Payment Card Industry (PCI)

# PCI Forensic Investigator (PFI)

## Program Guide

**Version 2.1**

.

.

## Document Changes

| Date | Version | Description |
|---|---|---|
| November 2012 | 2.0 | Amendments to support remote forensic investigations and minor administrative revisions |
| May 2014 | 2.1 | Minor revision to support revised report templates |

.

# Table of Contents

# 1 Introduction

This document provides an overview of the PCI Forensic Investigator Program ("PFI Program") operated and managed by PCI Security Standards Council, LLC ("PCI SSC"), and should be read in conjunction with the *PFI Supplement* and the *QSA Validation Requirements* (defined in *Appendix C* hereto), and the other documents referenced in Section 1.4 below. This document describes the following:

- PFI Program Background
- PFI Approval
- PFI Program Roles and Responsibilities
- PFI Investigations
- PFI Quality Assurance Program

For purposes of this document, terms used herein and defined in *Appendix C* hereto shall have the meanings set forth in *Appendix C*. All other terms used in this document without definition, if defined in the *PFI Supplement* or the *QSA Validation Requirements* shall have the meanings ascribed to them in the *PFI Supplement* or the *QSA Validation Requirements*, as applicable.

## 1.1 Background

To help ensure the security of cardholder data, entities that process, store or transmit cardholder data may be required to comply with PCI Standards (defined in *Appendix C* hereto) by applicable payment card industry rules and requirements of acquirers, issuers and/or Participating Payment Brands ("Industry Rules").

Additionally, in the event of a Security Issue (defined in *Appendix C* hereto), affected Compromised Entities may be required in accordance with applicable Industry Rules to notify their acquiring banks and/or affected Participating Payment Brands, and may be required to engage forensic investigators approved as part of the PFI Program to investigate the Security Issue, determine root cause, and report back to affected Participating Payment Brands and others. Such forensic investigations can be complex, challenging, and require the forensic investigator to possess highly specialized skills, proven staff and experience, and the ability to provide rapid and potentially global response.

## 1.2 PFI Program Overview

### *1.2.1 General*

Prior to the PFI Program, rules and requirements regarding eligibility, selection and performance of forensic investigators were often complicated and cumbersome, especially where multiple acquirers, issuers and/or Participating Payment Brands were involved.

The PFI Program reflects a simplification by PCI SSC of processes for identifying and engaging investigators to perform forensic investigations, streamlining the actual investigation requirements as well as related data and reporting requirements.

### *1.2.2 PFI Approval Process*

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 and in accordance with industry expectations, companies and individuals desiring to perform PFI Investigations must first be approved as PFIs or PFI employees (as applicable), and then must maintain that approval in Good Standing. Eligible candidate PFI companies may apply for PFI approval only during open enrollment periods determined by needs assessments performed by

PCI SSC on a periodic basis. Interested companies are encouraged to confirm open enrollment by contacting PCI SSC prior to submitting an application.

PFI approval involves: (a) initial eligibility and approval reviews, including provision of application and supplemental materials, as well as interviews of key PFI employees, (b) ongoing satisfaction of applicable PFI Validation Requirements and (c) annual renewal. Companies approved as PFIs are identified on the list of PCI Forensic Investigators maintained on the Website for a period of one (1) year from the date of their last PFI Program approval (or renewal).

Please refer to the *PFI Supplement* to review applicable PFI Validation Requirements and for specific information regarding approval as a PFI or PFI employee.

## 1.3 Fees

Fees to participate as a PFI in the PFI Program are specified *on the Website*.

Pricing and fees charged by PFIs for the services they provide to customers in connection with PFI Investigations are negotiated directly between the PFI and the applicable customer. Fees and pricing for PFI Investigations and related services of PFIs are not set by PCI SSC, and PCI SSC is not involved in any way with such fees or pricing.

## 1.4 Related Publications

The Payment Card Industry (PCI) PCI Forensic Investigator (PFI) Program Guide (the "PFI Program Guide") should be used in conjunction with the latest versions of the following other PCI SSC publications, each as available through the Website and further identified in Appendix C.

- *PFI Supplement*, which describes the requirements that must be satisfied by interested entities and individuals in order to participate in the PFI Program
- *QSA Validation Requirements*, which defines requirements that must be satisfied by all QSAs in order to perform QSA Assessments
- *PA-QSA Validation Requirements*, which defines specific additional requirements that must be satisfied by all PA-QSAs in order to assess payment applications under PCI SSC's PA-QSA program
- *PCI DSS*, which sets the foundation for other PCI Standards and related requirements
- *PCI DSS Glossary of Terms, Abbreviations, and Acronyms*
- *PA-DSS*, which defines the specific technical requirements and provides the related assessment procedures and templates used to validate payment application compliance and document the validation process
- *P2PE Standard,* which defines the specific technical requirements and provides the assessment procedures used to validate point-to-point encryption solutions

## 1.5 Updates to Documents and Security Requirements

Security is a never-ending race against potential attackers. As a result, PCI SSC regularly reviews, updates and improves the PCI Standards and related guidelines and requirements. PCI SSC reserves the right to modify, amend or withdraw any of its standards, guidelines or requirements at any time, and endeavours to work with interested industry stakeholders to help minimize the impact of such changes.

# 2 PFI Program Roles and Responsibilities

Information regarding Security Issues may come from a variety of sources, including but not limited to issuers, acquirers, law enforcement, Participating Payment Brands and the Compromised Entities that are themselves the subject of those Securities Issues.

At a high level, the roles and responsibilities of the various stakeholders in the PFI Program community are as follows:

## 2.1 Compromised Entity

In accordance with applicable Industry Rules, Compromised Entities are generally responsible for (without limitation) the following:

- Retaining evidence of compromise
- Acquiring the services of a PFI in the timeline required by affected Participating Payment Brands
- Cooperating with the PFI, acquirer, and/or Participating Payment Brand during the PFI Investigation
- Allowing the PFI to drive the PFI Investigation
- Participating in discussions with affected Participating Payment Brands and the PFI
- Resolving any security weaknesses identified by the PFI and/or any affected Participating Payment Brand
- Notifying acquirers and Participating Payment Brands
- Notifying and working with law enforcement as applicable

## 2.2 Participating Payment Brands

Each of the Payment Card Brands, individually, is responsible for developing and enforcing its own programs regarding when and how PFI Investigation may be required, including, but not limited to:

- Defining requirements regarding the use of PFIs and the disclosure, investigation and resolution of Security Issues
- Enforcement of requirements relating to forensic investigation
- Fines and/or penalties relating to cardholder data compromise
- Reserving the right to directly engage a PFI as it deems necessary
- Determining whether on-site attendance of a PFI at the Compromised Entity is necessary

## 2.3 PCI SSC

As part of its activities, PCI SSC engages in activities, including but not limited to, the following:

- Maintains the PCI Standards
- Operates and manages the PFI Program and either approves eligible entities and individuals to participate in the PFI Program as PFIs or PFI employees, as applicable, or designates an Approving Organization for such purpose
- Performs quality assurance (QA) reviews of PFIs
- Provides training and information regarding the PCI Standards and PCI SSC programs, including the PFI Program

***Note:*** *Except as specified in connection with the PFI QA Program, PCI SSC is not involved in the following:*

- *Acceptance and/or management of PFI Reports (defined in Section 3.3 below)*
- *Detailed review of PFI Reports*
- *Disclosure or investigation of actual or suspected cardholder data compromises*

## 2.4 PCI Forensic Investigators

PCI Forensic Investigators ("PFIs") are companies, organizations or other legal entities that are in compliance with all PFI company requirements (defined in the *PFI Supplement*) and have been approved as PFIs by PCI SSC (or another Approving Organization, as described in the *PFI Supplement*) for purposes of performing PFI Investigations.

Only PFIs approved by an Approving Organization and who are in PFI Good Standing are permitted to perform PFI Investigations, and then only in the specific PFI Regions for which they have been approved by PCI SSC. All approved PFIs are listed on the Website with applicable PFI Region(s).

***Note:*** *Not all QSAs are PFIs. In order to be approved as a PFI, an entity must already be qualified as a QSA, and then must satisfy additional requirements applicable to PFIs as set forth in the PFI Supplement.*

PFI responsibilities generally include (without limitation) the following:

- Driving and performing all aspects of PFI Investigations
- Verifying that the work product generated in connection with their PFI Investigations ("PFI Work Product") addresses all PFI Investigation procedure steps
- Strictly complying with the Forensic Investigation Guidelines attached as *Appendix A* hereto (the "PFI Guidelines")
- Strictly complying with evidence handling as further described below
- Investigation reporting and delivery of applicable PFI Reports as further described below
- Participating with the applicable Compromised Entities and affected Participating Payment Brands and (if applicable) acquirers in discussions regarding PFI Investigations in which they are involved and related Security Issues

# 3 PFI Investigations

## 3.1 General Requirements

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. Once approved through the PFI Program (and while in Good Standing as a PFI thereafter), a PFI is only 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.

## 3.2 Investigation Reporting

In accordance with applicable Industry Rules, the following reports must be produced as part of each PFI Investigation:

- ***Preliminary Incident Response Report*.** The current version of this template is available on the Website and must be completed by the PFI at the beginning of each PFI Investigation. Each completed Preliminary Incident Response Report must be delivered to each affected Participating Payment Brand, the applicable Compromised Entity, and such Compromised Entity's affected acquirer(s) (if the Compromised Entity is a merchant), in each case no later than five (5) business days after beginning PFI Investigation review of such Compromised Entity.
- ***Final Incident Report*.** A *Final Incident Report* must be completed by an approved PFI upon completion of each PFI Investigation. There are two versions of this template (referred to herein as a "Final PFI Report") available on the Website.. The *Final Incident Report for Remote Investigations* may be used where the investigation has been completed without the PFI attending onsite at the Compromised Entity. Each completed Final Incident Report must be delivered to each affected Participating Payment Brand, the applicable Compromised Entity, and such Compromised Entity's affected acquirer(s) (if the Compromised Entity is a merchant), in each case no later than ten (10) business days after completion of the PFI's review of such Compromised Entity.
- ***PIN Security Requirements Report*.** The current version of this template is available on the Website and must be completed by an approved PFI upon completion of each PFI Investigation in cases where PIN block or PIN data was compromised. Completed PIN Security Requirements Reports must be delivered to each affected Participating Payment Brand, the applicable Compromised Entity, and such Compromised Entity's affected acquirer(s) (if the Compromised Entity is a merchant), in each case no later than ten (10) business days after completion of the PFI's review of such Compromised Entity.
- ***Monthly Status Reports*.** On a monthly basis, each PFI must deliver to each Participating Payment Brand a detailed report of all of the PFI's ongoing PFI Investigations where such Participating Payment Brand is involved, including information regarding malware hashes, bad IPs and such other information as the affected Participating Payment Brand may reasonably request. If PCI SSC has specified a template for such reports, each PFI must utilize such template for all such reports.

- ***Trending Analysis Reports*.** On an annual basis or in such other interval as PCI SSC may specify from time to time, each PFI shall provide to PCI SSC and each Participating Payment Brand a trending analysis report, highlighting trends regarding PCI DSS compliance, method of compromise and such other information as PCI SSC may reasonably request from time to time. If PCI SSC has specified a template for such reports, each PFI must utilize such template for all such reports.

## 3.3 Delivery of Reports

In accordance with applicable Industry Rules, each PFI is responsible for secure and timely delivery of its Final Incident Reports, PIN Security Requirements Reports (if applicable), Preliminary Incident Response Reports, and all other reports required of PFIs in accordance with the PFI Program (such reports, collectively, "PFI Reports") to the recipients specified above. PFIs must work with the Compromised Entity and affected Participating Payment Brands to determine precisely how PFI Reports will be delivered, and in general, PFI Reports are to be sent via secure means including electronic transmission via secure connection (SFTP, SSL, etc.) and/or encryption (e.g., using PGP via e-mail or other mutually accepted security measures) of the PFI Report file before sending via insecure connection.

***Note**: All PFI Reports are subject to review and acceptance by the Participating Payment Brands and may be rejected if they do not meet all applicable requirements including, but not limited to, conformance to applicable PFI Report templates and scoping methodology. As part of such review, where appropriate, PFIs may be required to demonstrate relevant subject matter knowledge, including without limitation, knowledge in key-management and PIN compromise investigation where applicable. PFIs must revise and resubmit all rejected PFI Reports, and resolve all associated discrepancies with affected Participating Payment Brands, acquirers, and the Compromised Entity, in a timely manner. Final Incident Reports will not be considered to be accepted until approved in writing by all affected Participating Payment Brands and, if applicable, the Compromised Entity's acquirers.*

As described further herein, as part of the PCI SSC QA process, PFIs may be required to provide Participating Payment Brands with additional materials and information, including but not limited to draft PFI Reports and related work papers. Additionally, as described further in Section 4.4 below, as part of the PFI QA process, PCI SSC may audit the PFIs site.

In order to ensure that PFIs have all requisite authority to provide materials and information (including but not limited to final and draft PFI Reports and work papers) as described above, before beginning each PFI Investigation engagement, the PFI must inform the Compromised Entity that it shall be required to disclose the same as herein described and must obtain clear, unqualified permission and consent from the Compromised Entity to make such disclosures.

## 3.4 Evidence Handling

Each PFI must comply with the evidence-handling guidelines attached hereto as *Appendix B: Evidence Handling*.

# 4 PFI Quality Assurance Program

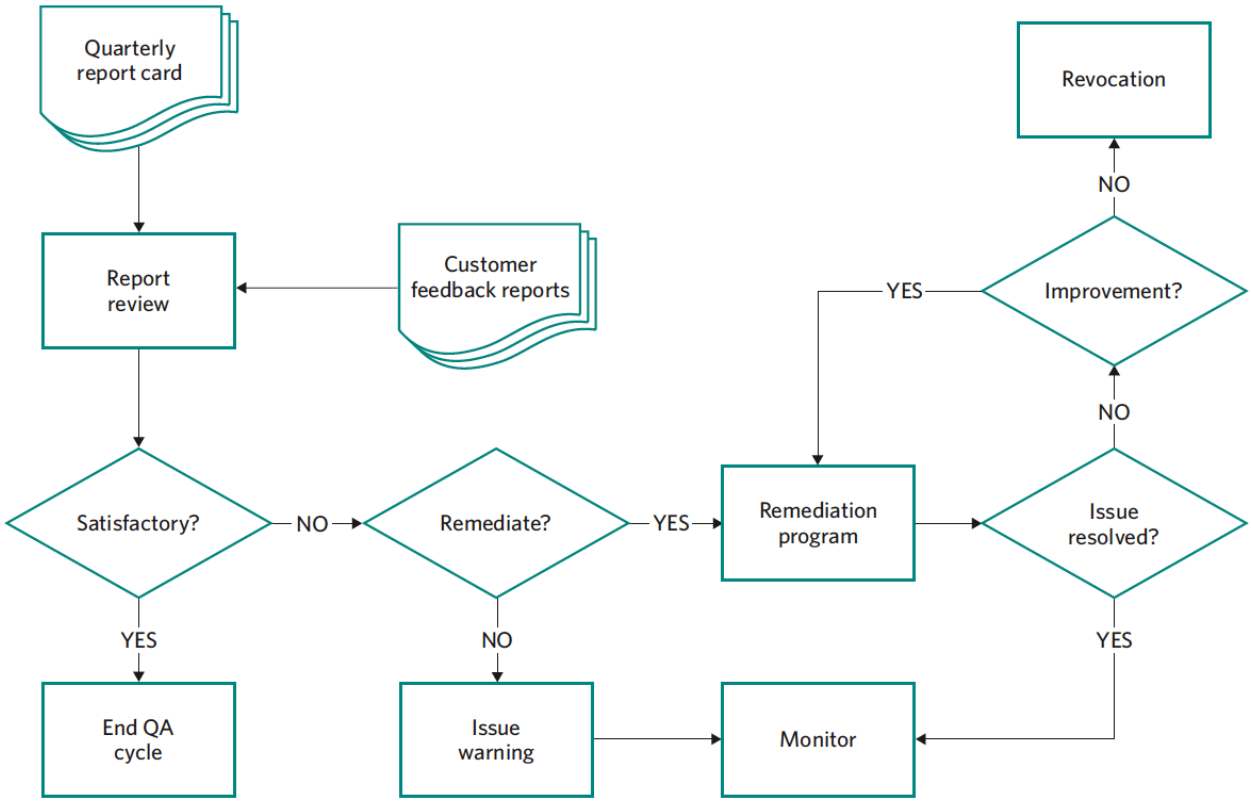
## 4.1 Overview

The goal of the PCI SSC PFI Quality Assurance Program ("PFI QA Program" or "QA") is to help ensure that PFIs and PFI employees comply with the PFI Validation Requirements, comply with the PFI's documented processes and procedures for PFI Investigations, and continually meet and produce PFI Work Product and related PFI Reports that meets or exceeds applicable PFI Program requirements.

PCI SSC seeks to achieve the above goal through its Feedback Process, PFI QA Program Audits and PFI Remediation Program, each described further below.

The QA Program collects feedback on PFI performance from the Participating Payment Brands and Compromised Entities. This feedback is assessed to determine if the PFI's performance is meeting the expected quality levels. So long as PCI SSC determines in its reasonable discretion that a PFI continues to satisfy applicable PFI Validation Requirements and meets prescribed quality levels for PFI Reports and related PFI services, that PFI will remain in Good Standing (defined in the *PFI Supplement*) as a PFI. Failure to satisfy applicable requirements or meet prescribed quality levels may result in any or all of the actions described in Section 4.4 below.

***QA Program Phases***



## 4.2 Feedback Process

### *4.2.1 Customer Feedback Reports and PFI Report Cards*

Following each PFI Investigation, the PFI must request that the applicable Compromised Entity and, if applicable, each affected acquirer, submit to PCI SSC a "Feedback Report" in the form attached as *Appendix D* to the *PFI Supplement*. Additionally, at the end of each quarterly review period (and more frequently if the PFI is in remediation), each Participating Payment Brand is asked to submit to PCI SSC a completed PFI Report Card in the form attached hereto as *Appendix D* for each PFI that completed a corresponding PFI Investigation during the relevant assessment period relating to a Security Issue that affected that Participating Payment Brand. Both of these feedback mechanisms address the following and other matters:

- Adherence to PFI Report templates;
- Adequacy of PFI Report content;
- Responsiveness to questions of affected Participating Payment Brands and others;
- Ability to meet applicable timelines in connection with compromise events;
- Adequacy of number of staff assigned to PFI Investigations;
- Competence of staff assigned to PFI Investigations;
- Adequacy of staff coverage across multiple events to meet event management timelines;
- Adherence to forensic scope;
- Ability to effectively communicate findings during forensic calls with Participating Payment Brands; and
- Being prepared with facts and evidence during conference calls.

### *4.2.2 Reviews and Scoring*

PCI SSC periodically reviews all Feedback Reports and PFI Report Cards, aggregates scores by PFI and question category, and notifies applicable PFIs if quality assurance issues arise.

Responses to questions in the PFI Report Card are provided on the following 4-point scale:

- Exceeds Expectations (4 points);
- Meets Expectations (3 points);
- Needs Improvement (2 points); or
- Unsatisfactory (1 point)

PFI Report Cards are organized into 6 separate sections, each of which contains several specific questions. For a given review period, question scores for each PFI Report Card section received for a given PFI are averaged, generating aggregated average scores for the PFI for each of the 6 PFI Report Card sections. As part of the QA process, PCI SSC then reviews these scores and takes appropriate action depending on the scores for the applicable review period, as follows:

- Warning (See Section 4.4 below): The PFI may be issued a warning if any aggregated average section score for a given review period falls between 2 and 3.

- Remediation (See Section 4.4 below): The PFI will be required to engage in remediation if either:
  - Any aggregate average section score for a given review period falls below 2, or
  - Three or more aggregate average section scores for a given review period fall between 2 and 3.

## 4.3 PFI Audits

As part of the QA process, PCI SSC reserves the right, upon reasonable notice and request, to conduct PFI site/facility audits for purposes of assessing whether the processes and procedures used by PFI for PFI Investigations comply with applicable PFI Program requirements, including but not limited to review of related books, records and other work product for such purpose, and each PFI must provide PCI SSC with reasonable access to such site/facility, books, records and other work product for such purposes.

## 4.4 Warnings, Remediation and Revocation

Failure by a PFI to satisfy applicable requirements or to meet prescribed PFI QA Program quality levels may result in any or all of the following:

- **Warning –**PFIs who fail to meet applicable PFI Validation Requirements or demonstrate a need for improvement in one or more areas of their PFI Investigations that must be improved may receive warnings from PCI SSC.
- **Remediation –** If the PFI fails to meet applicable PFI Validation Requirements, the quality of PFI Investigations otherwise becomes unsatisfactory, or moderate deficiencies have not been resolved after prior warning, PCI SSC reserves the right to require the PFI to enter into remediation as described further below.
- **Revocation –** If, despite prior remediation or warning, a PFI fails to meet applicable PFI Validation Requirements or PFI QA Program quality levels, PFI status will be revoked and the company will be removed from the PCI SSC list of approved PFIs, subject to appeal as described further below.

### *4.4.1 Remediation*

Upon entering remediation, the PFI must submit a remediation plan to PCI SSC, detailing how the PFI plans to improve the quality of its PFI Investigations and related work product. Additionally, as part of the remediation process, PFIs are required to comply with all applicable remediation program requirements, processes and procedures, as determined by PCI SSC from time to time, and may be required to provide PCI SSC and/or affected Participating Payment Brands with additional supporting documentation upon request. PFIs may be required to permit PCI SSC and/or its representatives to visit and audit the PFI's offices, facilities, books and records relating to the PFI's QA program, in each case at the expense of the PFI. During remediation, PFIs are permitted to perform PFI Investigations but all PFI Work Product is subject to heightened review. PCI SSC reserves the right to require performance of a mock investigation of any PFI as an element of remediation and/or in order to reinstate PFI status after revocation.

During remediation, PFIs must pay to PCI SSC a monitoring fee, as defined on the Website, for each Final Incident Report submitted and/or resubmitted to Participating Payment Brands.

Failure to comply with required remediation requirements, processes, or procedures may result in immediate termination of PFI approval.

If the PFI meets all applicable requirements and quality standards during remediation, remediation will cease and the PFI will again be considered to be in Good Standing. If the PFI fails to meet applicable PFI requirements or quality standards during remediation, PFI status will be revoked.

PCI SSC reserves the right at all times to annotate the PFI's listing on the PCI SSC list of approved PFIs to indicate the PFI's current approval status and related information, including but not limited to whether the PFI is in remediation.

### *4.4.2 Revocation*

If PFI status is revoked, the PFI will be removed from the PCI SSC list of approved PFIs and is no longer recognized by PCI SSC as approved to perform PFI Investigations. PFIs may appeal revocation, but must meet all applicable PFI Validation Requirements, and any applicable remediation requirements in order to regain Good Standing as a PFI.

All appeals must be submitted to PCI SSC in writing within thirty (30) days of revocation, addressed to the PCI SSC General Manager and follow all applicable procedures as specified by PCI SSC. PCI SSC will review all relevant information submitted in connection with such appeals, and all decisions of PCI SSC regarding revocation on appeal are final.

PCI SSC may at any time after revocation notify applicable Participating Payment Brands and/or acquirers or other third parties of such revocation, specifying the reasons therefor.

Upon revocation, a PFI is ineligible for approval as a PFI for a period of six (6) months after the date of revocation or unsuccessful resolution of appeal, whichever is later.

# Appendix A: Forensic Investigation Guidelines

In accordance with applicable Industry Rules, a Compromised Entity that stores, processes, or transmits payment card data and is the subject of a Security Issue must ensure that only a PCI Forensic Investigator approved under the PCI SSC PFI Program is engaged to perform a forensic investigation thereof. All PFIs are required to adhere to the following forensic investigation guidelines in all PFI Investigations. Compromised Entities can also use these guidelines to monitor the work of the PFI.

PFI Investigations must be conducted using the following scope and methodology:

1. The PFI will determine the scope of the forensic investigation and relevant sources of electronic evidence. This includes, but is not limited to:
    - Assessment of all external and internal connectivity points within each location involved.
    - Assessment of network access controls between compromised system(s) and adjacent and surrounding networks.
2. The PFI will acquire electronic evidence from the Compromised Entity's host and network-based systems.
    - If the forensic investigation is conducted onsite at the Compromised Entity's premises, both hard drive and volatile memory acquisition must be performed by either recognized law enforcement agencies or the PFI.
    - If the forensic investigation is being done remotely, the PFI must assess the Compromised Entity's environment to determine whether connectivity allows for acquiring evidence over the Internet. If evidence is to be collected remotely the PFI must use a secure connection (secure tunnel only back to the PFI's IP address). If remote evidence acquisition is not possible the PFI must instruct the Compromised Entity to ship evidence to the PFI. The PFI must ensure the Compromised Entity follows defined preservation guidelines so as not to corrupt the evidence.
3. All potential electronic evidence must be preserved on a platform suitable for review and analysis by a court of law, if applicable.
4. Forensically examine electronic evidence to find cardholder data and establish an understanding of how the compromise or other Security Issue may have occurred.
5. Verify that cardholder data is no longer at risk and/or has been removed from the environment.
6. Verify that the Compromised Entity has contained the incident.
7. The PFI must use the PCI SSC-approved PFI Report templates for each PFI Investigation and provide all required reports to all applicable parties as required in accordance with the *PFI Program Guide.* Additionally, the PFI must make all draft PFI Reports and PFI Investigation work papers available to affected Participating Payment Brands upon request.
8. The PFI must include in its contracts with Compromised Entities provisions ensuring the PFI's authority to provide all final and draft PFI Reports and PFI Investigation work papers to affected Participating Payment Brands and acquirers as required herein or in the *PFI Program Guide* at the same time as the report is sent to the Compromised Entity, in each case without any further authorization of such Compromised Entity. Additionally, each such contract must require the Compromised Entity to acknowledge and agree that the investigation is being carried out as part of the PFI Program, that all PFI Report information shall be shared with affected Participating Payment

Brands throughout the investigation and that the investigation is not to be directed or controlled in any way by the Compromised Entity.

9. The PFI must ensure that all forensic reports generated in connection with its PFI Investigations are its own independent work product, not altered to exclude any factual evidence found, and contain no material omissions.

10. Perform external and internal vulnerability scans, including network and application scans. Determine and describe the type of processing environment (check all that apply):
    - Processor connected directly to the Participating Payment Brands
    - Participating Payment Brand direct-connect processor
    - Issuer only
    - Acquirer only
    - Both issuer and acquirer
    - Pre-paid issuer
    - Third-party processor
    - Merchant
    - Other

11. Check and determine cardholder data that is at risk. This includes:
    - Identifying the total number of accounts impacted for each payment brand.
    - List of associated account information at risk:
        - Full magnetic-stripe data (e.g., Tracks 1 and 2)
        - PIN blocks and clear-text PINs. To identify potential presence of PIN blocks, also look for the PIN block format code field (see Account Data Layout Format*, PIN Security Requirements Report Template For PFI Investigations,* for more information)
        - CAV2, CID, CVC2, CVV2
        - Account number
        - Expiration date
        - Cardholder name
        - Cardholder address
        - Cardholder e-mail address
        - Other relevant data elements, excluding personally identifiable information
    - The PFI must examine all potential locations, including payment applications, to determine if full magnetic-stripe data, CAV2, CID, CVC2, CVV2, and/or PIN blocks are stored (whether encrypted or unencrypted) on production, backups, tables, development, test, software engineer, and administrator's machines.
    - The PFI must also check volatile memory for cardholder data, if an onsite investigation is undertaken.
    - If malware was used to capture cardholder data, the PFI must review any malware output logs and validate whether cardholder data was captured and stored.
    - The PFI must perform malware analysis and document technical findings on the forensic

report.

- Other logs that must be reviewed include the following:
  - Server
  - Application
  - Transaction
  - Troubleshooting
  - Debug
  - Exception or error files
  - Firewall
  - Antivirus
  - IDS
  - IPS
  - Windows Event Logs
  - Remote Access
- The PFI must provide at risk account information to the affected Participating Payment Brands .

12. Determine timeframe of accounts at risk. For example:
    - How long accounts were stored on the system(s).
    - The transaction date(s) of accounts stored on the system(s).
13. Perform incident validation and assessment. This includes:
    - Establishing how the compromise or other Security Issue occurred.
    - Identifying the source of the Security Issue.
    - Determining the window of system vulnerability. This is defined as the frame of time in which a weakness(s) in an operating system, application or network could be exploited by a threat to the time that weakness(s) is properly remediated.
    - Determining whether any cryptographic keys have been exposed or compromised.
    - Reviewing the entire debit and/or credit processing environment to identify all compromised or affected systems; considering the e-commerce, corporate, test, development, production systems, VPN, modem, DSL, cable modem connections, and any third-party connections.
    - Identifying Participating Payment Brands affected.
    - If applicable, review endpoint security of the Participating Payment Brands Participating Payment Brands and determine risk.
    - Identifying the date(s) that account data was transferred out of the network by the intruder or malware.

- Recovering the files with account data that was transferred out of the network by the intruder or malware.

  ***Note:*** *It is critical for the PFI not to access external systems that may have been used by the hacker as dump sites. The PFI must work with appropriate law enforcement prior to accessing non-Compromised Entity systems*

- Identifying date(s) when the entity began using the payment application, version number and vendor. Determine whether the payment application is PA-DSS compliant.
- Identifying payment application vendor and any third party entity engaged by the Compromised Entity to support the payment application.
- Identifying the date(s), if available, when the entity installed a patch or an upgrade to no longer retain prohibited data.
- Identifying the date(s) that malware was installed on the system, if applicable.
- Identifying the date(s) when malicious code, such as packet sniffer and/or key logger, was activated to capture payment card data on the network and system. The PFI must include date(s) of when malware was de-activated.
- Determining the window of intrusion. This is the first confirmed date that the intruder or malware entered the system to the date of containment

14. Determine what PCI Standards and related requirements apply:
    - PCI DSS
    - PCI PTS Security Requirements
    - PCI POS PTS Security Requirements
    - PCI Encrypting PIN PAD (EPP) Security Requirements
    - PA-DSS
    - P2PE Standard
15. If malware or bad IPs are identified in the compromise, the PFI must submit the malware code and bad IPs via a secure distribution to the applicable Participating Payment Brands.
16. Provide detailed analysis and feedback regarding all inconclusive PFI Investigations and the PFI's good-faith opinion as to the reason(s) each such investigation was inconclusive.

# Appendix B: Evidence Handling

## Definitions

For the purposes of this document, “evidence” encompasses both digital and physical evidence unless stated otherwise.

Digital evidence can be defined as information transmitted or stored in a binary form, including the storage device if applicable, which may be examined in relation to a crime or civil action directly or indirectly involving computers and or digital storage media devices. Digital evidence may also incorporate a variety of logs (to include but not limited to event, system, security, firewall, audit, access, etc.) used to monitor events contained within computer systems or computer infrastructures**.**

Physical evidence is defined as any evidence that is not included in the above digital evidence definition such as documents, photographs, case notes, etc…that are applicable to the data compromise event being investigated.

## Minimum Standards for Evidence Collection

Organizations must:

- Have clearly written standards and procedures for identifying, collecting, handling and preserving the integrity of evidence gathered during PFI Investigations.
- Have documentation that employees handling evidence are aware of the organization’s policies and procedures.
- Have documented procedures, advice, and guidance for Compromised Entities to follow if remote data acquisition is used
- Provide a list of forensic tools and/or applications used to acquire evidence, including software versions and dates implemented into service.
- Establish and comply with procedures regarding how all types of digital evidence are acquired so as to not change, manipulate, contaminate or destroy original evidence.
- Provide a secure area for storage of evidence and a dedicated, controlled facility for storage and analysis.
- Provide documentation of how evidence collection is validated, documentation establishing that forensic tools are being correctly used in accordance with accepted industry practice, and documentation of how the PFI validates the tools selected for the type of examination being conducted.
- Document any failed attempts to acquire evidence and the reason(s) why such failures occurred.
- Ensure organizational employees collecting evidence are proficient in use of the tools being used for each PFI Investigation. Such proof shall be documented and retained by the organization for a period of at least three years.
- Have in place a process for remedial training of employees who show or exhibit that forensic tools are being used in a manner not consistent with approved training regarding such tools.
- Meet all applicable laws and regulations

## Evidence Auditing

On a monthly basis, organizations will:

- Inventory all evidence to ensure evidence is present, labelled, disposed/destroyed, etc.
- Review the storage facility and evidence safe/vault logs
- Review and inventory existing forensic tools and kit to determine whether tools require updating

## Chain of Custody

Organizations must have policies and procedures documented and in an accessible location on chain of custody control. Organizations must document the integrity of all evidence under its control. At a minimum, procedures must address the following:

- How evidence is marked
- How evidence is stored under proper seal
- The meeting of all applicable laws and regulations
- Evidence custodian(s) responsible for inventory, proper storage, custody of keys, etc.
- Audit log that includes the following:
  - Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) address, IP address of a system, hash value)
  - Name, title, and phone number of each individual clearly documented who collected or handled the evidence during the investigation
  - Time and date (including time zone) of each occurrence of evidence collection or handling
  - Location where the evidence is stored
  - An accounting for evidence at all times: Whenever evidence is transferred from person to person, chain of custody forms must detail the transfer and include each party's signature.

## Evidence Handling

Organizations must have policies and procedures which manage the preservation of evidence. At a minimum, procedures must include the following:

- Log all evidence and including description, dates, and times.
- Document any activity on the computer, components, or devices.
- Take photographs of system configuration, network connections, etc. if an onsite investigation is undertaken.
- Label all evidence applicable to each specific case/event.
- Secure evidence according to organization's policy pending computer forensic analysis.
- Perform analysis on forensic copies of evidence.
- Pack all digital evidence in antistatic packaging using only approved and accepted bagging and containers.
- Label all containers used to package and store evidence clearly and properly.

Transportation of evidence, including that collected remotely, must be consistent with accepted procedures within the forensics community as to not cause damage to the collected evidence. Some recommendations may include:

- Keep digital evidence away from magnetic fields such as those produced by radio transmitters, speaker magnets, and magnetic mount emergency lights. Other potential hazards that the first responder must be aware of include seat heaters and any device or material that can produce static electricity.
- Avoid keeping evidence in a vehicle for prolonged periods of time. Heat, cold, and humidity can damage or destroy evidence.
- Ensure that computers and electronic devices are packaged and secured during transportation to prevent damage from shock and vibration.
- Document the transportation of the evidence and maintain the chain of custody on all evidence transported.
- Ensure that examination of evidence is not performed on a computer connected to an infrastructure with Internet access.
- Take all reasonable steps to ensure the admissibility of evidence in connection with criminal and other legal proceedings in accordance with applicable jurisdictional requirements.

## Preservation of Evidence

Organizations must have a dedicated storage facility for digital evidence so as to preserve and maintain evidence from any change. Recommendations include:

- Use a climate-controlled environment not subject to extreme temperature or humidity, no exposure to magnetic fields, moisture, dust, vibration, or any other elements which may damage or destroy evidence.
- Lab facilities must be physically secured with restricted access to avoid unauthorized access to the evidence.
- Facility must contain evidence safe or vault to prevent unauthorized access.

## Disposal/Destruction of Evidence

Organizations must have clearly written standards and defined procedures for disposal and destruction of evidence.

Organizations performing digital forensics for the purposes of a computer forensics investigation shall dispose of evidence as applicable to local, State, Federal, and/or National laws governing disposal of such evidence. The duty for disposal and destruction is the onus of the organization; however it is recommended that all evidence be held for at least one year from completion of the case unless required by applicable law of the region/country in which the Security Issue occurred.

When disposal/destruction is approved for physical or digital evidence, the organization shall use an industry-approved standard such as NIST, FIPS, etc.

## Auditing of Evidence Policies and Procedures and Case Investigations

Periodic audits, along with day-to-day review of forensic reports, provide an effective means to ensure that quality is being achieved and implemented in work product. Audits also ensure that forensic examiners perform work in a manner consistent with the policies and procedures of the organization. In compliance with this criteria,

- Each completed case must be reviewed by a peer or supervisor with knowledge of forensic examinations.
- Lab policies and procedures must be reviewed at least once a year to validate whether current and applicable to the lab.
- An audit of the laboratory and examiners must be conducted by using accepted standards and criteria by a recognized computer forensics body to ensure compliance and quality.
- Documentation of the audit and reviews must be retained for at least one calendar year or in accordance with laboratory standards.
- If compliance or performance issues are located in a case or lab audit, a process must be in place to remediate or rectify the findings so as to ensure the lab operates in accordance to the lab Policies and Procedures.

# Appendix C: Glossary of Terms

The terms set forth below, when used in the *PFI Program Guide,* shall have the definitions set forth below, regardless of whether capitalized. When used in the *PFI Program Guide,* terms defined in the *PFI Supplement* or *QSA Validation Requirements* and not defined in the *PFI Program Guide* (including this Appendix) shall have the meanings ascribed to them in the *PFI Supplement* or *QSA Validation Requirements,* as applicable.

| Term | Definition |
|---|---|
| **802.11** | IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz, 3.6 GHz and 2.4 GHz public spectrum bands. |
| **Acquirer** | Financial institution that enters into agreements with merchants to accept a Participating Payment Brand's branded cards as payment for goods and services. Commonly referred to as the "merchant bank." |
| **Agent** | Any contractor, including third-party processors and servicers, whether a client or non-client, engaged by a client to provide services or act on its behalf in connection with the Participating Payment Brands' payment services. |
| **Approving Organization** | Refers 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. |
| **Authentication** | The process of verifying the true origin or nature of the sender and/or the integrity of the text of a message. |
| **Authorization** | A process by which an issuer approves a transaction for a specified amount with a merchant. |
| **Card Verification Value (CVV)** | A unique three-digit "check number" encoded on the magnetic stripe of all valid cards. The number is calculated by applying an algorithm (a mathematical formula) to the stripe-encoded account information, and is verified online at the same time that a transaction is authorized. Referred to as CAV, CVC, CVV, or CSC depending on Participating Payment Brand. The following list provides the terms for each card brand:<br>▪ CAV – Card Authentication Value (JCB)<br>▪ CVC – Card Validation Code (MasterCard)<br>▪ CVV – Card Verification Value (Visa and Discover)<br>▪ CSC – Card Security Code (American Express)<br>***Note:*** *The second type of card validation value or code is the three-digit value printed to the right of the credit card number in the signature panel area on the back of the card. For American Express cards, the code is a four-digit, unembossed number printed above the card number on the face of all payment cards. The code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic. The following provides an overview:*<br>▪ *CID – Card Identification Number (American Express and Discover)*<br>▪ *CAV2 – Card Authentication Value 2 (JCB)*<br>▪ *CVC2 – Card Validation Code 2 (MasterCard)*<br>▪ *CVV2 – Card Verification Value 2 (Visa)* |
| **Cardholder** | The person or entity whose name is embossed or printed on the face of a card or encoded on the magnetic stripe. |

| Term | Definition |
|---|---|
| **Cardholder Data** | Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms* |
| **Common Point of Purchase** | Refers to the location of a legitimate transaction (usually a purchase or cash advance transaction) common to a number of accounts involved in a fraud scheme of similar character. The "common point of purchase" is assumed to be the point of compromise. |
| **Compromise** | Process that exposes cardholder account information to third parties, placing cardholders at risk of fraudulent use. |
| **Compromised Entity** | A merchant, service provider, financial institution or other entity that: processes, stores or transmits Cardholder Data, is required to comply with any PCI Standard, and is at the time in question required pursuant to Industry Rules to undergo a PFI Investigation of a specific Security Issue by a PFI. |
| **Cryptographic Key** | A parameter used in conjunction with a cryptographic algorithm that determines:<br>▪ The transformation of plain-text data into ciphertext data,<br>▪ The transformation of ciphertext data into plain-text data,<br>▪ A digital signature computed from data,<br>▪ The verification of a digital signature computed from data,<br>▪ An authentication code computed from data, or<br>▪ An exchange agreement of a shared secret |
| **Electronic Commerce or e-commerce** | The purchase of goods and services over the Internet without a paper transaction between buyer and seller. |
| **Encryption** | An online data security method that scrambles data so that it is difficult to interpret without a corresponding decryption key. |
| **Entity** | An organization that stores, processes, or transmits account information. Typically the victim in a compromise. Also refers to any payment industry organization that must be PCI DSS compliant. |
| **Event** | Refers to a single event of a known or suspected data compromise. It is used interchangeably with the term "incident." |
| **Financial Institution** | A financial institution that issues payment cards and/or acquires merchant transactions on behalf of a Participating Payment Brand. |
| **Hacker** | A person who deliberately logs on to other computers by circumventing the security system. This is sometimes done to steal valuable information or to cause damage that might be irreparable. |
| **IEEE** | The Institute of Electrical and Electronics Engineers, Inc., an international non-profit, professional organization for the advancement of technology. |
| **Incident** | Refers to each single occurrence of known or suspected data compromise. It is used interchangeably with the term "event." |
| **Industry Rules** | Defined in Section 1.1 of the *PFI Program Guide*. |
| **Issuer** | A financial institution that issues Participating Payment Brand card products. |
| **Magnetic Stripe** | A strip of magnetic tape located on the back of all bankcards. The magnetic stripe is encoded with identifying account. On a valid card, the account information on the magnetic stripe matches similar embossed information located on the front of the card. |

| Term | Definition |
|---|---|
| **Merchant** | An entity that enters into a card acceptance agreement with an acquirer or processor. |
| **Merchant Bank** | See "Acquirer." |
| ***PA-QSA Validation Requirements*** | Refers to the then-current version of the *Payment Card Industry (PCI) Data Security Standard QSA Validation Requirements—Supplement for Payment Application Qualified Security Assessors (PA-QSA)* (or successor document thereto), as made publicly available by PCI SSC. |
| **PAN** | Primary Account Number. |
| **Participating Payment Brand** | Refers to a global Participating Payment Brand or scheme that is also a limited liability company member of PCI SSC, currently: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, Visa Inc., and/or their respective affiliates. |
| **Payment Application Data Security Standard (or "PA-DSS")** | Refers to 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. |
| **Payment Card Industry Data Security Standard (or "PCI DSS")** | Refers to 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. |
| **Payment Card Industry (PCI) PIN Transaction Security Requirements (or "PTS Requirements")** | A set of measures created for the safe transmission and processing of cardholder PINs during ATM and point-of sale (POS) PIN-entry device (PED) transactions. All participants in the payment processing chain that manage cardholder PINs and encryption keys must be in full compliance with the *PCI PIN Transaction Security Requirements.* |
| **PCI Forensic Investigator or PFI** | Refers to a company, organization or other legal entity that is in compliance with all PFI company Requirements (defined in the *PFI Supplement*) and has been approved as a PFI by PCI SSC (or another Approving Organization, if applicable) as a PFI. A list of PFIs can be obtained at www.pcisecuritystandards.org |
| **PCI SSC** | Refers to PCI Security Standards Council, LLC, an open global forum, launched in 2006, that develops, manages, and provides education and awareness regarding the PCI Standards, including: the PCI DSS, PA-DSS and PTS Requirements. For more information on PCI SSC, visit www.pcisecuritystandards.org |
| **PCI Standards** | Refers to the security standards published and managed by PCI SSC, including without limitation, the PCI DSS and the PA-DSS. |
| **Personal Identification Number (PIN)** | An alphabetic and/or numeric code which may be used as a means of cardholder identification. |
| **PFI Investigation** | Refers to the forensic investigation of a Security Issue for a Compromised Entity pursuant to applicable Industry Rules |
| ***PFI Supplement*** | Refers to 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. |
| **Point of Compromise** | Refers to the location where account number data was obtained by unauthorized third parties. |

| Term | Definition |
|---|---|
| **QSA** | A security company qualified by the PCI SSC to perform a PCI Data Security Assessment according to the PCI Security Audit Procedures. Please visit the Website for details on QSA program requirements. |
| ***QSA Validation Requirements*** | Refers to the then-current version of the *Payment Card Industry (PCI) Data Security Standard Validation Requirements for Qualified Security Assessors (QSA)* (or successor document thereto), as made publicly available by PCI SSC. |
| **Security Issue** | Refers to an actual or suspected compromise or other incident that, in accordance with applicable Industry Rules, requires forensic investigation |
| **Third-Party Processor** | A service provider organization acting as the client's agent to provide authorization, clearing, or settlement services for merchants and financial institutions. |
| **Website** | Refers to the PCI SSC website at www.pcisecuritystandards.org. |

# Appendix D: PFI Report Card

This PFI Report Card is intended to be completed by affected Participating Payment Brands following forensic investigation by a PFI, and is available directly from the PFI or online at www.pcisecuritystandards.org. Please send completed PFI Report Cards to PCI SSC at pfi@pcisecuritystandards.org.

### *Contact Information*

| **Participating Payment Brand** | |
|---|---|
| Company name | |
| Contact for organization | |
| Telephone | |
| E-mail | |
| **PFI Company** | |
| Company name | |
| PFI employee who performed the PFI Investigation | |
| Telephone | |
| E-mail | |
| Reporting period (quarter, year) | |
| Number of final PFI reports reviewed | |

*[Questions begin on next page.]*

## *Report Card*

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

**4 = Exceeds Expectations 3 = Meets Expectations 2 = Needs Improvement 1 = Unsatisfactory 0 = Not Applicable**

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

| ***Timeliness** is a key element for PFIs. Please rate these items as per your Participating Payment Brand's expectations.* | | |
|---|---|---|
| 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. While answering the questions below, please consider whether or not there were examples of mistakes made in methodology or the handling of a client 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 followed the evidence-handling guidelines as outlined in *Appendix B* of the *PFI Program Guide*). | Select one |
| | Comments: | |
| 3 | 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 your Participating Payment Brand and Participating Payment Brand client(s). | Select one |
| | 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. | Select one |
| | Comments: | |
| 4 | The PFI company clearly identified any extenuating circumstances that impacted the investigation. | Select one |
| | Comments: | |
| ***Competence*** *is an elementary component for evaluation. In assessing Competence, consider whether or not the PFI representative: was able to complete an 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(s). | 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: | |