Payment Card Industry (PCI)

Qualification Requirements

For PCI Forensic Investigators (PFIs)

Version 3.2
June 2019

Document Changes

Date	Version	Description
November 2012	2.0	Amendments to support remote forensic investigations and minor administrative revisions
August 2016	3.0	Updated to align with *PFI Program Guide v3.0*, *QSA Qualification Requirements v2.1* and other PCI SSC program documents Enhanced Independence requirements Updated PFI Company/Employee application process to use online portal
April 2018	3.1	Added new PFI Employee training requirements, removed requirement for Core PFIs to be QSAs.
June 2019	3.2	Added “within 18 months” to Section 3.1.2 for the redacted report submittals when applying to be a PFI Company Enhanced section 4.2 Background Checks Clarified that PFI candidate applications must be completed within 12 months

Table of Contents

1 Introduction

This document supplements and should be read in conjunction with the *PFI Program Guide* and the *QSA Qualification Requirements*, as well as the other documents referenced in Section 1.2 below. Capitalized and other terms used but not otherwise defined herein shall be defined as provided in Appendix D, as applicable.

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 QSA Companies) 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 qualified 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 qualified as, and engaging with, forensic investigators.

PFI Program

In an effort to help ensure that each PFI Company 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 Company and each PFI Employee (including Core Forensic Investigators and Lead Investigators)is required at all times to satisfy all applicable PFI Qualification Requirements, and must demonstrate the same as part of initial PFI qualification and annually thereafter.

IMPORTANT NOTE:

Qualification as a PFI Company or PFI Employee requires that the company in question at all times be a PCI SSC-qualified QSA Company. Accordingly, qualification as a PFI Company will immediately and automatically terminate if the underlying QSA Company qualification is revoked, cancelled, withdrawn or terminated.

Once qualified, and thereafter while in Good Standing, a PFI Company is eligible to perform PFI Investigations of Security Issues where the PFI Company 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 Company is then qualified in accordance with the PFI Program.

This document is intended for candidate and existing PFI Companies and PFI Employees, as well as Approving Organizations, and sets forth the additional requirements that must be satisfied by a given QSA Company and its employees in order to be qualified as a PFI Company, 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 Requirements in order to be qualified as a PFI

Company or PFI Employee and maintain Good Standing as such.

1.1 Qualification Process Overview

PFI Company qualification involves: (a) review of initial application materials submitted by the candidate PFI Company to determine whether the materials satisfy minimum eligibility requirements ("Document Review"), (b) follow-up information requests and interviews with key PFI Employees (collectively, "Qualification Review"), and (c) annual renewal.

To initiate the PFI Company application process, the candidate PFI Company (QSA Company) must first request an application fee invoice from PCI SSC by sending an e-mail to pfi@pcisecuritystandards.org. Once paid, the candidate PFI Company will be granted access to the online application. The candidate PFI Company must fully complete and submit the online application to the Approving Organization, including all of the materials specified in the PFI Application Checklist attached hereto as Appendix A ("PFI Application Package"). Candidates that meet all applicable minimum requirements of the Document Review may participate in the Qualification Review process (described further below).

Companies successful at the Qualification Review stage are then issued the initial regional invoice. Once the invoice is paid, the company is identified as a PFI Company 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 its last PFI Program qualification (or renewal), and may renew annually thereafter, subject to PFI Program requirements and rules. Only those PFI Companies on the PFI List are recognized by PCI SSC to perform PFI Investigations. Companies not identified on the PFI List are not recognized by PCI SSC as PFI Companies.

1.2 Related Publications

The *PFI Qualification Requirements* should be used in conjunction with the current versions of the following other PCI SSC publications, each as available through the Website and defined as provided for in Appendix D:

- *PFI Program Guide*
- *QSA Qualification Requirements*
- *PCI DSS*
- *PA-DSS*
- *PCI DSS Glossary of Terms, Abbreviations, and Acronyms* (see Website)
- *P2PE Standard*
- *PCI 3DS Core Security Standard*

1.3 PFI Application and Initial Qualification Process

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

Information that must be submitted as part of the PFI Application Package is specified in the PFI Application Checklist attached hereto as Appendix A. All PFI Application Packages must include all documentation specified in the PFI Application Checklist. All remaining materials specified in the PFI Qualification Requirements but not required as part of the PFI Application Package must be provided to the Approving Organization as part of the Qualification Review process and, in any event, prior to final qualification by the Approving Organization. Applications must be completed within 12 months of being granted Portal access.

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.*

1.4 Additional Information Requests

In an effort to maintain the integrity of the PFI Program, PCI SSC may from time to time request that PFI Companies and/or PFI Employees submit additional information or materials to the Approving Organization in order to demonstrate adherence to applicable PFI Requirements, as part of the PFI requalification process, or as part of PCI SSC's PFI Company quality assurance process, including but not limited to in connection with remediation, revocation, or appeals. Unless otherwise agreed by the Approving Organization in a specific instance, all such additional information and materials must be submitted in accordance with the corresponding PCI SSC request, in English or with a certified English translation. PFI Companies are required to respond to each such request with the requested information and/or documentation no later than three (3) calendar weeks from receipt of the corresponding written request or as otherwise requested by PCI SSC.

2 PFI Business Requirements

This section addresses the minimum PFI Company business requirements that each PFI Company must satisfy, and where applicable, the business-related PFI Company information and materials that each PFI Company (or candidate) must provide to the Approving Organization, in order to be qualified and maintain Good Standing as a PFI Company.

2.1 QSA Requirements

Each PFI Company must be a QSA Company in Good Standing (as further described in the *QSA Qualification 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 Qualification Requirements*.

The requirements set forth in the *PFI Qualification Requirements*, and the information and materials specifically required from PFI Companies and candidate PFI Companies hereunder, are in addition to the requirements and the information and materials to be provided under the *QSA Qualification 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 Company 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 Company or PFI Employee regarding Required Certifications and Consents.

2.3 Independence

PFI Companies and PFI Employees must satisfy the requirements of this Section 2.3 and the separate independence requirements specified in the *QSA Qualification Requirements* (all of the foregoing, collectively, the "Independence Requirements"):

Note: *Any agreement, relationship or restriction that materially impairs (or has the appearance of so impairing) the PFI Company's or PFI Employee's independence, professional judgment, integrity, objectivity, impartiality, or professional skepticism in rendering its findings, conclusions or PFI Reports, without appropriate disclosure and countervailing measures, is deemed to violate these independence requirements*

- PFI Companies and PFI Employees must perform all PFI Investigations, and render and deliver all associated PFI Services, conclusions, findings and PFI Reports (defined in the *PFI Program Guide*), in a manner that is free from sources of influence and other factors that might reasonably be expected to compromise or have the appearance of compromising in any material respect their independence, professional judgment, integrity, objectivity, impartiality or professional skepticism in performing, rendering or delivering the same, or their ability to do so in a timely and professional manner in accordance with all applicable PFI Requirements (each a "Threat," and collectively, "Threats"), whether such Threats arise from actual, apparent or potential conflicts of interest, lack of independence from the Entity Under Investigation (and/or its associated personnel, representatives, contractors, professional advisors or agents) or otherwise.
- PFI Companies and PFI Employees must not enter into, accept or endure any agreement,

terms or other commitment, obligation or restriction (with the Entity Under Investigation or otherwise) that might reasonably be expected or perceived to (a) introduce (or increase the likelihood of introducing) any Threat into the PFI Investigation process or any PFI Report or (b) grant to the Entity Under Investigation or any other person or entity any right to modify or provide final approval with respect to the conclusions, judgements or findings of any PFI Report, delay or interfere with the performance of PFI Services, or restrict the PFI Company's access to employees or other resources of the Entity Under Investigation to which access is reasonably required or requested in order to enable the PFI Company to perform its PFI Services in accordance with all applicable PFI Program requirements.

- With respect to each PFI Investigation, the PFI Company must enter into a written agreement directly with the applicable Entity Under Investigation, which at a minimum: (a) expressly includes such terms and provisions as may be necessary, reasonable or appropriate, or otherwise required by PCI SSC for purposes of enabling the PFI Company and its PFI Employees to perform such PFI Investigation, and render and deliver all associated PFI Services, conclusions, findings and PFI Reports, in each case, in a professional, unfettered manner, without delay, and in accordance with all applicable PFI Requirements (including without limitation, the requirements specified in this Section 2.3 regarding independence, professional judgment, integrity, objectivity, impartiality and professional skepticism), and (b) establishes that such terms and provisions shall govern to the exclusion of any conflicting terms of any other provisions or agreements between or among the PFI Company, such Entity Under Investigation and/or any third party.
- PFI Companies and PFI Employees are not permitted to perform any PFI Investigation for any company, organization or other entity for which the PFI Company (or any then-current PFI Employee of such PFI Company) has performed, within the then preceding three (3) years, a PCI DSS Assessment, ASV Assessment or QIR Installation (as defined in the then-current version of (or successor document to) the *Payment Card Industry (PCI) Qualification Requirements for Qualified Integrators and Resellers (QIRs)* appearing on the Website).
- A PFI Company that has performed a PA-DSS Assessment, P2PE Assessment or 3-D Secure Assessment (as defined in the then-current version of (or successor document to) the *QSA Qualification Requirements For Payment Application Qualified Security Assessors (PA-QSA), Payment Card Industry (PCI) Qualification Requirements For Point-to-Point Encryption (P2PE)™ Qualified Security Assessors – QSA (P2PE)* and *PA-QSA (P2PE)* or *Payment Card Industry (PCI) 3-D Secure (PCI 3DS) Qualification Requirements for 3DS Assessors* (as applicable) appearing on the Website) of a product or solution that was involved in a given Security Issue is only permitted to assess the involvement of that product or solution as part of a PFI Investigation if the PFI Company ensures that the business unit and personnel utilized by such PFI Company 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 Company in connection with the PFI Investigation.
- PFI Companies and PFI Employees are not permitted to perform any PFI Investigation for any company, organization or other entity that is using any product, solution or service provided by or through the PFI Company or PFI Employee other than:
  - PFI Investigation services
  - Contract preparation

Note: *The provision of any service that may impact an Entity Under Investigation's PCI DSS compliance is deemed to violate these independence requirements.*

- Access to network configurations and plans
- Access to physical location maps and/or any relevant entry passes
- Inclusion and participation in incident-management exercises

- PFI Companies and PFI Employees must abstain from providing any service or advice to Entities Under Investigation that may violate independence, should a PFI Investigation be required; these may include (but are not limited to) services, changes, or advice relating to IT infrastructure, network hardening, endpoint protection, physical security or any PCI DSS requirement.

- PFI Companies may be engaged to perform services pertaining to the anticipated investigation outside of the PFI Region(s) for which they have been qualified by PCI SSC only with prior written consent of PCI SSC for each engagement for which there may be lack of available PFI Companies in the region.

2.4 Insurance Coverage

2.4.1 Requirements

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

2.4.2 Provisions

- Each PFI Company must provide to the Approving Organization an insurance certificate evidencing the above Professional Errors and Omissions coverage.
- The PFI Company 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 Company'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 PFI Companies.

Note: *In accordance with the QSA Qualification Requirements, the PFI Company must also provide to PCI SSC insurance proof-of-coverage statements covering all such subcontractors to demonstrate that insurance satisfying applicable insurance coverage requirements has been purchased and is maintained for all such subcontractors.*

2.5 PFI Company Fees

2.5.1 Requirement

Initial Processing Fees

Interested parties must contact PCI SSC at pfi@pcisecuritystandards.org to be issued the application processing fee invoice. The invoice will offer several payment methods, such as check, credit card or bank wire. The initial processing fees will be credited toward regional qualification fee(s) (see below) if/when the applicant is qualified as a PFI Company, except as provided below. Once payment is received, the primary contact will be granted access to the online PFI Company application.

Qualification and Renewal fees

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

- For the first year of qualification, the applicable initial regional PFI Company fees (per region) must be paid in full within 30 days of receipt of the invoice(s).
- For each subsequent year the applicable annual regional PFI Company renewal fee(s) 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 effective legal notice of a fee change. Failure to qualify as a PFI Company within 12 months of application submission will result in forfeiture of application and/or initial processing fees.*

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 Company and submitted to the Approving Organization as part of the completed PFI Application Package. Among other things, the PFI Addendum includes attestation by the candidate PFI Company that the candidate PFI Company has satisfied all applicable PFI Requirements.

3 PFI Company Capability Requirements

This Section addresses the minimum PFI Company capability requirements that each PFI Company must satisfy, and where applicable, the capability-related PFI Company information and materials that each candidate PFI Company must provide to the Approving Organization, in order to be qualified and maintain Good Standing as a PFI Company. As elsewhere in this document, the requirements and provisions below are necessary to establish and maintain Good Standing as a PFI Company and are in addition to the requirements and provisions of the QSA Program.

3.1 PFI Company – Experience

3.1.1 Requirements

At all times, the PFI Company must:

- 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 Company 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 Company 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 Company has been qualified.
- Ensure that it employs at least one (1) QSA Employee at all times on a full-time basis and requires the QSA Employee to review all technical aspects of all of its PFI Investigations.
- 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 Employee (defined in the *QSA Qualification Requirements For Payment Application Qualified Security Assessors (PA-QSA)*) that is in Good Standing as such is available to be assigned to each PFI Investigation, if needed.
- 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 such professional certifications 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 Company.
- Ensure that each PFI Employee stays up to date on current trends, threats and emerging technologies (for example, mobile, tokenization, cloud, etc.).
- Ensure that each PFI Employee 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/or PFI Employees in Good Standing, and
  - Reviewed by its QSA Employee.
- Only engage in—and only permit its PFI Employees to engage in—PFI Investigations with respect to which the PFI Company 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 Company is then qualified by PCI SSC and satisfies all corresponding regional PFI Program requirements (including but not limited to payment of applicable qualification and renewal fees) in accordance with applicable PFI Program requirements.
- Upon reasonable request of any Participating Payment Brand, attend requested 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 qualified as a PFI Company and maintain Good Standing as a PFI Company:

- Descriptions of the types of forensic examinations that the PFI Company (or candidate) has performed.
- At least two (2) redacted forensic investigation reports from within the last 18 months of multi-box environments, such as a website and server or point-of-sale device and interconnected card payment network. The reports must include, as a minimum, 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 merchants, service providers, financial institutions, or other entities for which the PFI Company (or candidate) has performed forensic security investigations within the 12 months prior to the PFI Company application date
- Proof of existing relationships with appropriate cyber-crime-oriented law enforcement agencies pertinent to each PFI Region for which the PFI Company (or candidate) has applied for qualification as a PFI Company (or has been qualified as a PFI Company)
- Documentation that the PFI Company (or candidate) employs a minimum of at least one (1) Core Forensic Investigator for each PFI Region for which the PFI Company (or candidate) has applied for qualification (or has been qualified) at all times (and initiates qualification procedures for all candidate Core Forensic Investigators at the time of the initial PFI Company application)

- Documentation that the PFI Company (or candidate) employs a minimum of one (1) QSA Employee at all times.
- List of PFI Company's language proficiencies
- Proof of substantial and appropriate knowledge and experience in investigating security breaches and compromises of data to enable the PFI Company (or candidate) 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 (or candidates) of the PFI Company (or candidate) 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 Company (or candidate) with respect to whom the PFI Company (or candidate) is seeking or has obtained qualification as a PFI Employee satisfies all PFI Employee requirements
- Annually, documentation that each PFI Employee of the PFI Company (or candidate) has successfully completed required PCI SSC training as well as annual training for incident response and computer forensics professionals such as renewal of certifications
- Prompt notice of any change to any of the information previously provided to the Approving Organization with respect to the PFI Company or any PFI Employee (or candidate, as applicable) thereof, as a result of which the Good Standing of such PFI Company or PFI Employee (or candidate) could reasonably come into question, or the PFI Company or PFI Employee (or candidate) could reasonably become ineligible for qualification under the PFI Program

3.2 PFI Company – Services

3.2.1 Requirements

Each PFI Company 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 a 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: *PFI Companies 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.*

- Employ at least one PCI SSC-qualified QSA Employee (in compliance with all requirements applicable to QSA Employees as set forth in the *QSA Qualification Requirements*) at all times.
- Initiate each PFI Investigation at the applicable Entity Under Investigation's facilities no later than five (5) business days after the date of execution of the applicable PFI Investigation services agreement between the PFI Company and such Entity Under Investigation.
- 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.
- Promptly notify PCI SSC of all changes to subject matter experts utilized by the PFI Company in connection with PFI Investigations.

3.2.2 Provisions

The PFI Company (or candidate) 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.

The PFI Company (or candidate) must provide to the Approving Organization a list of all subject matter experts that the PFI Company reasonably anticipates engaging to assist the PFI Company in the performance of its PFI Investigations (the "Subcontractor List").

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 Company (meaning this work cannot be subcontracted to non-employees, unless PCI SSC has given prior written consent for each 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 PCI SSC PFI Employee training annually
- Successfully complete annual training for incident response and computer forensics professionals such as renewal of certifications (in addition to any required PCI SSC training).
- Adhere to the PCI SSC Code of Professional Responsibility.
- 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 Company shall permit any of its subcontractors to include, any company logo or reference to a company other than the responsible PFI Company, 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 the PFI Qualification 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 Company (or candidate) is seeking qualification as a PFI Employee:

- Résumé
- 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 additional requirements, and the corresponding PFI Company 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 Company. Subcontracted resources are not permitted to fulfill this role.
- Operate in a role that is primarily as a forensic investigator within the applicable PFI Company'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

In addition to the items described in section 3.3.2, the following information must be provided to the Approving Organization with respect to each individual for whom the PFI Company (or candidate) is seeking qualification as a Core Forensic Investigator:

- Résumé 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 Company Administrative Requirements

This Section addresses the minimum PFI Company administrative requirements that each PFI Company must satisfy, and where applicable, the administrative PFI Company information and materials that each PFI Company (or candidate) must provide to the Approving Organization, in order to be qualified and maintain Good Standing as a PFI Company. These requirements and provisions are in addition to the requirements and provisions of the QSA Program.

4.1 Contact Person

4.1.1 Requirement

The PFI Company 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 Company'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 Company 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

4.2.1 Requirement

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

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

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

4.2.2 Provisions

The PFI Company (or candidate PFI Company) must provide PCI SSC with responses to each of the following:

- Attestation that its policies and hiring procedures include performing background checks: Examples of background checks include previous employment history, criminal record, credit history, and reference checks.
- A written statement that it successfully completed such background checks for each candidate PFI Employee.
- A summary description of current PFI personnel background check policies and procedures, which must require and include the following:
  - Verification of aliases (when applicable)
  - Comprehensive country and (if applicable) state level review of records of any criminal activity such as felony (or non-US equivalent) convictions or outstanding warrants, within the past five years minimum
  - Annual background checks consistent with this section for each of its PFI Employees for any change in criminal records, arrests or convictions

4.3 Adherence to PCI Procedures

Each PFI Company 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 Program Guide*.
- All PFI Reports are generated for each PFI Investigation.

4.3.1 Requirements

The PFI Company must prepare all PFI Reports 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 each case, in accordance with the *PFI Program Guide.*

4.4 Quality Assurance

4.4.1 Requirements

- Each PFI Company must have implemented a quality assurance program governing all aspects of PFI Investigations and related PFI Company 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 Company 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 Section 4.3 of the QSA Qualification Requirements).

- The PFI Company and each PFI Employee must adhere to all requirements and procedures of the aforementioned PFI Company 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 Company must provide a Feedback Report in the form attached hereto as Appendix C to each Entity Under Investigation (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 Company site visits for purposes of auditing the processes and procedures used by PFI Company in connection with PFI Investigations; and each PFI Company must comply with all such requests and provide PCI SSC with reasonable access for such purposes.

4.4.2 Provisions

- Each PFI Company (or candidate) 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, Entities Under Investigation or others, as applicable.
  - Sole responsibility for submitting PFI Reports to Participating Payment Brands, Entities Under Investigation or others, as applicable.
- Each PFI Company (or candidate) shall, upon request, provide to the Approving Organization a description of the contents of the PFI Company's quality assurance manual, to confirm that the manual addresses all aspects of the PFI Company'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 Company (or candidate) 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 Company or to cause the PFI Company to no longer be eligible for PFI Company qualification.
- 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 Qualification Requirements,* each PFI Company 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 Company (or candidate) 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 Company (or candidate) must provide to the Approving Organization a blank 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 Company (or candidate) 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 Company must:

- Prior to each PFI Investigation, pursuant to a written agreement directly with the applicable Entity Under Investigation, obtain from that Entity Under Investigation (a) full authorization to provide to each affected Participating Payment Brand (and, if the Entity Under Investigation is a merchant, the affected acquirer(s)), a copy of each PFI Report (and each version and portion thereof) resulting from such PFI Investigation, except to the extent prohibited by applicable law, and (b) such Entity Under Investigation's acknowledgement of the PFI Company's obligations pursuant to these PFI Qualification Requirements, including without limitation, the Independence Requirements set forth in Section 2.3 above.
- After each PFI Investigation, simultaneously with its delivery of each portion (excluding the Executive Summary) of the proposed Final PFI Report (and PIN Security Requirements Report, if applicable) resulting from such PFI Investigation to the Entity Under Investigation (or any contractor, representative, professional advisor, agent or affiliate thereof), deliver a copy thereof to each affected Participating Payment Brand (and, if the Entity Under Investigation is a merchant, each affected acquirer(s)), except to the extent prohibited by applicable law.
- After each PFI Investigation, simultaneous with its delivery of each complete proposed Final PFI Report (and PIN Security Requirements Report, if applicable) resulting from such PFI Investigation to the Entity Under Investigation (or any contractor, representative, professional advisor, agent or affiliate thereof), deliver a copy thereof to each affected Participating Payment Brand (and, if the Entity Under Investigation is a merchant, each affected acquirer(s)), except to the extent prohibited by applicable law.
- Follow the PFI Guidelines and utilize the incident report templates as outlined in the *PFI Program Guide*, for all PFI Investigations.
- Participate in all discussions of the PFI Investigation as reasonably requested by the Entity Under Investigation, the affected acquirer(s) if the Entity Under Investigation is a merchant, and/or the affected Participating Payment Brands.
- Ensure and certify in each Final PFI Report that each PFI Investigation has been conducted strictly in accordance with all applicable PFI Requirements (including without limitation, the Independence Requirements provided for in Section 2.3 above).
- Ensure and certify in each Final PFI Report that the judgments, conclusions and findings therein:
    - accurately reflect, include and are based solely upon the factual evidence as gathered, discovered and determined to be relevant to the PFI Investigation by the PFI Company in its sole discretion during the course of that PFI Investigation
    - reflect the independent judgments, findings and conclusions of the PFI Company and its PFI Employees only, acting in their sole discretion; and
    - were not in any manner influenced, directed, controlled, modified, provided or subjected to any prior approval by the subject Entity Under Investigation, any contractor, representative, professional advisor, agent or affiliate thereof, or any other person or entity other than the PFI Company and its PFI Employees.

- Upon request of any affected Participating Payment Brand, promptly 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 Company, 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 Company (or candidate) must provide to the Approving Organization evidence acceptable to the Approving Organization that the PFI Company meets the requirements of Section 4.6.1 above.

5 PFI Annual Renewal

5.1 Requirements

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

5.2 Provisions

The following must be provided to PCI SSC and/or will be considered during the renewal process for both PFI Companies 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 Entities Under Investigation that have undergone PFI Investigation by the PFI Company, as well as Approving Organization(s) and Participating Payment Brands.

Appendix A: PFI Application Checklist

Note: Failure to successfully qualify as a PFI Company within 12 months of initial application submission will result in forfeiture of all PFI Program application and initial processing fees and closure of the application.

Requirement		Information/Documentation Needed
Business Requirements	☐	The candidate PFI Company must be a QSA Company in Good Standing (e.g., not in remediation or delinquent on fees).
	☐	PFI Addendum signed in unmodified form by a duly authorized officer of the candidate PFI Company.
Independence	☐	Description of the candidate PFI's practices to maintain independence.
Insurance Coverage *May vary based on geographic region and applicable law.*	☐	Insurance certificate evidencing minimum coverage level of $5,000,000 USD for Professional Errors and Omissions.
	☐	Insurance certificate(s) evidencing all other required insurance coverage levels in accordance with the QSA Qualification 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 Company qualification.
PFI Experience and Service	☐	Summary description and samples of the types of forensic examinations it has performed.
	☐	Two independent references regarding the candidate PFI Company from forensic security engagements it has performed within the prior 12 months.
	☐	Documentation that the candidate PFI Company employs a minimum of one (1) fulltime QSA Employee at all times.
	☐	Documentation that the candidate PFI Company employs a minimum of one (1) Core Forensic Investigator for each PFI Region for which the candidate is seeking PFI Company qualification.
	☐	Documentation that the candidate PFI Company 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 Company maintains appropriate equipment and storage facilities for use in the event of an incident response request.
	☐	Documentation that the candidate PFI Company can ensure that a PA-QSA Employee (in Good Standing as such) is available to be assigned to each PFI Investigation.

Requirement	Information/Documentation Needed	
PFI Employee Skills and Experience	☐	Résumés for all candidate 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 industry-recognized incident response certification for each PFI Employee, such as 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.
	☐	Background check procedure and policy attestation as required in section 4.2.2, including: • Attestation that its policies and hiring procedures include performing background checks. • A summary description of current PFI personnel background check policies and procedures.
PFI QA Program	☐	Designation of Quality Assurance Manager.
	☐	Description of contents of the candidate PFI Company's quality assurance manual.
Evidence Handling	☐	Copies of the candidate PFI Company's policies and procedures regarding evidence handling, preservation, integrity and collection, along with associated standard form of employee acknowledgement.
	☐	Evidence of candidate PFI Employees' proficiency in using the candidate PFI's forensic investigation tools (such as copies of relevant certifications or evidence of training).

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 Applicant ("Applicant" or "Company") as of the date of PCI SSC's signature below (the "Addendum Effective Date"), for purposes of adding and modifying certain terms of the *Qualified Security Assessor (QSA) Agreement* between PCI SSC and Company dated as of the QSA Agreement Date below, as in effect as of the Addendum Effective Date (the "Agreement").

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 Duly Authorized 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. While this Addendum is in effect:

1. Capitalized terms defined in this Addendum shall have the meanings ascribed to them herein for all purposes of this Addendum and the Agreement.
2. Capitalized terms used in this Addendum without definition shall have the meanings ascribed to them in or pursuant to the Agreement, the *PFI Qualification Requirements*, or the *PFI Program Guide,* as applicable.
3. The following terms shall have the following meanings:
    a) "PFI Documents" means the *PFI Qualification Requirements* and the *PFI Program Guide*.
    b) "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 Entities Under Investigation in connection with this Addendum and/or the PFI Program.
    c) "*PFI Qualification Requirements*" means the then-current versions of the *Payment Card Industry (PCI) Data Security Standard* and the *QSA Qualification Requirements for PCI Forensic Investigators (PFIs)* (or successor document thereto), as made publicly available by PCI SSC.
    d) "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 "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.
4. Intending to broaden and not otherwise modify or limit any of the definitions of the terms appearing in the Agreement, the following terms appearing in the Agreement are hereby amended as follows:
    a) The term "Services" shall also include the PFI Services.
    b) The term "QSA Requirements" shall also include the PFI Company requirements.
    c) The term "QSA Qualification 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.
    f) The term "PCI SSC Assessment" shall also include PFI Investigations.
    g) The term "QSA Company client" shall also include Entities Under Investigation.

B. PFI Services. Subject to the terms and conditions of the Agreement, this Addendum and the PFI Documents, for PFI Program purposes, while Company is in Good Standing as a PFI Company (or in compliance with the terms of PFI Program remediation), PCI SSC hereby qualifies Company to conduct PFI Investigations of Entities Under Investigation 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 qualified as a PFI and is in compliance with all applicable regional PFI Program requirements (including but not limited to fee payments).

Company agrees to monitor the Website at least weekly for changes to the PFI Documents and to 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 comply with and perform each PFI Investigation in strict compliance with all PFI Requirements, including but not limited to, the requirements set forth in the PFI Documents 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 SSC Standards.

D. Subcontractors.

1. Notwithstanding anything to the contrary in the Agreement, 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 (a) Company shall be primarily responsible and liable for the performance of all services by such subcontractors in connection with such PFI Investigations; (b) Company 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; (c) in the event PCI SSC notifies Company of its rejection of any such subcontractor, Company shall immediately cease its use of such subcontractor in connection with such PFI Investigation; (d) Company shall not use any subcontractor for a given PFI Investigation of a given Entity Under Investigation if such subcontractor or any employee thereof is an Affiliate or employee of such Entity Under Investigation or any Affiliate thereof; and (e) Company shall only use subcontractors appearing on its then-current Subcontractor List if possible under the circumstances.
2. Upon notification by Company of any change to its Subcontractor List, Company's Subcontractor List will be deemed to have been updated accordingly. PCI SSC reserves the right to remove any subcontractor from such 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, such Subcontractor List will be deemed to have been updated accordingly.

4. PFI List; Promotional References; Restrictions

A. So long as Company is in Good Standing as a PFI Company or in compliance with PFI Program remediation, PCI SSC may, in its sole discretion, identify Company as a PFI on the PFI List (as defined in the *PFI Qualification Requirements*) 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 qualification status information and details (including without limitation, qualification, suspension, remediation, or revocation status).

B. So long as Company is in Good Standing as a PFI Company or in compliance with PFI Program remediation and 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.

5. Quality Assurance

A. To the extent any data or other information obtained or generated by Company relating to any Entity Under Investigation in the course of providing PFI Services thereto may be subject to any confidentiality restrictions between Company and such Entity Under Investigation, Company must provide in each agreement containing such restrictions (and in the absence of any such agreement must agree with such Entity Under Investigation 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, the Agreement and this Addendum.

B. Company hereby acknowledges and agrees that, as further described in Section 4 of the *PFI Program Guide,* as part of its PFI Program quality assurance process PCI SSC periodically reviews submitted Feedback Reports, and that Company's ongoing status as a PFI ultimately depends (among other things) on the feedback and scores received by PCI SSC in connection with those reviews. Company agrees that all decisions of PCI SSC regarding the PFI Program, participation therein, and any conflict between or among relevant PCI SSC Program documents are final, binding, and made in the sole discretion of PCI SSC, including without limitation, decisions regarding qualification, PFI listing and delisting, weighing and criteria for Feedback Reports, remediation and revocation procedures and requirements, and all other PFI Program matters.

6. Term and Termination

A. Term

This Addendum shall become effective as of the Addendum Effective Date and, unless earlier terminated in accordance with the Agreement, 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 qualification and re-qualification requirements for each such one-year term. This Addendum shall immediately terminate upon termination of the Agreement and as otherwise specified in the Agreement.

B. 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 and performing all PFI Services, provided that, if and to the extent instructed by PCI SSC in writing, Company shall

complete any and all PFI Services for which Company was engaged prior to such expiration or termination; (iv) to the extent Company is instructed to complete any PFI Services pursuant to preceding clause (iii), Company will deliver all corresponding outstanding PFI Reports to the required recipients as required pursuant to the PFI Documents, the Agreement and this Addendum and any applicable provisions of Company's agreement with the applicable Entity Under Investigation, and shall remain responsible after such expiration or 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) if requested by PCI SSC, Company shall obtain (at Company's sole cost and expense) the services of a replacement PFI Company acceptable to PCI SSC for purposes of completing those PFI Services for which Company was engaged prior to such expiration or termination but which Company has not been instructed to complete pursuant to clause (iii) above; (vi) Company shall return or destroy, in accordance with the terms of Section A.6 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; (vii) Company shall, within fifteen (15) days of PCI SSC's written request, in a manner acceptable to PCI SSC, notify those of its Entities Under Investigation with which Company is then engaged to perform PFI Investigations or other PFI Services of such expiration or termination; and (viii) notwithstanding anything to the contrary in this Addendum, the Agreement, or elsewhere, PCI SSC may notify any of its Members and any acquirers, Entities Under Investigation, or others of such expiration or termination and the reason(s) therefore. The provisions of this Section shall survive the expiration or termination of this Addendum for any or no reason.

7. 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.

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 or hereafter in accordance with its terms, the Agreement, as modified and in effect immediately prior to the effectiveness of this Addendum, 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 company ("PFI" or "PFI Company") 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 Company. 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 postal mail to:*

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

All responses are optional and this form may be submitted anonymously and should be completed in English.

Contact Information

Feedback Participant	
Company name	
Contact name	
Telephone	
E-mail	
PFI Company	
Company name	
PFI Employee(s) 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 rating 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).*

Feedback Area		Response
***Timeliness:** Please rate the PFI Company's performance relative to your own expectations prior to the PFI Investigation.*		
1	Primary and preliminary reports were delivered within an appropriate timeframe.	Rating
	Comments:	
2	Regular status updates were provided by the PFI Company as required by involved Participating Payment Brand(s).	Rating
	Comments:	
3	The PFI Company supplied resources for this engagement sufficient to enable adherence to agreed-upon timelines for the investigation.	Rating
	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.	Rating
	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. ***Note:** Arrival time may depend on the geographic location of the trouble site, weather conditions, available transportation and other issues.*	Rating
	Comments:	
6	The PFI Company provided at-risk account numbers in a timely fashion.	Rating
	Comments:	
***Accuracy:** In assessing Accuracy, consider whether or not there were instances where you believe the PFI Company 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*).	Rating
	Comments:	

Feedback Area		Response
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).	Rating
	Comments:	
Ethics: *In assessing Ethics, consider whether or not there were situations in which you believe the PFI Company 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 PFI Companies and QSA Companies throughout the PFI Investigation (See Section 2.3 of the *PFI Qualification Requirements* and Section 2.2 of the *QSA Qualification Requirements*) and was not the same QSA Company that conducted the initial or any subsequent PCI DSS Assessment of the Entity Under Investigation.	Rating
	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.	Rating
	Comments:	
Cooperation: *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.	Rating
	Comments:	
2	The PFI Company was regularly and readily available for communication with the affected Participating Payment Brand(s) and their client(s).	Rating
	Comments:	
3	The PFI Company assigned an appropriately qualified Lead Investigator to respond to and address issues with affected Participating Payment Brands and the investigated organization throughout the PFI Investigation.	Rating
	Comments:	
4	The PFI Company clearly identified any extenuating circumstances that impacted the investigation	Rating
	Comments:	

Feedback Area		Response
Competence: *In assessing Competence, consider whether or not the PFI Company 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	Rating
	Comments:	
2	The PFI Company investigators were articulate in communicating the investigative findings.	Rating
	Comments:	
3	The PFI Company demonstrated sufficient understanding of the PCI DSS and the PA-DSS (if applicable).	Rating
	Comments:	
4	The PFI Company clearly understood how to scope the PFI Investigation.	Rating
	Comments:	
Reporting: *Please assess the PFI's performance relating to the following:*		
1	The PFI Company adhered to all PFI Report templates.	Rating
	Comments:	
2	All final PFI Reports provided adequate content and data that clearly tied the conclusion back to the evidence.	Rating
	Comments:	

Appendix D: Terminology

The terms set forth in this section, when used in this document, shall have the meanings set forth in this section, regardless of whether capitalized. When used but not defined in the *PFI Qualification Requirements,* each term defined in *the PFI Program Guide*, *QSA Qualification Requirements,* or *QSA Agreement* shall have the corresponding meaning ascribed to it in the first of the *PFI Program Guide*, *QSA Qualification Requirements,* or *QSA Agreement* (taken in that order) to define such term.

Term	Meaning
PCI 3-D Secure Assessor (or 3DS Assessor)	A QSA Company that provides services to 3-D Secure Core Component vendors in order to validate such vendors' 3-D Secure Components adhere to the requirements of the *PCI 3DS Core Security Standard* and that has satisfied and continues to satisfy all requirements applicable to PCI 3DS Assessors (or is in compliance with remediation under the PCI 3DS Program), as described in the *Payment Card Industry (PCI) 3-D Secure (PCI 3DS) Qualification Requirements for 3DS Assessors*.
PCI 3DS Core Security Standard	The then-current versions of (or successor documents to) the *Payment Card Industry 3-D Secure (PCI 3DS) Security Requirements and Assessment Procedures for EMV® 3-D Secure Core Components: ACS, DS, and 3DS Server* 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.
Approving Organization	PCI SSC, or such other organization as PCI SSC may from time to time designate to review and qualify entities as PFIs for purposes of participation in the PFI Program.
ASV Assessment	An information security vulnerability assessment performed by a PCI SSC-qualified Approved Scanning Vendor in accordance with the *PCI SSC Qualification Requirements for Approved Scanning Vendors (ASV)* or successor document thereto.
Cardholder Data	Defined in the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms*.
Entity Under Investigation	Defined in the *PFI Program Guide*.
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 Company, that the PFI Company is in Good Standing as a QSA Company (as described in the QSA Qualification Requirements), the PFI Company's PFI qualification has not been revoked, terminated, suspended, cancelled, or withdrawn, the PFI Company is in compliance with all PFI Company requirements, and the PFI Company 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 Company's QSA Agreement or PFI Addendum, or any other agreement with PCI SSC; and (b) With respect to a given PFI Employee, that the PFI Employee is in compliance with all PFI Employee requirements.

Term	Meaning
Industry Rules	Defined in Section 1.1 of the *PFI Program Guide*.
Lead Investigator	With respect to a given PFI Investigation, a Core Forensic Investigator designated by the applicable PFI Company to lead that PFI Investigation.
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 (or is in compliance with remediation under the PA-DSS Program), as described in the *QSA Qualification Requirements For Payment Application Qualified Security Assessors (PA-QSA)*.
Participating Payment Brand	Defined in the *QSA Agreement*.
PFI Company (or PFI)	A PCI Forensic Investigator Company, as defined in the *PFI Program Guide*.
PFI Addendum	An addendum to the QSA Agreement in the form attached hereto as *Appendix B*.
PFI Company requirements	The requirements applicable to PFI Companies and the provisions required of PFI Companies as set out in the *PFI Qualification Requirements* and *PFI Program Guide*, and such additional requirements as PCI SSC may establish for PFI Companies from time to time in connection with the PFI Program.
PFI Employee	A full-time employee of a PFI Company who has been qualified 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, 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	Defined in the *PFI Program Guide*.
PFI Program	The PCI Forensic Investigator Program as managed by PCI SSC and as further described herein and in the *PFI Program Guide*.

Term	Meaning
PFI Program Guide	The then-current version of the *Payment Card Industry (PCI) Forensic Investigator (PFI) Program Guide* (or successor document thereto), as made publicly available by PCI SSC.
PFI Qualification Requirements	The then-current version of this *Qualification Requirements for PCI Forensic Investigators (PFIs)* (or successor document thereto), as made publicly available by PCI SSC on the Website.
PFI Region	With respect to a given PFI Company, a geographical region (as identified in Appendix B hereto) with respect to which such PFI Company has been and is qualified to perform PFI Investigations as part of the PFI Program and satisfies all applicable PFI Company Requirements (including but not limited to payment of all applicable regional qualification and renewal fees).
PFI Reports	Defined in Section 3.3 of the *PFI Program Guide* (see also Section 4.3.1).
PFI Requirements	Collectively, the PFI Company requirements and the PFI Employee requirements.
Qualified Integrators and Reseller (or QIR)	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 on the Website and amended by PCI SSC from time to time in its sole discretion, including but not limited to, all supplements and addenda thereto.
Security Issue	Defined in the *PFI Program Guide*.
Website	Refers to the PCI SSC website at www.pcisecuritystandards.org.