Payment Card Industry (PCI)

PCI Forensic Investigator (PFI)

Program Guide

Version 3.0

August 2016

Document Changes

Date	Version	Description
November 2012	2.0	Amendments to support remote forensic investigations and minor administrative revisions
August 2014	2.1	Minor revision to support revised report templates
August 2016	3.0	Updated to align with other PCI SSC program documents Updated section 3.2 Investigative Reporting to include naming convention Added section 3.5 PFI Portal Process to include case number Updated section 4.4 Warnings, Remediation and Revocation to include consequences of multiple/recurring warnings/remediation Updated and clarified Forensic Investigation Guidelines (Appendix A) Updated and clarified Evidence Handling Guidelines (Appendix B) to include evidence retention Updated Participating Payment Brand Reporting (Appendix D) for consistency with evolving processes

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 *Payment Card Industry Qualification Requirements for PCI Forensic Investigators (PFIs) ("PFI Qualification Requirements")* and the *QSA Qualification 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 Company and PFI Employee Qualification
- PFI Program Roles and Responsibilities
- PFI Investigations
- PFI Quality Assurance Program

For purposes of this document, terms used herein and defined in Appendix C shall have the meanings set forth in Appendix C. All other terms used in this document without definition, if defined in the *PFI Qualification Requirements* or the *QSA Qualification Requirements*, shall have the meanings ascribed to them in the *PFI Qualification Requirements* or the *QSA Qualification 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 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, affected Entities Under Investigation 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 qualified by PCI SSC 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 Qualification Process

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 and in accordance with industry expectations, companies and individuals desiring to perform PFI Investigations must first be qualified as PFI Companies or PFI Employees (as applicable), and then must maintain that qualification in Good Standing.

PFI qualification involves: (a) initial eligibility and qualification reviews, including provision of application and supplemental materials, as well as possible interviews of key PFI Employees, (b) ongoing satisfaction of applicable PFI Requirements and (c) annual renewal. Companies qualified as PFI Companies 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 qualification (or renewal).

Please refer to the *PFI Qualification Requirements* to review applicable PFI Requirements and for specific information regarding qualification as a PFI Company or PFI Employee.

1.3 Fees

Fees to participate as a PFI Company in the PFI Program are specified on the Website and discussed further in the *PFI Qualification Requirements*.

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

1.4 Related Publications

This *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 Qualification Requirements*, which describes the requirements that must be satisfied by interested entities and individuals in order to participate in the PFI Program
- *QSA Qualification Requirements*, which defines requirements that must be satisfied by all QSAs in order to perform QSA Assessments
- *PA-QSA Qualification 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 endeavors 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 Entities Under Investigation 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 Entity Under Investigation

In accordance with applicable Industry Rules, the Entity Under Investigation is generally responsible for (without limitation) the following:

- Having a documented incident response plan
- Retaining evidence of compromise
- Limiting data exposure
- Acquiring the services of a PFI Company in the timeline required by affected Participating Payment Brands
- Cooperating with the PFI Company, acquirer, and/or Participating Payment Brand during the PFI Investigation
- Allowing the PFI Company to drive the PFI Investigation
- Participating in discussions with affected Participating Payment Brands and the PFI Company
- Resolving any security weaknesses identified by the PFI Company and/or any affected Participating Payment Brand
- Managing third-party contracts (e.g., hosting/service providers)
- Notifying acquirers and Participating Payment Brands
- Notifying and working with law enforcement as applicable

2.2 Participating Payment Brands

Each of the Participating Payment 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 PFI Companies 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 Company as it deems necessary
- Determining whether on-site attendance of a PFI Company at the Entity Under Investigation is necessary

2.3 PCI SSC

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

- Maintaining the PCI Standards
- Operating and managing the PFI Program and either qualifying eligible entities and individuals to participate in the PFI Program as PFI Companies or PFI Employees, as applicable, or designating an Approving Organization for such purpose
- Managing PFI Quality Assurance (QA) Programs
- Providing 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 Qualification Requirements*) or applicable terms of PFI Program remediation, and have been qualified as PFI Companies by PCI SSC (or another Approving Organization, as described in the *PFI Qualification Requirements*) for purposes of performing PFI Investigations.

Only PFI Companies and PFI Employees qualified by an Approving Organization and who are in PFI Good Standing (or in compliance with the terms of PFI Program remediation) are permitted to perform PFI Investigations, and then only in the specific PFI Regions for which they have been qualified by PCI SSC. All qualified PFI Companies are listed on the Website with applicable PFI Region(s).

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

PFI Company responsibilities generally include (without limitation) the following:

- Driving and performing all aspects of PFI Investigations
- Determining the scope of the investigation and the relevant sources of evidence
- Making recommendations on how the Entity Under Investigation should prioritize containment and secure cardholder data
- 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 Entities Under Investigation and affected Participating Payment Brands and (if applicable) acquirers in discussions regarding PFI Investigations in which they are involved and related Security Issues
- Performing a PIN-security and key-management investigation and a PCI PIN-security assessment *if a PIN compromise is suspected*
- Providing their customers a feedback form, which when completed can be submitted directly to PCI SSC

3 PFI Investigations

3.1 General Requirements

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 Requirements. Once qualified through the PFI Program (and while in Good Standing—or in compliance with the terms of remediation) as a PFI Company thereafter—a PFI Company is only 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.

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 Company at the beginning of each PFI Investigation. Each completed Preliminary Incident Response Report must be delivered to each affected Participating Payment Brand, the applicable Entity Under Investigation, and such Entity's affected acquirer(s) (if the Entity Under Investigation is a merchant), in each case no later than five (5) business days after beginning PFI Investigation review of such Entity Under Investigation.

  To facilitate the identification and processing of reports, Preliminary Incident Response Reports should adhere to the following naming convention when submitting to the brands: yyyymmdd.PRELIM.*entityname,* for example, 20160812.PRELIM.WingnutAutomotive.

- ***Final PFI Report*.** A Final PFI Report (template available on the Website) must be completed by a PFI Company upon completion of each PFI Investigation. The completed Final PFI Report must be delivered to each affected Participating Payment Brand, the applicable Entity Under Investigation, and such Entity Under Investigation's affected acquirer(s) (if the Entity Under Investigation is a merchant), in each case no later than ten (10) business days after completion of the corresponding PFI Investigation of such Entity Under Investigation.

  To facilitate the identification and processing of reports, Final PFI Reports should adhere to the following naming convention when submitting to the brands: yyyymmdd.FINAL.*entityname,* for example, 20160824.FINAL.WingnutAutomotive.

  Note: *Before sending the Final PFI Report to the affected Participating Payment Brands, the PFI Company must follow the Assessor PFI Portal Process (see Section 3.5 below) to receive a case number that uniquely identifies the case without identifying the Entity Under Investigation to PCI SSC. The case number must be included in the Final PFI Report.*

- ***PIN Security Requirements Report***. The current version of this template is available on the Website and must be completed by a PFI Company 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 Entity Under Investigation, and such Entity Under Investigation's affected acquirer(s) (if the Entity Under Investigation is a merchant), in each case no later than ten (10) business days after completion of the corresponding PFI Investigation of such Entity Under Investigation.

- ***Monthly Status Reports.*** On a monthly basis, each PFI Company must deliver to each Participating Payment Brand a detailed report of all of the PFI Company's ongoing PFI Investigations where such Participating Payment Brand is involved, including information regarding threat indicators (for example, malicious toolkits or other malware, malicious IP addresses, anonymous relay addresses, etc.) 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 Company 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 Company 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 Company must utilize such template for all such reports.

Note: *Changes by the PFI Company to the PFI Report templates are strictly limited to those described in FAQ article 1324 on the Website.*

3.3 Delivery of Reports

In accordance with applicable Industry Rules, each PFI Company is responsible for secure and timely delivery of its Preliminary Incident Response Reports, Final PFI Reports and PIN Security Requirements Reports (if applicable), and all other reports required of PFI Companies in accordance with the PFI Program (such reports, collectively, "PFI Reports") to the recipients specified above. PFI Companies must work with the Entity Under Investigation 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 (e.g., transport security using strong cryptography), 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, PFI Companies may be required to demonstrate relevant subject matter knowledge, including without limitation, knowledge in key-management and PIN compromise investigation where applicable. PFI Companies must revise and resubmit all rejected PFI Reports, and resolve all associated discrepancies with affected Participating Payment Brands, acquirers, and the Entity Under Investigation, in a timely manner.*

As described further herein, as part of the PCI SSC QA process, PFI Companies 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 PFI Company's site.

In order to ensure that PFI Companies 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 Company must inform the Entity Under Investigation that it shall be required to disclose the same as herein described and must obtain clear, unqualified permission and consent from the Entity Under Investigation to make such disclosures.

3.4 Evidence Handling

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

3.5 PFI Portal Process

For each PFI Investigation, the PFI Company must request a case reference number via the PFI Portal prior to delivery of the Final PFI Report to the affected Participating Payment Brands. This unique case reference number must be included within the Final PFI Report and will be used by PCI SSC in the PFI Quality Assurance Program for quality monitoring purposes. Delivery of any PFI Report without this case reference number by the PFI Company will be considered failure to comply with PFI Requirements and grounds for warning, remediation, and/or revocation of PFI Company qualification.

In addition to obtaining a unique case reference number via the PFI Portal, PFI Companies must submit through the PFI Portal certain basic details relevant to each PFI Investigation, including (without limitation) identification of the PFI Company and Lead PFI and which Participating Payment Brands are affected by the Security Issue, as well as upload the completed Appendix A from the Final PFI Report. The uploaded Appendix A must not contain any confidential or identifying details—for example, the name, address or IP addresses of the Entity Under Investigation. If information submitted through the PFI Portal changes after initial submission of the Final PFI Report, the PFI Company must update the information in the PFI Portal to accurately reflect the changes.

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 PFI Companies and PFI Employees comply with applicable PFI Requirements, comply with the PFI Company's documented processes and procedures for PFI Investigations, and continually produce and deliver 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 Program remediation, each described further below.

The PFI QA Program collects feedback on PFI Company performance from the Participating Payment Brands and Entities Under Investigation. This feedback is assessed to determine if the PFI Company's performance is meeting expected quality levels. So long as PCI SSC determines in its reasonable discretion that a PFI Company continues to satisfy applicable PFI Requirements and meets prescribed quality levels for PFI Reports and related PFI Services, that PFI Company will remain in Good Standing (defined in the *PFI Qualification Requirements*) as a PFI Company.

4.2 Feedback Process

4.2.1 Customer Feedback Reports and Participating Payment Brand Reports

Following each PFI Investigation, the PFI Company must request that the applicable Entity Under Investigation and, if applicable, each affected acquirer, submit to PCI SSC a "Feedback Report" in the form attached as Appendix C to the *PFI Qualification Requirements*.

Additionally, each affected Participating Payment Brand will complete the PFI Case Summary Report for Payment Brand Use (each a "PFI Case Summary Report") within the PFI Portal on a per-case basis, linked to the case by the case reference number. Appendix D provides an overview of the criteria against which PFI Companies are scored.

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 Case Summary Reports, aggregates scores by PFI Company and question category, and notifies applicable PFI Companies of corresponding results.

Questions in the PFI Case Summary Reports are completed with yes/no responses.

As part of the QA process, on a quarterly basis, question scores received for a given PFI Company are averaged, and the aggregated scores for the PFI Company are categorized as Satisfactory, Needs Improvement or Unsatisfactory. PCI SSC then reviews these scores and takes appropriate action depending on the scores for the applicable review period. See Section 4.4 below.

4.3 PFI Audits

As part of the QA process, PCI SSC reserves the right, upon reasonable notice, to conduct PFI Company site/facility audits for purposes of assessing whether the processes and procedures used by the PFI Company for PFI Investigations comply with applicable PFI Requirements, including but not limited to review of related books, records and other work product for such purpose, and each PFI Company 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 Company to satisfy applicable requirements or to meet prescribed PFI QA Program quality levels may result in any or all of the following:

- **Warning –** PFI Companies that fail to meet applicable PFI Requirements or demonstrate a need for improvement in one or more areas of their PFI Investigations may receive warnings from PCI SSC. The PFI Company may be issued a warning if either:
  - A Needs Improvement result (via the quarterly aggregated results) is achieved; or
  - Other quality concerns are identified.
- **Remediation –** If the PFI Company fails to meet applicable PFI Requirements, the quality of PFI Investigations otherwise becomes unsatisfactory, or moderate deficiencies have not been resolved, PCI SSC reserves the right to require the PFI Company to enter into remediation as described further below. Without limiting the foregoing, a PFI Company may be required to engage in remediation if:
  - An Unsatisfactory result (via quarterly aggregated results) is achieved;
  - A Needs Improvement result (via the quarterly aggregated results) is achieved three (3) times within one (1) rolling calendar year; or
  - Other quality concerns are identified.
- **Revocation –** Beginning October 1, 2016 (at which time all PFI Companies will begin anew with a record of zero consecutive remediations), regardless of prior remediation or warning, if a PFI Company fails to satisfy applicable PFI Company Requirements or achieve satisfactory PFI QA Program quality levels, PFI Company status may be revoked and the company may be removed from the PCI SSC list of PFI Companies, subject to appeal as described further below. Without limiting the foregoing, revocation will be pursued if PCI SSC determines that remediation is warranted for a given PFI Company more than twice within any rolling five (5) year period; and failure to comply with required remediation requirements, processes, or

Note: *A PFI Company remaining in remediation for multiple consecutive quarters for the same issue is considered one (1) remediation.*

procedures may result in immediate revocation of PFI Company qualification.

4.4.1 Remediation

Upon entering remediation, the PFI Company must submit a remediation plan to PCI SSC, detailing how the PFI Company plans to improve the quality of its PFI Investigations and related work product. Additionally, as part of the remediation process, PFI Companies 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. PFI Companies may be required to permit PCI SSC and/or its representatives to visit and audit the PFI Company's offices, facilities, books and records relating to the PFI Company's QA program, in each case at the expense of the PFI Company. During remediation, PFI Companies 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 Company as an element of remediation and/or in order to reinstate PFI Good Standing status after revocation.

To begin remediation, PFI Companies must pay to PCI SSC an administrative fee, as defined on the Website.

If the PFI Company meets all applicable requirements and quality standards during remediation, remediation will cease and the PFI Company will again be considered to be in Good Standing. If the PFI Company fails to meet applicable PFI Requirements or quality standards by the end of the designated remediation period, PFI Company qualification will be revoked.

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

4.4.2 Revocation

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

All appeals must be submitted to PCI SSC in writing within thirty (30) days of revocation, addressed to the PFI Program 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 Company is ineligible for qualification as a PFI Company for a period of three (3) years after the date of revocation.

Appendix A: Forensic Investigation Guidelines

In accordance with applicable Industry Rules, an Entity Under Investigation that stores, processes, or transmits cardholder data (or service providers with whom cardholder data is shared, or that could affect the security of cardholder data) and is the subject of a Security Issue may be required to ensure that only a PCI Forensic Investigator qualified 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. Entities Under Investigation can also use these guidelines to monitor the work of the PFI Company.

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

1. The PFI Company will determine the scope of the forensic investigation and relevant sources of electronic evidence. (Scope may be modified by the Participating Payment Brands affected by the potential payment card event.) This includes, but is not limited to:
    - Assessment of all external and internal connectivity points within each location involved.
    - Assessment of all potential investigative locations—for example, locations of cardholder data, unauthorized access points, etc.—including: inside the CHD and locations outside the CDE if any evidence leads the PFI Investigation outside the CDE.
    - Assessment of network access controls between compromised system(s) and adjacent and surrounding networks.
2. The PFI Company will acquire electronic evidence from the Entity Under Investigation's host and network-based systems.
    - If the forensic investigation is conducted onsite, both hard drive and volatile memory acquisition must be performed by either recognized law enforcement agencies or the PFI Company.
    - If the forensic investigation is being done remotely, the PFI Company must assess the environment to determine whether connectivity allows for acquiring evidence over the Internet. If evidence is to be collected remotely the PFI Company must use a secure connection (secure tunnel only back to the PFI Company's IP address). If remote evidence acquisition is not possible the PFI Company must instruct the Entity Under Investigation to ship evidence to the PFI Company. The PFI Company must ensure the Entity Under Investigation 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—for example, by:
    - Confirming that the cardholder data is no longer being stored or examining the security controls implemented to protect cardholder data; and
    - Confirming that such controls are in place and operating as intended, e.g., CHD discovery search, log collection/review, network traffic monitoring, etc.

6. Verify that the Entity Under Investigation has contained the incident—for example, by:
   - Examining the attack vector/root cause of the compromise and
   - Confirming that the corrective actions taken to protect cardholder data are effective, in place and operating as intended—e.g., migrating to alternate payment processing method/provider, replacing network-accessible POS devices with stand-alone terminals, log collection/review, network traffic monitoring, vulnerability scanning, penetration testing, etc.
7. The PFI Company 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, and ensure the Table of Changes is updated with the changes and versions appropriately documented.
8. The PFI Company must include in its contracts with Entities Under Investigation 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 Entity Under Investigation, in each case without any further authorization of such Entity Under Investigation. Additionally, each such contract must require the Entity Under Investigation 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 Entity Under Investigation or parties acting on behalf of the Entity Under Investigation.
9. The PFI Company 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 per the table in section A1 of the Final PFI Report and "Type of business entity" table in the PFI Preliminary Incident Response Report.
11. Identify and determine cardholder data that is at risk. This includes:
    - Identifying the total number of accounts potentially impacted for each applicable Participating Payment Brand(s).
    - Listing of associated account information at risk, including without limitation, all items in table 3.4 of the Final PFI Report and "Type of data impacted" table in the PFI Preliminary Incident Response Report (to the extent available).
    - The PFI Company must examine all potential locations, including payment applications, to determine if full magnetic-stripe data, EMV Cryptograms, PAN, CAV, 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 Company must also check volatile memory for cardholder data, if an onsite investigation is undertaken.
    - If malware was used to capture cardholder data, the PFI Company must review any malware output logs and validate whether cardholder data was captured and stored.
    - The PFI Company 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 Company must provide at-risk account information to the affected Participating Payment Brands no later than the time the Final PFI Report is submitted to the applicable Participating Payment Brand(s).

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 including:
    - 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 and notifying Participating Payment Brands affected.
    - If applicable, reviewing endpoint security of the Participating Payment Brands and determining 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 Company not to access external systems that may have been used by the attacker as dump sites. The PFI Company must work with appropriate law enforcement prior to accessing non-Entity Under Investigation 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 Entity Under Investigation 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 Company 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
    - PCI PA-DSS
    - PCI P2PE Standard
    - PCI Token Service Provider (TSP) Requirements

15. If threat indicators—for example, malicious toolkits or other malware, malicious IP addresses, anonymous relay addresses, etc.—are identified, the PFI Company must submit a sample of the threat indicators via a secure distribution to the applicable Participating Payment Brands. Such samples may consist of IP addresses, URLs, registry settings, filenames/locations, domain names, e-mail addresses, malware code samples, or checksum values, etc.

16. Provide detailed analysis and feedback regarding all inconclusive PFI Investigations and the PFI Company's good-faith opinion as to the reason(s) each such investigation was inconclusive.

Appendix B: Evidence Handling

Purpose

The following requirements are intended to help ensure (i) the objectivity and transparency of PFI Investigations and related evidence recovery processes, (ii) the continuity and integrity of the evidence generated and/or gathered during such investigations, and (iii) the ability of third parties to repeat the same processes and arrive at the same results.

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 (including but not limited to application, database, system, security, firewall, audit, access, etc.) used to monitor events 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 Security Issue being investigated.

Minimum Standards for Evidence Collection

PFIs must:

- Have and adhere to clearly written standards, policies, and procedures for identifying, collecting, handling and preserving the integrity of evidence gathered during PFI Investigations.
- Have documentation (e.g., acknowledgement form or other attestation) that employees handling evidence are aware of the PFI Company’s standards, policies, and procedures.
- Have documented procedures, advice, and guidance for Entities Under Investigation to follow if remote data acquisition is used.
- Possess and maintain 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 evidence (digital and physical) are acquired so as to not delete, change, manipulate, contaminate, or destroy the integrity of original evidence.
- Possess and maintain a secure area for storage of evidence and a dedicated, controlled facility for storage, preservation, and analysis.
- For each PFI Investigation, collect and maintain documentation establishing in detail:
    - How evidence collection is validated;
    - That forensic tools are being correctly used in accordance with accepted industry practice; and
    - How the PFI Company 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 employees handling evidence are proficient in use of the tools being used for each PFI Investigation. Such proof shall be documented and retained by the PFI Company for a period of at least three (3) years.

- Have a process in place for remedial training of employees who may not be performing investigations or utilizing forensic tools in a manner consistent with PCI DSS, Participating Payment Brand compliance programs and PFI Requirements.
- Meet and abide by all applicable laws and regulations.

Evidence Auditing

On a monthly basis, PFI Companies will:

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

Chain of Custody

PFI Companies must have documented chain-of-custody standards, policies, and procedures available in a location accessible to all PFI Employees. PFI Companies must document the integrity of all evidence under its control. At a minimum, procedures must address the following:

- How evidence is marked or labelled
- 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 at each “touch point” 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 (i.e., each “touch point”), chain-of-custody log forms must detail the transfer and include each party’s signature.

Evidence Handling

PFI Companies must have standards, policies and procedures to 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.
- Acquire visual reminders (e.g., photographs, screen captures, diagrams, etc.) of system configurations, computer and peripheral device setup, network connections, etc. if an onsite investigation is undertaken.
- Label all evidence applicable to each specific case/event.
- Secure evidence to safeguard from allegations of mishandling or tampering according to PFI Company’s policies pending forensic analysis.

- Perform analysis on forensic copies of evidence.
- Pack all digital evidence in antistatic packaging using only approved and accepted bagging and/or containers.
- Inventory and 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 storing evidence in a vehicle for prolonged periods of time. Heat, cold, and humidity can damage or destroy evidence.
- Ensure that computers, media 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 performed *only* from computer systems and infrastructures with *no public network or Internet access*.
- Take all reasonable steps to ensure the admissibility of evidence in connection with criminal and other legal proceedings in accordance with applicable regional and/or jurisdictional requirements.

Preservation of Evidence

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

- Use a climate-controlled environment not subject to extreme temperatures 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.

Destruction/Disposal of Evidence

PFI Companies must have clearly written standards and defined procedures for secure destruction and disposal of evidence. PFI Companies performing digital forensics investigation shall dispose of evidence in accordance with all applicable local, state, federal, and/or national laws governing disposal of such evidence. The duty for destruction and disposal is the onus of the PFI Company; however all evidence must be held for at least one year from the dissemination date of the Final PFI Report (as submitted to the payment brands) unless required by applicable law of the region/country in which the Security Issue occurred.

When destruction/disposal is approved for physical or digital evidence, the PFI Company 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 PFI Company. 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 by a peer or supervisor with knowledge of forensic examinations at least annually 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.
- 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 Qualification Requirements* or *QSA Qualification Requirements* and not defined in the *PFI Program Guide* (including this Appendix) shall have the meanings ascribed to them in the *PFI Qualification Requirements* or *QSA Qualification Requirements,* as applicable.

Term	Definition
Acquirer	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms.*
Approving Organization	Defined in the *PFI Qualification Requirements*.
Authentication	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.
Authorization	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.
Card Verification Code or Value	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.
Cardholder	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.
Cardholder Data (or CHD)	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms.*
Compromise	Process that exposes cardholder account information to third parties, placing cardholders at risk of fraudulent use.
Entity Under Investigation	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	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.
Electronic Commerce or e-commerce	The purchase of goods and services over the Internet without a paper transaction between buyer and seller.
Encryption	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.
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.
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	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.
Magnetic Stripe Data	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.

Term	Definition
Merchant	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.
Merchant Bank	See "Acquirer" (Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms)*
PA-QSA Qualification Requirements	Refers to the then-current version of the *Payment Card Industry (PCI) Qualification Requirements for Payment Application Qualified Security Assessors (PA-QSA)* (or successor document thereto), as made publicly available by PCI SSC.
PAN	Primary Account Number. Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms.*
Participating Payment Brand	Defined in the *QSA Agreement*.
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, PFI, or PFI Company	Refers to a company, organization, or other legal entity that is in compliance with all PFI Company Requirements (defined in the *PFI Qualification Requirements*) and has been qualified as a PFI Company and/or PFI Employee 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, PA-DSS, and P2PE.
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 an Entity Under Investigation pursuant to applicable Industry Rules for PFI Program purposes.
PFI Portal	The secure web portal designated by PCI SSC for the applicable purpose in connection with the PFI Program.
PFI Qualification Requirements	Refers to the then-current version of the *Payment Card Industry (PCI) Data Security Standard, QSA Qualification Requirements for PCI Forensic Investigators (PFIs)* (or successor document thereto), as made publicly available by PCI SSC.

Term	Definition
Point of Compromise	Refers to the location where account number data was obtained by unauthorized third parties.
QSA	Defined in the *PCI DSS Glossary of Terms, Abbreviations and Acronyms*.
QSA Qualification Requirements	Refers to the then-current version of the *Payment Card Industry (PCI) Data Security Standard Qualification 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 by a PFI.
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: Participating Payment Brand Reporting

Following each PFI Investigation, affected Participating Payment Brands complete and submit a report to PCI SSC. PFI Companies are scored against the following criteria:

- Timeliness/Cooperation
- Accuracy/Competence
- Ethics
- Reporting

The type(s) of questions from the Portal Case Summary Reporting may include:

Timeliness/Cooperation	
1	PFI Company met incident-response time expectations as required by the PFI Program Guide.
2	PFI Company was regularly available for communication with affected card brand and brand client(s
3	PFI Company maintained timely communication regarding the project timeline, such as communication of any issues, obstacles, or other extenuating circumstances.
4	PFI Company provided at-risk account numbers to the affected card brands in a timely fashion.
5	PFI Company submitted requisite reporting in a timely manner, including resulting updates to reporting.
Accuracy/Competence	
1	PFI Company assigned an appropriately qualified Lead Investigator to effectively respond to and address issues with engaged parties throughout the PFI Investigation; and who displayed appropriate knowledge for providing an accurate assessment of the affected entities' PCI status at the time of the incident.
2	PFI Company scoped the investigation appropriately to encompass all areas where payment card data may have been processed, stored, or transmitted.
3	PFI Company followed the evidence-handling guidelines (as outlined in Appendix B of the *PFI Program Guide*).
4	PFI Company submitted acceptable final report to the affected card brand with minimal iterations.
Ethics	
1	PFI Company fulfilled the objective of providing an independent, unbiased representation of the facts of the case, including no significant or intentional omissions or misrepresentations of facts.
2	PFI Company maintained independence throughout the engagement, including fulfilling PFI duties without wilful and/or unreasonable delays in conducting the investigation for any reason.
Reporting	
1	PFI Company used the appropriate templates for reports.
2	PFI Company provided thorough, consistent detail as to how either the event was conclusive or not. The items to address are initial attack vector, centralization/storage of card data, and exfiltration method.