, or support validated PA-DSS payment applications on behalf of merchants as part of the PCI SSC Qualified Integrators and Resellers Program. |
| QIR Qualification Requirements | The then current version of the *Payment Card Industry (PCI) Qualification Requirements for Qualified Integrators and Resellers (QIRs)* (or successor document thereto), as made publicly available and amended by PCI SSC from time to time in its sole discretion, including but not limited to, all supplements and addenda thereto. |

| Term | Meaning |
|---|---|
| QSA Assessment | An on-site PCI DSS assessment performed by a QSA. |
| QSA Validation Requirements | The then-current version of the *Payment Card Industry (PCI) Data Security Standard Validation Requirements for Qualified Security Assessors (QSA)* (or successor document thereto), as made publicly available by PCI SSC. |
| Security Issue | An actual or suspected compromise or other incident that, pursuant to applicable Industry Rules, requires forensic investigation by a PFI. |
| Website | The PCI SSC website at www.pcisecuritystandards.org. |

## 1.2 Approval Process Overview

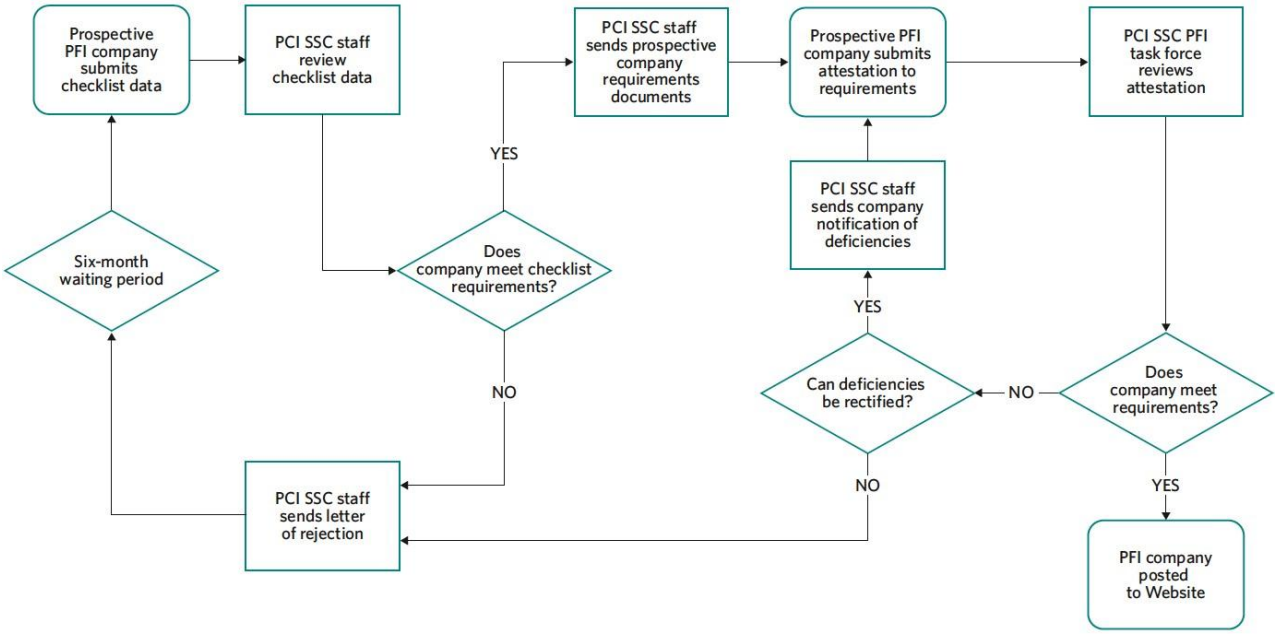
PFI approval involves: (a) review of initial application materials submitted by the PFI (company) to determine minimum eligibility ("Initial Document Review"), (b) follow-up information requests and interviews with key PFI employees (collectively, "Approval Review"), and (c) annual renewal.

To initiate the PFI approval process, the candidate PFI must first submit a complete initial PFI application package to the Approving Organization, including all of the materials specified in the Initial PFI Application Checklist attached hereto as *Appendix A* (such materials and payment, together, an "Initial PFI Application Package"). Candidates that meet all applicable minimum requirements at the Initial Document Review stage are then invited to provide all remaining required documentation and may participate in the Approval Review process (described further below).

Companies successful at the Approval Review stage are then identified as PFIs on the list of PCI Forensic Investigators maintained on the Website (the "PFI List") for a period of one (1) year from the date of their last PFI Program approval (or renewal), and may renew annually thereafter. Companies not identified on the PFI List are not recognized by PCI SSC as PFIs.

Eligible candidate PFI companies may apply for PFI approval only during open enrollment periods determined by PCI SSC based upon periodic needs assessment. Interested companies are encouraged to confirm open enrollment by contacting PCI SSC directly at the contact e-mail or number set forth in Section 1.4 below, prior to applying for consideration.

### *PFI Approval Process*



## 1.3 Related Publications

The PFI Supplement should be used in conjunction with the current versions of the following other PCI SSC publications, each as available through the Website and defined in Section 1.1 above:

- *PFI Program Guide*
- *QSA Validation Requirements*
- *PCI DSS*
- *PA-DSS*
- *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (see Website)
- *P2PE Standard*

## 1.4 PFI Application and Approval Process

In addition to outlining the requirements that a PFI must meet to perform PFI Investigations, this *PFI Supplement* describes the information that must be provided to the Approving Organization as part of the PFI application and approval process. Each outlined requirement is followed by the information that must be submitted to the Approving Organization to document that the QSA applying to become a PFI meets or exceeds the stated requirements.

Information that must be submitted as part of the Initial PFI Application Package is specified in the Initial PFI Application Process Checklist attached hereto as *Appendix A.* All Initial PFI Application Packages must include all of the documentation specified in the Initial PFI Application Checklist. All remaining materials specified in this PFI Supplement but not required as part of the Initial PFI Application Package must be provided to the Approving Organization as part of the Approval Review process, and in any event, prior to final approval by the Approving Organization.

Please note: The PFI Addendum must be executed and submitted to the Approving Organization in English, and is binding in English, even if translated and reviewed in another language. All application materials produced by the applicant (such as descriptions and references) must be submitted in English, and any application materials submitted in a language other than English (for example, business licenses and insurance certificates) must be accompanied by a certified English translation.

Applicants should send their request for access to the PFI Application Program by e-mail to pfi@pcisecuritystandards.org

## 1.5 Additional Information Requests

In an effort to maintain the integrity of the PFI program, PCI SSC may from time to time request that PFIs and PFI employees submit additional information or materials to the Approving Organization in order to demonstrate adherence to applicable PFI Validation Requirements or as part of the PFI approval process. Unless otherwise agreed by the Approving Organization in a specific instance, all such additional information and materials must be submitted in English or with a certified English translation. PFIs are required to respond to each such request with the required information or documentation no later than three (3) weeks from receipt of the corresponding written request.

# 2 PFI Business Requirements

This Section addresses the minimum PFI business requirements that each PFI must satisfy, and where applicable, the business-related PFI information and materials that each PFI must provide to the Approving Organization, in order to be approved and maintain approval as a PFI.

## 2.1 QSA Requirements

Each PFI must be a QSA in Good Standing as a QSA (as further described in the QSA Validation Requirements), including without limitation, continuing compliance with all requirements applicable to QSA companies regarding Business Legitimacy, Independence, Insurance and all other matters addressed in the QSA Validation Requirements.

The requirements set forth in this PFI Supplement, and the information and materials specifically required from PFIs and candidate PFIs hereunder, are in addition to the requirements and the information and materials to be provided under the QSA Validation Requirements.

## 2.2 Required Certificates, Licenses and Permits

Some jurisdictions may require companies and/or individuals engaged in forensic and/or private investigation or other services in connection with Security Issues to be certified or licensed to do so or to obtain other permits, authorizations, permissions or consents in connection with such work ("Required Certifications and Consents"). It is the responsibility of each PFI to determine which, if any, Required Certifications and Consents are required, and to obtain all Required Certifications and Consents prior to engaging in PFI work. Neither PCI SSC nor any other Approving Organization is or shall be responsible for making any such determination or for obtaining or informing any PFI or PFI employee regarding Required Certifications and Consents.

## 2.3 Independence

In addition to meeting all independence requirements in accordance with the QSA Validation Requirements:

- PFIs must limit sources of influence that might compromise independent judgment in performing PFI Investigations.
- PFIs are not permitted to perform any PFI Investigation for any company, organization or other entity for which the PFI (or any then-current PFI employee of such PFI) has performed a QSA or ASV Assessment or a QIR Installation (as defined in the QIR Qualification Requirements) within the then preceding three years.
- A PFI that has performed a PA-QSA Assessment or P2PE Assessment (as defined in the then-current version of (or successor document to) the *PCI SSC QSA Qualification Requirements Supplement for Point-to-Point Encryption Qualified Security Assessors (QSA (P2PE) and PA-QSA (P2PE))* of a product that was involved in a given Security Issue is only permitted to assess the involvement of that product as part of a PFI Investigation if the PFI ensures that the business unit and personnel utilized by such PFI in connection with such Assessment are reasonably separate and isolated from, and do not interfere with the independence or decision-making of, the business unit and personnel utilized by such PFI in connection with the PFI Investigation.

- PFIs are not permitted to perform PFI Investigations for any company, organization or other entity that is using any product or service provided by or through the PFI, other than the PFI Investigation services.

## 2.4 Insurance Coverage

### *2.4.1 Requirements*

In addition to the insurance coverages required under the QSA Validation Requirements, each PFI must obtain and maintain at all times such additional insurance as is necessary to ensure that the PFI at all times carries an aggregate of at least $5,000,000 in coverage for Professional Errors and Omissions (including the Professional Errors and Omissions coverage required under the QSA Validation Requirements).

### *2.4.2 Provisions*

- Each PFI must provide to the Approving Organization an insurance certificate evidencing the above Professional Errors and Omissions coverage.
- The PFI shall provide to the Approving Organization proof of coverage statements for all subcontractors identified on the Subcontractor List (defined in Section 3.2.1 below), demonstrating to the Approving Organization's satisfaction that all such subcontractors are covered under the PFI's insurance or that such subcontractors have in effect their own insurance coverage satisfying all insurance requirements of the PFI Program as they apply to PFIs.

## 2.5 PFI Fees

### *2.5.1 Requirement*

**Initial Processing Fees**

The PFI Application Package must contain a check, payable to “PCI SSC”, to cover applicable initial processing fees for each geographic region in which the applicant PFI has applied for approval to perform PFI Investigations. These initial processing fees will be credited toward regional approval fee(s) (see below) if and when the applicant is approved as a PFI.

**Approval and Renewal fees**

Once a company is approved as a PFI, the following additional fees apply:

- For the first year of approval in each PFI Region, the applicable initial regional PFI approval fee, which must be paid in full within 30 days of notification.
- For each subsequent year of approval in each PFI Region, the applicable annual regional PFI renewal fee, which must be paid in full within 30 days of notification.

***Note:*** *All fees associated with the PFI Program are posted on the Website. All such fees are non-refundable, updated annually, and subject to change upon notice from PCI SSC. Posting of a revised fee schedule on the Website shall be deemed to constitute notice of a fee change.*

## 2.6 PFI Addendum

In order to participate in the PFI program, the PFI Addendum (See *Appendix B* hereto) must be signed in unmodified form by a duly authorized officer of the candidate PFI and submitted to the Approving Organization as part of the completed PFI Application Package. Among other things, the PFI Addendum includes attestation by the PFI that the PFI has satisfied all applicable PFI validation Requirements.

# 3 PFI Capability Requirements

This Section addresses the minimum PFI capability requirements that each PFI must satisfy, and where applicable, the capability-related PFI information and materials that each PFI must provide to the Approving Organization, in order to be approved and maintain approval as a PFI.

## 3.1 PFI Company – Experience

### *3.1.1 Requirements*

In addition to satisfying all requirements applicable to QSAs as part of the QSA Program, in order to maintain Good Standing as a PFI, a PFI must at all times:

- Fulfill all PFI company requirements and promptly notify PCI SSC of any failure to do so.
- Comply with all terms and conditions of all agreements between the PFI and PCI SSC, including without limitation, the QSA Agreement and the PFI Addendum.
- Have one or more dedicated forensic investigation divisions, departments, units or practices, of which all employees participating in any technical aspect of any PFI Investigation are PFI employees.
- Ensure that each PFI Investigation conducted by the PFI is supervised by a Lead Investigator.
- Ensure that there is at least one (1) Core Forensic Investigator at all times on a full-time basis for each of the PFI Regions for which the PFI has been approved.
- Ensure that all Lead Investigators on each PFI investigation have completed required PFI Program training and/or information sessions within the two-year period prior to leading a given PFI Investigation (including without limitation, Participating Payment Brand-specific training such as PIN security compliance validation training).
- Ensure that a PA-QSA who has completed all required PA-QSA examinations with a passing score and who possesses adequate knowledge and experience of the PA-DSS to competently perform PA-QSA Assessments is available to be assigned to each PFI Investigation
- Ensure that each PFI employee has successfully completed annual training for incident response and computer forensics professionals such as renewal of certifications, including but not limited to; information systems audit training to support professional certifications such as CISSP, CISM, CISA, or GIAC certification (in addition to any required PCI SSC training).
- Ensure that each PFI employee is proficient in the use of each forensic tool used by the PFI.
- Ensure that each of its PFI employees is in Good Standing as a PFI employee.
- Track PFI employee compliance with all PFI employee requirements and promptly notify PCI SSC if any of its PFI employees fails to satisfy any PFI employee requirement.

- Ensure that all technical aspects of all of its PFI Investigations are performed and managed solely by Lead Investigators, Core Forensic investigators and PFI employees in Good Standing.
- Only engage in (and only permit its PFI employees to engage in) PFI Investigations with respect to which the PFI has determined in good faith (immediately prior to initiating such PFI Investigation) that the data loss associated with the Security Issue under investigation originated in a PFI Region for which the PFI is then approved by PCI SSC and has paid all applicable regional approval and renewal fees in accordance with applicable PFI Program requirements.
- Upon reasonable request of any Participating Payment Brand, attend required conference calls with Participating Payment Brands and third parties, such as Point-Of-Sale (POS) vendors, resellers, integrators and others, addressing issues related to payment applications and/or security practices.

### *3.1.2 Provisions*

The following information must be provided or demonstrated to the satisfaction of the Approving Organization in order to be approved as a PFI and maintain PFI approval:

- Descriptions of the types of forensic examinations that the PFI has performed.
- At least one (1) redacted Forensic Investigation Report of a Payment Card Industry or similar investigation of a multi box environment such as a website and server or Point Of Sale device and interconnected card payment network. The report should include, but not be limited to, details on:
    - Tools used in the investigation and investigation procedures
    - How data was acquisitioned and analyzed
    - Network Infrastructure and diagram
    - Payment or data flow diagram
    - Results of the investigation
    - Timeline of the investigation
    - Conclusions on the investigative findings
    - If made the recommendations for remediation
- Two independent references from Compromised Entities for which the candidate PFI has performed forensic security investigations within the 12 months prior to the PFI application date
- Proof of existing relationships with appropriate cyber-crime oriented law enforcement agencies pertinent to each PFI Region for which the PFI has applied
- Documentation that the PFI employs a minimum of at least one (1) Core Forensic
- Investigator for each PFI Region for which the candidate PFI has applied for approval (or has been approved) at all times (and initiates approval procedures for all candidate Core Forensic Investigators at the time of the initial PFI application)
- List of PFI's language proficiencies

- Proof of substantial and appropriate knowledge and experience in investigating financial industry-related security breaches and compromises of payment card related data to enable the PFI to perform PFI Investigations in a proficient manner in accordance with industry practice and expectations
- Proof of competence in the use of industry-recognized forensic tools and software applications, as well as an investigative methodology that meet industry recognized legal and law enforcement standards
- List of all PFI employees of the PFI and their respective individual qualifications
- Proven methodology for acquiring and analyzing digital evidence including live response and volatile memory analysis
- Proven methodology for investigating data security compromises involving each of the following:
    - Key-management compromises involving PIN/ATM fraud;
    - Brick and mortar compromises involving full magnetic-stripe data; and
    - E-commerce compromises involving web applications
- Proficiency to analyze/reverse-engineer malware
- Attestation that each employee of the PFI with respect to whom the PFI is seeking or has obtained approval as a PFI employee satisfies all PFI employee requirements
- Annually, documentation that each Core Forensic Investigator of the PFI has successfully completed annual training for incident response and computer forensics professionals such as renewal of certifications (in addition to any required PCI SSC training)
- Prompt notice of any change to any of the information previously provided with respect to the
- PFI or any PFI employee thereof as a result of which the Good Standing of such PFI or PFI employee could come into question or the PFI or PFI employee would no longer be eligible for approval under the PFI Program

## 3.2 PFI Company – Services

### *3.2.1 Requirements*

Each PFI must satisfy the following requirements:

- Maintain, on a 24-hour per day basis throughout the year, a staff of PFI employees who provide the first level of phone and incident response for each applicable PFI Region.
- Maintain sufficient number of PFI employees and other staff to appropriately respond to emergency situations and deploy the necessary response team within 24 hours of notice of the applicable Security Issue.

> ***Note:*** *PFIs must factor in delays and variations in arrival time, which may depend on the geographic location of the trouble site, weather conditions, available transportation, and other issues.*

- Initiate each PFI Investigation at the applicable Compromised Entity's facilities no later than five (5) business days after the date of execution of the applicable PFI Investigation services agreement between the PFI and such Compromised Entity.
- Deploy staff in response to emergency situations within 24 hours of discovery. Ensure the availability of emergency PFI employees to provide second-level analyst support in connection with each PFI Investigation, including upon discovery of and during ongoing investigation of the corresponding Security Issue.
- Maintain appropriate equipment and storage facilities to ensure timely availability of required and appropriate equipment in connection with each Security Issue for which the PFI is engaged to perform PFI Investigation services.
- Provide to the Approving Organization a list of all subject matter experts that the PFI reasonably anticipates engaging to assist the PFI in the performance of its PFI Investigations (the "Subcontractor List").
- Promptly notify PCI SSC of all changes to subject matter experts utilized by the PFI in connection with PFI Investigations.

### *3.2.2 Provisions*

The PFI must provide evidence satisfactory to the Approving Organization to substantiate that it meets each of the requirements of Section 3.2.1 above, including without limitation, equipment and storage requirements, and incident response and emergency deployment requirements.

## 3.3 PFI Employees

### *3.3.1 PFI Employee Requirements*

Each individual who performs, manages or is otherwise involved in any technical aspect of any PFI Investigation must meet all of the following requirements:

- Full-time employee of the PFI (meaning this work cannot be subcontracted to non-employees, unless PCI SSC has given prior written consent for the applicable subcontracted worker in each instance).
- Knowledgeable in identifying full magnetic-stripe data, CVV2 and PIN blocks.
- Active incident response certification, such as SANs GIAC Certified Incident Handler (GCIH), GIAC Certified Forensics Analyst (GCFA), or equivalent certification satisfactory to the Approving Organization; or a minimum three (3) years of forensic investigation/incident handling experience.
- Successfully complete annual training for incident response and computer forensics professionals such as renewal of certifications (in addition to any required PCI SSC training).
- Such other requirements as PCI SSC may reasonably establish from time to time for PFI employees.

***Notes:***

- Only PFI employees who satisfy the above requirements are authorized to perform, manage or otherwise be involved with any technical aspects of any PFI Investigation.
- Approved subcontractors are not permitted to include, and no PFI shall permit any of its subcontractors to include, any company logo or reference to a company other than the responsible PFI, in any PFI report or other materials in connection with work performed as a subcontractor for the PFI.
- Upon reasonable request of PCI SSC, each PFI employee may be required (and agrees to) demonstrate the aforementioned skills (and all other skills and expertise required of such individuals pursuant to these PFI Validation Requirements) to the Approving Organization.

### 3.3.2 Provisions

The following information must be provided to the Approving Organization with respect to each individual for whom the PFI is seeking approval as a PFI employee:

- Proof of Incident Response certification, such as SANs GIAC Certified Incident Handler (GCIH) or GIAC Certified Forensics Analyst (GCFA), if applicable.

### 3.3.3 Special Requirements for Core Forensic investigators

#### 3.3.3.1 Requirements

Each PFI employee utilized as a Core Forensic Investigator must satisfy the following requirements, and the corresponding PFI must make the provisions set forth below to the Approving Organization in connection with each such PFI employee:

- Satisfy all PFI employee requirements.
- Be a full-time employee of the PFI. Subcontracted resources are **not** permitted to fulfill this role.
- Be a PCI SSC-approved QSA employee in compliance with all requirements applicable to QSA employees as set forth in the *QSA Validation Requirements*.
- Operate in a role that is primarily as a forensic investigator within the applicable PFI's
- dedicated PFI Investigation division, department, unit, or practice.
- Possess sufficient information security knowledge and experience to conduct technically complex enterprise security investigations in a proficient manner in accordance with industry expectations.
- Possess a Bachelor of Science (or equivalent) or higher degree in Computer Science, Electrical Engineering, Computer Engineering and/or Forensics, or a minimum five (5) years of equivalent industry experience.
- Satisfy all such other requirements as PCI SSC may reasonably establish from time to time for Core Forensic Investigators, including without limitation, if requested by PCI SSC, demonstration of expertise in performing forensic investigations.

#### *3.3.3.2 Provisions*

The following information must be provided to the Approving Organization with respect to each individual for whom the PFI is seeking approval as a Core Forensic Investigator:

- Resume demonstrating a BS or higher degree in Computer Science, Electrical Engineering, Computer Engineering and/or Forensics or minimum five (5) years of equivalent industry experience.

# 4 PFI Administrative Requirements

This Section addresses the minimum PFI administrative requirements that each PFI must satisfy, and where applicable, the administrative PFI information and materials that each PFI must provide to the Approving Organization, in order to be approved and maintain approval as a PFI.

## 4.1 Contact Person

### *4.1.1 Requirement*

The PFI must designate one primary and one secondary contact responsible for liaising with PCI SSC and the Participating Payment Brands regarding each of the following:

- PFI Investigations; and
- Oversight of PFI's internal quality assurance program for PFI Investigations (described further in Section 4.4 below).

***Note:*** *Different primary and secondary contacts may be responsible for PFI Investigations and PFI quality assurance.*

### *4.1.2 Provisions*

The following contact information must be provided to the Approving Organization for each primary and secondary contact referred to above:

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

## 4.2 Background Checks

PFIs must satisfy all background check requirements applicable to QSAs as specified in the *QSA Validation Requirements.*

## 4.3 Adherence to PCI Procedures

Each PFI must ensure that:

- Only PFI employees are permitted to manage, perform or otherwise be involved in any technical aspects of PFI Investigations.
- All PFI Investigations and all related work product strictly comply with the PFI Guidelines.
- All PFI Reports are generated for each PFI Investigation.

### 4.3.1 Requirements

The PFI must prepare all of the following reports (each such report and each other report relating to PFI Investigations as required from time to time in accordance with the PFI Program, a "PFI Report") based on evidence obtained by following the PFI Guidelines, and ensure delivery of such reports to the appropriate Participating Payment Brands or other parties in accordance with the *PFI Program Guide.*

- *Preliminary Incident Response Report*. For each PFI Investigation, the PFI must prepare and deliver applicable Preliminary Incident Response Reports in accordance with the PFIProgram Guide, following the Preliminary Incident Response Report template and instructions as then available on the Website.
- *Final Incident Report*. For each PFI Investigation, the PFI must prepare a Final Incident Report in accordance with the PFI Program Guide following the Final Incident Report Template and instructions as then available on the Website*.*
- *PIN Security Requirements Report*. For each PFI Investigation that involved a compromise of PIN Block or PIN data, the PFI must prepare a PIN Security Requirements Report in accordance with the PFI Program Guide, following the PIN Security Requirements Report Template and instructions as then available on the Website*.*
- *Monthly Status Reports*. On a monthly basis, the PFI must deliver *Monthly Status Reports* to the Participating Payment Brands in accordance with the PFI Program Guide.
- *Trending Analysis Reports*. On an annual basis or as otherwise specified by PCI SSC, the PFI must provide to PCI SSC and each Participating Payment Brand *Trending Analysis Report* in accordance with the PFI Program Guide.

## 4.4 Quality Assurance

### 4.4.1 Requirements

- Each PFI must have implemented a quality assurance program governing all aspects of PFI Investigations and related PFI practices and procedures in accordance with the PFI Program Guide, including without limitation: review process for generation of all PFI Reports and reviews of performed PFI Investigations, supporting documentation, and information to be documented in PFI Reports.
- Each PFI must have documented the details of the aforementioned quality assurance program in a program manual that includes, without limitation, all required PFI Report templates (such program manual may (but need not) be included as part of the program manual required in accordance with subsection 4.4 of the QSA Validation Requirements).
- The PFI and each PFI employee must adhere to all requirements and procedures of the aforementioned PFI quality assurance program, and must adhere with all applicable PFI Program quality assurance requirements, including but not limited to instructions and/or requirements of PCI SSC or the applicable Approving Organization contained in each of the following:
    - Applicable warning letters
    - Probation requirements and/or processes
    - Remediation requirements, processes and related fees

- Revocation requirements and/or processes
- Reinstatement requirements and/or processes
- Appeals requirements and/or processes

- The PFI must provide a Feedback Report in the form attached hereto as *Appendix C* to each Compromised Entity (and if applicable, to each acquirer) at the completion of its PFI Investigation thereof and request that it be promptly completed and delivered to PCI SSC.
- PCI SSC reserves the right, upon reasonable notice, to conduct PFI site visits for purposes of auditing the processes and procedures used by PFI for PFI Investigations; and each PFI must comply with all such requests and provide PCI SSC with reasonable access for such purposes.

### *4.4.2 Provisions*

- Each PFI must designate a quality assurance manager to the Approving Organization and provide to the Approving Organization a description of the responsibilities thereof, which responsibilities shall include, at a minimum, the following:
  - Oversight of quality assurance for all PFI Reports.
  - Review and approval of all PFI Reports prior to distribution to Participating Payment Brands, compromised entities or others, as applicable.
  - Sole responsibility for submitting PFI Reports to Participating Payment Brands, compromised entities or others, as applicable.
- Each PFI shall provide to the Approving Organization a description of the contents of the PFI's quality assurance manual, to confirm that the manual addresses all aspects of the PFI's procedures and requirements for PFI Investigations and report review processes, including without limitation, a requirement that all PFI employees must comply with all PFI employee requirements.
- Additionally, each PFI must provide to PCI SSC prompt written notice of any change to any information previously provided to PCI SSC or any other Approving Organization if such change is reasonably likely to impact the Good Standing of such PFI or to cause the PFI to no longer be eligible for PFI approval.
- All information, materials and documentation must be provided to the Approving Organization in English or with a certified English translation.

## 4.5 Evidence Handling

### *4.5.1 Requirements*

In addition to complying with all requirements regarding evidence retention as set forth in the QSA Validation Requirements, each PFI and PFI employee must comply with the evidence handling requirements set forth in *Appendix B* of the *PFI Program Guide*.

### *4.5.2 Provisions*

- The PFI must provide to the Approving Organization a copy of its policies and procedures for handling and preserving the integrity of evidence and how evidence is collected.
- The PFI must provide to the Approving Organization a copy of the documentation that all employees sign acknowledging the company's policies and procedures for handling and

preserving the integrity of evidence and how evidence is collected.

- PFI must provide to the Approving Organization proof that employees collecting evidence are proficient in use of the tools being used for the examination. This can be demonstrated by copies of certifications or notable experience in résumés.

## 4.6 Scope and Reporting

### *4.6.1 Requirements*

Each PFI must:

- Prior to each PFI Investigation, obtain from the applicable Compromised Entity full authorization to provide to each affected Participating Payment Brand (and, if the Compromised Entity is a merchant, the affected acquirer(s)), a copy of each PFI Report resulting from such PFI Investigation, except to the extent prohibited by applicable law.
- After each PFI Investigation, deliver a copy of the Final Incident Report (and PIN Security Requirements Report, if applicable) resulting from such PFI Investigation to each affected Participating Payment Brand (and, if the Compromised Entity is a merchant, each affected acquirer(s)), except to the extent prohibited by applicable law.
- Follow the PFI Guidelines and follow the incident report templates as outlined in the PFI Program Guide, for all PFI Investigations.
- Participate as reasonable, appropriate or required in all discussions of the PFI Investigation with the Compromised Entity, the affected acquirer(s) if the Compromised Entity is a merchant, and the affected Participating Payment Brands.
- Ensure that each PFI Investigation is not and shall not be directed or controlled in any way by the subject Compromised Entity, and include a legally binding statement to that effect in each of its agreements with Compromised Entities regarding PFI Investigation.
- Ensure that each Final Incident Report reflects the independent judgment and conclusions of the PFI and accurately reflects and includes all factual evidence found.
- Upon request of any affected Participating Payment Brand, make drafts of applicable PFI Reports and related work papers available to such Participating Payment Brand.
- Upon request of any affected Participating Payment Brand in connection with a given Security Issue investigated or being investigated by the PFI, reasonably cooperate with such Participating Payment Brand in such Participating Payment Brand's investigation of such Security Issue.
- Upon request of any affected Participating Payment Brand, provide to such Participating Payment Brand a list of corresponding affected payment card account information found from each PFI Investigation, including without limitation, exposed payment card account numbers and related details.

### *4.6.2 Provisions*

Each PFI must provide to the Approving Organization evidence acceptable to the Approving Organization that the PFI meets the requirements of Section 4.6.1 above.

# 5 PFI Initial Approval and Annual Renewal

## 5.1 Requirements

Each PFI and PFI employee must renew under the PFI Program on an annual basis, based on the applicable initial PFI (or PFI employee) approval date.

## 5.2 Provisions

The following must be provided to PCI SSC and/or will be considered during the renewal process for both PFIs and PFI employees:

- Payment of all applicable annual PFI renewal fees
- For each PFI employee, proof of completion of all required applicable annual PCI SSC training and information sessions, as applicable (e.g., proof that each Lead Investigator has completed all required PFI Program training and/or information sessions within the preceding two (2) year period; and that each PFI employee has successfully completed annual training for incident response and computer forensics professionals);
- For each PFI employee, proof of incident response and computer forensics training within the
- 12 months prior to renewal to support professional certifications (such as CISSP, CISM, or
- CISA certification), in addition to any required PCI SSC training; and
- Satisfactory feedback from Compromised Entities that have undergone PFI Investigation by the PFI, as well as Approving Organization(s) and Participating Payment Brands.

# Appendix A: Initial PFI Application Checklist

| Requirement | Information/Documentation Needed | |
|---|---|---|
| **Business Requirements** | ☐ | The candidate PFI must be a QSA in QSA Good Standing (e.g., not in remediation or delinquent on fees). |
| **Independence** | ☐ | Description of the candidate PFI's practices to maintain independence. |
| **Insurance Coverage**<br>*May vary based on geographic region and applicable law.* | ☐ | Insurance certificate evidencing minimum coverage level of $5,000,000 for Professional Errors and Omissions. |
| | ☐ | Insurance certificate(s) evidencing all other required insurance coverage levels in accordance with the QSA Validation Requirements. |
| | ☐ | Proof of coverage statements for all proposed subcontractors. |
| **Initial Processing Fees** | ☐ | Check payable to PCI SSC covering all applicable Initial Processing Fee(s) for all PFI Regions for which the candidate is requesting PFI approval. |
| **PFI Experience and Service** | ☐ | Summary description and samples of the types of forensic examinations it has performed. |
| | ☐ | Two independent references regarding the candidate PFI from forensic security engagements it has performed within the prior 12 months. |
| | ☐ | Documentation that the candidate PFI candidate employs a minimum of one (1) Core Forensic Investigator for each PFI Region for which the candidate is seeking PFI approval. |
| | ☐ | Documentation that the candidate PFI maintains, on a 24-hour per day basis throughout the year, staff of qualified analysts who provide the first level of phone and incident response globally or regionally as appropriate. |
| | ☐ | Documentation that the candidate PFI maintains appropriate equipment and storage facilities for use in the event of an incident response request. |
| | ☐ | Documentation that the candidate PFI can ensure that a PA-QSA who has completed all required PA-QSA examinations with a passing score and who possesses adequate knowledge and experience of the PA-DSS to competently perform PA-QSA assessments is available to be assigned to each PFI Investigation. |
| **PFI Employee Skills and Experience** | ☐ | Resumes for all Core Forensic Investigators, each demonstrating a Bachelor's of Science (or equivalent) or higher degree in Computer Science, Electrical Engineering, Computer Engineering and/or Forensics or minimum five (5) years of equivalent industry experience. |
| | ☐ | Proof of Incident Response certification for each PFI employee, such as SANs GIAC Certified Incident Handler (GCIH) or GIAC Certified Forensics Analyst (GCFA). |
| **Administrative Requirements** | ☐ | Contact information for each primary and secondary contact as required by Section 4.1.2 above. |

| Requirement | Information/Documentation Needed | |
|---|---|---|
| **PFI QA Program** | ☐ | Designation of Quality Assurance Manager |
| | ☐ | Description of contents of the PFI's quality assurance manual |
| **Evidence Handling** | ☐ | Copies of PFI policies and procedures regarding evidence handling, preservation, integrity and collection, along with associated standard form of employee acknowledgement |
| | ☐ | Evidence of PFI employees' proficiency in using the PFI's forensic investigation tools (such as copies of relevant certifications) |

# Appendix B: PFI Addendum

## Addendum to Qualified Security Assessor (QSA) Agreement for PCI Forensic Investigators

### 1. Introduction

This Addendum to Qualified Security Assessor (QSA) Agreement for PCI Forensic Investigators (the "Addendum") is entered into by and between PCI Security Standards Council, LLC ("PCI SSC") and the undersigned PCI Forensic Investigator Applicant ("Company") as of the date of PCI SSC's approval hereof (the "Addendum Effective Date"), as evidenced by PCI SSC's signature hereto, for purposes of adding and modifying certain terms of the *Qualified Security Assessor (QSA) Agreement* between PCI SSC and Company (the "Agreement"), as in effect as of the Addendum Effective Date. Capitalized terms defined in this Addendum shall have the meanings ascribed to them herein for all purposes of this Addendum and the Agreement. Capitalized terms used herein without definition shall have the meanings ascribed to them in the Agreement or the PFI Supplement (defined below), as applicable.

In consideration of the mutual covenants herein set forth, the sufficiency of which is acknowledged, Company and PCI SSC agree to the terms and conditions set forth herein.

### 2. General Information

| **PCI Forensic Investigator Applicant** | | | | |
|---|---|---|---|---|
| Company Name: | | | | |
| QSA Agreement Date: | | | | |
| Location/Address: | | | | |
| State/Province: | | City: | | |
| Country: | | Postal Code: | | |
| PFI regions applying for (*see Fee Schedule on Website*): | | | | |

| **Applicant's Officer** | | | |
|---|---|---|---|
| | | | |
| *Applicant's Officer's Signature* ↑ | | | *Date* ↑ |
| Name: | | Title: | |

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

## 3. Terms and Conditions

A. Definitions

1. Terms in Addendum

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

a) "PFI Documents" means the PFI Supplement and the PFI Program Guide

b) "PFI Program" means PCI SSC's PCI Forensic Investigator Program.

c) "PFI Program Guide" means the then-current version of the *Payment Card Industry (PCI) PCI Forensic Investigator (PFI) Program Guide* (or successor document thereto), as made publicly available by PCI SSC.

d) "PFI Services" means all PFI Investigations performed by Company and all related obligations of Company and services provided by Company to PCI SSC and/or Compromised Entities in connection with this Addendum and the PFI Program.

e) "PFI Supplement" means the then-current version of the *Payment Card Industry (PCI) Data Security Standard, QSA Validation Requirements, Supplement for PCI Forensic Investigators (PFIs)* (or successor document thereto), as made publicly available by PCI SSC.

f) "Affiliate" means, with respect to a given entity, any separate legal entity that directly or indirectly controls, is controlled by, or is under common control with such entity, where

g) the term "control" (and each derivate thereof) means the right to exercise a majority of the voting power, or power to direct the activities or operations, of the entity in question.

2. Terms in Agreement

While this Addendum is in effect, and intending to broaden and not limit any of the definitions of the terms appearing in the Agreement, the following terms appearing in the Agreement are hereby amended as follows for purposes of the Agreement:

a) The term "Services" shall also include the PFI Services.

b) The term "QSA Requirements" shall also include the PFI company requirements (as defined in the PFI Supplement).

c) The term "QSA Validation Requirements" shall also include the PFI Documents.

d) The term "PCI Materials" shall also include the PFI Documents.

e) The term "QSA Program" shall also include the PFI Program for purposes of Sections A.5 and A.7 of the Agreement.

B. PFI Services

Subject to the terms and conditions of the Agreement, this Addendum and the PFI Documents, PCI SSC hereby approves Company to conduct PFI Investigations of Compromised Entities with respect to Security Issues where Company has determined (in good faith, prior to initiating the corresponding PFI Investigation) that the data loss associated with such Security Issues originated in a PFI Region for which Company is then approved as a PFI and has paid applicable regional PFI fees in accordance with the PFI Program.

Company agrees to monitor the Website at least weekly for changes to the PFI Supplement and/or the PFI Program Guide. Company will incorporate all such changes into all PFI investigations initiated on or after the effective date of such changes.

C. Performance of PFI Services

1. Company agrees that it will perform each PFI Investigation in strict compliance with the PFI Guidelines (as defined in the PFI Supplement) in effect as of the commencement date of such PFI Investigation. Without limiting the foregoing, in connection with each PFI Investigation, Company hereby agrees: (a) to prepare all PFI Reports following the applicable PFI Report templates in the form then available through the Website; (b) that each PFI Report prepared by Company will be signed by a duly authorized officer of Company and delivered as and when required under the PFI Program Guide; and (c) upon request of any affected Participating Payment Brand, to provide reasonable cooperation to such Participating Payment Brand in connection with the investigation of the corresponding Security Issue(s) by such Participating Payment Brand.
2. Company acknowledges and agrees that PCI SSC, in an effort to maintain the integrity of the PFI Program, may request from time to time that Company demonstrate its adherence to applicable PFI Requirements. Each such request shall be in writing and Company shall respond thereto with documented evidence of such adherence in form and substance acceptable to PCI SSC no later than three (3) weeks from Company's receipt of such written request.
3. Company hereby agrees that it will at all times protect all cardholder data in accordance with the requirements of the PCI DSS and all other applicable PCI Standards.

D. PFI Service Staffing; Subcontractors.

Company shall ensure at all times that it satisfies all staffing requirements specified in the PFI Documents with respect to PFI employees, Core Forensic Investigators and Lead Investigators involved in PFI Investigations performed by Company.

Notwithstanding anything to the contrary in the Agreement, the Company may engage appropriate third party subject matter experts to perform specific aspects of PFI Investigations where necessary, without first obtaining the consent of PCI SSC; provided that (i) the PFI shall be primarily responsible and liable for the performance of all services by such subcontractors in connection with such PFI Investigations; (ii) the PFI shall promptly notify PCI SSC of each such engagement via electronic mail to pfi@pcisecuritystandards.org and shall promptly notify each affected Participating Payment Brand, prior to such subcontractor performing any such subcontracted for services if practicable, and in any event within one (1) business day after such services have begun in connection with each PFI Investigation in each instance; (iii) in the event PCI SSC notifies the PFI of its rejection of any such subcontractor, the PFI shall immediately cease its use of such subcontractor in connection with such PFI Investigation; (iv) the PFI shall not use any subcontractor for a given PFI Investigation of a given Compromised Entity if such subcontractor or any employee thereof is an Affiliate or employee of such Compromised Entity or any Affiliate thereof; and (v) the PFI shall only use subcontractors appearing on the then-current Subcontractor List if possible under the circumstances.

Upon notification by the PFI of any change to the Subcontractor List, the PFI's Subcontractor List will be deemed to have been updated accordingly. PCI SSC reserves the right to remove any subcontractor from a PFI's Subcontractor List if the subcontractor fails, upon reasonable request of the Approving Organization, to demonstrate appropriate subject matter expertise to the satisfaction of the Approving Organization. Upon such removal, the PFI's Subcontractor List will be deemed to have been updated accordingly.

E. PFI Validation Requirements

Company agrees to adhere to all PFI company requirements, and in connection therewith, to comply with all requirements and make all provisions required pursuant to the PFI Supplement, including without limitation, all PFI Business Requirements, PFI Capability Requirements, and PFI Administrative Requirements, as set forth in Sections 2, 3 and 4 of the PFI Supplement.

Company agrees to ensure that all of its PFI employees are in compliance with all applicable PFI employee requirements and, as applicable, all requirements applicable to Core Forensic Investigators. Company warrants that, to the best of Company's ability to determine, all in the PFI Program is and shall be accurate and complete as of the date such information is provided. Company acknowledges that PCI SSC may from time to time require Company to provide a representative to attend any mandatory training programs in connection with the PFI Program, which may require the payment of attendance and other fees.

## 4. PFI Program Fees

Company shall pay all applicable PFI Program fees (collectively, "PFI Fees"), including without limitation, applicable regional Initial Processing Fees, regional PFI approval fees and renewal fees, training fees and fees associated with remediation, in each case as and in the manner specified from time to time by PCI SSC in the PFI Documents or otherwise. Company acknowledges that PCI SSC may review and modify such fees at any time and from time to time, provided that PCI SSC shall notify Company of such change and such change shall be effective thirty (30) days after the date of such notification. Should Company not agree with any such change, Company may terminate this Addendum upon written notice to PCI SSC at any time within such 30-day period. All PFI Fees paid by Company in connection with the PFI Program and its participation in any aspect thereof are nonrefundable (regardless of whether Company is ultimately approved as a PFI, Company has been removed from the PFI List, this Addendum or the Agreement has been terminated or otherwise).

## 5. PFI List; Promotional References; Restrictions

A. So long as Company is in Good Standing (as defined in the PFI Supplement) as a PFI, PCI SSC may, at its sole discretion, identify Company as a PFI on the PFI List (as defined in the PFI Supplement) or in such other publicly available list of PFIs 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 PFI List), together with corresponding PFI approval status information and details (including without limitation, approval, suspension, remediation, or revocation status).

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

C. Company shall not: (i) make any false, misleading or incomplete statements regarding, or misrepresent the requirements of any standard or guideline published by PCI SSC, including without limitation, any requirement regarding the implementation of the PCI DSS or the application thereof to any third party, or (ii) state or imply that the any standard or guideline published by PCI SSC requires usage of Company's products or services.

## 6. Compromised Entity Data; Quality Assurance

A. To the extent any data or other information obtained or generated by Company relating to any Compromised Entity in the course of providing PFI Services thereto may be subject to any confidentiality restrictions between Company and such Compromised Entity, Company must provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such Compromised Entity in writing) that Company may disclose each PFI Report and all related information and work papers to PCI SSC and/or the Participating Payment Brands as required in accordance with the PFI Documents.

B. Each agreement between Company and each Compromised Entity shall include such provisions as may be required or necessary to ensure that Company has all rights, licenses and other permissions necessary for Company to comply with its obligations and requirements pursuant to this Addendum and the PFI Program. Any failure of Company to comply with this requirement shall be deemed a breach of Company's representations and warranties under the Agreement for purposes of Section A9.3 thereof, and upon any such failure, PCI SSC may remove Company's name from the PFI List and/or terminate the Agreement and/or this Addendum in its sole discretion.

C. Company agrees that all PFI quality assurance procedures and requirements established by PCI SSC from time to time as part of the PFI Program shall apply to Company in its capacity as a PFI, including without limitation, procedures and requirements applicable during remediation, and Company shall comply with all such procedures and requirements. Without limiting the generality of the foregoing, Company hereby acknowledges that PCI SSC utilizes the PFI Report Card process in connection with its PFI quality assurance initiatives and that Company's ongoing status as a PFI will ultimately depend on (among other things) the scores it receives as part of such PFI Report Card process. PFI agrees that all decisions of PCI SSC regarding the PFI Program and participation therein shall be final, binding, and made in the sole discretion of PCI SSC, including without limitation, decisions regarding approval, PFI listing and delisting, weighting and criteria for PFI Report Card scoring, remediation procedures and requirements and all other PFI Program matters.

## 7. Term and Termination

A. Term

This Addendum shall become effective as of the Addendum Effective Date and, unless earlier terminated in accordance with this Section 7.A, shall continue for an initial term of one (1) year, and thereafter shall renew for additional subsequent terms of one year, subject to Company's successful completion of applicable approval and renewal requirements and payment of applicable PFI Fees for each such one-year term (each a "Contract Year"). This Addendum shall immediately terminate upon termination of the Agreement.

B. Termination by Company

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

C. Termination by PCI SSC

PCI SSC may terminate this Addendum effective as of the end of any Contract Year by providing Company 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 Company's breach of any representation or warranty under this Addendum; or (ii) with fifteen (15) days' prior written notice following Company's breach of any term or provision of this Addendum (including without limitation, Company's failure to comply with any PFI company requirement), provided such breach remains uncured when such 15-day period has elapsed.

D. Effect of Termination

Upon any termination or expiration of this Addendum: (i) Company will no longer be identified as a PFI on the PFI List; (ii) Company shall immediately cease all advertising and promotion of its status as a PFI; (iii) Company shall immediately cease soliciting for any further PFI Services and shall only complete PFI Investigations for which Company was engaged prior to the applicable notice of termination; (iv) Company will deliver all outstanding PFI Reports to the required recipients as required pursuant to the PFI Documents and any applicable provisions of Company's agreement with the applicable Compromised Entity and shall remain responsible after termination for all of the obligations, representations and warranties hereunder with respect to all PFI Reports submitted to any Participating Payment Brand or acquirer prior to or after termination; (v) Company 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 PFI Services; and (vi) PCI SSC may notify any of its Members and/or acquirers of such termination. The provisions of this section shall survive the expiration or termination of this Addendum for any or no reason.

## 8. Third-Party Beneficiaries

Company hereby agrees that each Participating Payment Brand shall be an express third party beneficiary of this Agreement and, accordingly, shall have available to it all rights, whether at law or in equity, to enforce the provisions of this Agreement on its own behalf and in its own right directly against Company.

## 9. 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 (as previously amended and in effect) shall remain in full force and effect in accordance with its terms.

# Appendix C: Feedback Report

This Feedback Report is intended to be completed by the entity that has undergone forensic investigation by a PCI SSC PCI Forensic Investigator ("PFI") and, if applicable, by each acquirer of that entity, in each case at the conclusion of the PFI's forensic investigation.

***Note:*** *This Feedback Report should not be completed or submitted by the PFI. Completed Feedback Forms should be submit directly to PCI SSC by the investigated entity or acquirer (as applicable), via e-mail to pfi@pcisecuritystandards.org or by mail to the PCI SSC address provided in the PFI Supplement. All responses are optional and this form may be submitted anonymously and should be completed in English.*

### *Contact Information*

| **Feedback Participant** | |
|---|---|
| Company name | |
| Contact person | |
| Name | |
| Telephone | |
| E-mail | |
| **PFI Company** | |
| Company name | |
| PFI employee who performed the PFI Investigation | |
| Contact Name | |
| Telephone | |
| E-mail | |
| Reporting period | |
| Reports reviewed | |

*[Questions begin on next page.]*

## *Feedback Report*

For each question below, please indicate the response that best reflects your experience and provide comments where appropriate:

**5 = Strongly Agree 4 = Agree 3 = Neutral 2 = Disagree 1 = Strongly Disagree 0 = Not applicable**

***Note:*** *PCI SSC recognizes that there can be extenuating circumstances that impact of the outcome of a given PFI Investigation and related reporting. While providing feedback, if you feel extenuating circumstances apply, please make appropriate notes in the comments section(s).*

| | | |
|---|---|---|
| ***Timeliness*** *is a key element for PFIs. Please rate the PFI's performance relative to your own expectations prior to the PFI Investigation.* | | |
| 1 | Primary and preliminary reports were delivered within an appropriate timeframe. | Select one |
| | Comments: | |
| 2 | Regular status updates were provided by the PFI company as required by involved Participating Payment Brand(s). | Select one |
| | Comments: | |
| 3 | The PFI company supplied resources for this engagement sufficient to enable adherence to agreed-upon timelines for the investigation. | Select one |
| | Comments: | |
| 4 | The PFI company maintained regular communication regarding the project timeline and any issues, obstacles, or other extenuating circumstances that may have delayed completion. | Select one |
| | Comments: | |
| 5 | The PFI company met response time expectations such as deploying staff to respond in an emergency situation within 24 hours to five (5) days of discovery, as required by the Participating Payment Brand.<br>***Note:*** *Arrival time will depend on the geographic location of the trouble site, weather conditions, and available transportation* | Select one |
| | Comments: | |
| 6 | The PFI company provided at-risk account numbers in a timely fashion. | Select one |
| | Comments: | |

| | | |
|---|---|---|
| ***Accuracy*** *is another key element. In assessing Accuracy, consider whether or not there were instances where you believe the PFI made mistakes in methodology or in handling the investigation that led to an unsatisfactory forensic investigative report.* | | |
| 1 | The PFI company and personnel followed the proper methodologies as outlined in the PFI Guidelines (*Appendix A* to the *PFI Program Guide*). | Select one |
| | Comments: | |
| 2 | The PFI company and personnel identified all applicable causes of compromise during the investigation (i.e., in your opinion they did not miss anything and their conclusions were consistent with available evidence). | Select one |
| | Comments: | |
| ***Ethics*** *are important as well. In assessing Ethics, consider whether or not there were situations in which you believe the PFI or its personnel misrepresented or withheld information based on pressure from a key client, acquiring entity, or otherwise.* | | |
| 1 | The PFI company demonstrated compliance with all independence requirements for PFIs and QSAs throughout the PFI Investigation (See Section 2.2 of the PFI Supplement and Section 2.2 of the QSA Validation Requirements) and was not the same QSA company that conducted the initial or any subsequent QSA Assessment of the Compromised Entity. | Select one |
| | Comments: | |
| 2 | The PFI company fulfilled the objective of providing an independent, unbiased representation of the facts of the case. There were no significant or intentional omissions or misrepresentations of facts or unreasonable delays in conducting the investigation. In addition, the Lead Investigator or a suitable PFI process manager was available to answer questions about the investigation if necessary or appropriate. | Select one |
| | Comments: | |
| ***Cooperation*** *is also important. In assessing Cooperation, consider whether or not the PFI company was readily available for discussion of forensic findings and/or follow up questions and account data at risk was provided in a timely manner.* | | |
| 1 | The PFI company completed tasks on time. | Select one |
| | Comments: | |

| | | |
|---|---|---|
| 2 | The PFI company was regularly available for communication with the affected Participating Payment Brand(s) and their client(s). | Select one |
| | Comments: | |
| | The PFI company assigned an appropriately qualified Lead Investigator to respond to a address issues with affected Participating Payment Brands and the investigated organization throughout the PFI Investigation. | |
| | Comments: | |
| | The PFI company clearly identified any extenuating circumstances that impacted the investigation | |
| | Comments: | |
| ***Competence*** *is an elementary component for evaluation. In assessing Competence, consider whether or not the PFI or its personnel: were able to complete the PFI Investigation to your satisfaction; possessed the necessary skills or understanding of the task during the investigation; and was able to communicate the findings in a competent manner.* | | |
| 1 | If a given PFI employee investigator did not have sufficient understanding of an issue, the PFI company had the applicable knowledge and assigned appropriately qualified investigators who performed duties effectively and in a timely manner | Select one |
| | Comments: | |
| 2 | The PFI company investigators were articulate in communicating the investigative findings. | Select one |
| | Comments: | |
| 3 | The PFI company demonstrated sufficient understanding of the PCI DSS and the PA-DSS (if applicable). | Select one |
| | Comments: | |
| 4 | The PFI company clearly understood how to scope the PFI Investigation. | Select one |
| | Comments: | |

| | | |
|---|---|---|
| ***Reporting*** *with consistent format and adequate content is necessary to facilitate incident response. Please assess the PFI's performance relating to the following:* | | |
| 1 | The PFI company adhered to all PFI Report templates. | Select one |
| | Comments: | |
| 2 | All final PFI Reports provided data that clearly tied the conclusion back to the evidence. | Select one |
| | Comments: | |