Payment Card Industry (PCI)
Data Security Standard
Final PFI Report

Template for Final PFI Report

Version 3.2

July 2021

Document Changes

Date	Version	Description
August 2014	1.0	To introduce the template for submitting Final PFI Report
February 2015	1.1	Clarification to Appendix A
August 2016	2.0	Combined the following templates to create the Final PFI Report: • PFI RT Remote Final PFI Response Template • PFI RT Final PFI Response Template Added a Table of Changes for PFI Assessors to capture various iterations of the report. Added additional reporting to include the case number, client/PFI/acquiring bank contact information, brand acceptance, malware family, phishing email samples and date of containment. Clarified definitions for "cause of breach" and "contribute to breach." Clarified reporting regarding the number of cards exposed. Added an instruction to include the "date of containment." Clarified that all times/dates must be in GMT. Changed "Compromised Entity" to "Entity Under Investigation" throughout the document. Added new appendix to address the impacted entities. Other minor corrections and edits made for clarification and/or format.
August 2017	2.1	Added various clarification language and guidance notes throughout document Added options for disk/system imaging in section 1.4 Clarified the intent of the term “breach” for PFI Investigation and reporting purposes in section 1.5 Added options for “unknown,” “inconclusive” and “other” in sections 1.5 and 3.5 Added “transmit” and the inclusion of software add-ins in section 3.2 Clarified “at risk” and added guidance and additional reporting options in section 3.4 Removed section 5.3 to reduce redundancy, renumbered remainder of section 5 accordingly Added fields to report evidence of previous PCI DSS assessment/validation in section A.1 Clarified reporting requirements for dates and timestamps (Appendix F)

Date	Version	Description
June 2019	3.0	Clarified that any amendments to the report must be clearly evidenced in the Table of Changes in the revised report and the report version number incremented appropriately Clarified that containment must be validated by the PFI in section 1.5.1 Added clarification in Appendix A, section A.2 for previously-descoped requirements (partial PCI DSS assessments), the PFI must perform appropriate testing and validation to verify the non-applicability of any PCI DSS requirements that have been previously de-scoped Added definition for Window of payment card data storage in Appendix E Added PCI PTS Security Requirements Report template as Appendix G
June 2020	3.1	Added reminder that all fields in the report are mandatory, must be completed and the report template/contents must not be modified (also updated FAQ 1324 on the PCI SSC website) Added section 2.2 “Account data in the environment reviewed” to identify data accessible to the Entity Under Investigation during the incident under investigation Added clarification to Appendix A (A2) reporting instructions Added new template form for Appendix B indicators of compromise (available on PFI Portal) Added reminder that Appendix C must be completed if conclusive evidence of a breach exists; added date and version fields to Appendix C template Removed outdated Appendix D
October 2020	3.1r1	Moved the note in section 1.5.1 to section 1.5, as it applies whether or not conclusive evidence of a breach exists.
June 2021	3.2	Clarified in section 1.5.1 to report only containment actions that have been validated by the PFI (all containment actions completed by the Entity Under Investigation (and/or their agents) should be detailed in section 6.1) Removed unnecessary field (“Total number of cards and other data found”) from section 2.2 Replaced “present” with “found within the scoped environment” for clarification in section 2.2 Split the “other” and “maybe” options in section 3.4 into two separate report items for clarity Clarified in section 6.1, 6.2 to include actions that the entity’s agents have taken to contain the incident Added field to section A.1 for details if a third-party hosting provider was involved or potentially responsible for the incident under investigation Clarified in section A.2, note 4, that a “No” responses must include a description of only what was not in place (PFI should not describe anything that was in place) Added fields in Appendix A.1, A.2 for third-party service provider (TPSP) information; added new column in section 5.2 for TPSP name-alias mapping as to not disclose TPSP identity in Appendix A Added UnionPay to Accepted Card Brands throughout

Table of Changes

This table must be used by PFI Companies to document changes that have been made with each iteration of the Final PFI Report.

Note: *The judgements, conclusions and findings in PFI Reports must be based solely on the factual evidence obtained during the investigation and reflect the independent judgement, findings and conclusion of the PFI Company. If an amendment is required to a Final PFI Report post-issue, for example to correct a factual error or omission, the amendment must be clearly evidenced in the Table of Changes in the revised report and the report version number incremented appropriately.*

Company Name	Name/Title	Date	Version	Detailed Description of the Change (Include section number, page number and content of changes)

Table of Contents

Instructions for the Template for Final PFI Report

This reporting template provides reporting tables and reporting instructions for PFIs to use and must be ***completed fully***. This can help provide reasonable assurance that a consistent level of reporting is present among PFIs. Do not delete any sections or rows of this template, but feel free to add rows as needed (see FAQ 1324 on the Website for details).

Definitions for certain terms in this template are provided at *Appendix E*. Capitalized terms not otherwise defined in this document have the meanings set forth in the *Payment Card Industry (PCI) Qualification Requirements for PCI Forensic Investigators* and *Payment Card Industry (PCI) PCI Forensic Investigators Program Guide* as available on the PCI Security Standards Council ("PCI SSC") website.

Dates and timestamps throughout the report must be reported in accordance with *Appendix F*.

Use of this Reporting Template is mandatory for all Final PFI Reports and must be completed fully.

1 Contact Information and Executive Summary

Summary of Investigation:	

1.1 Contact information

Client			
Company name:		Case number:	
Company address:			
Company URL:			
Company contact name:			
Company contact role or position:			
Contact phone number:			
Contact e-mail address:			
Acquiring Bank(s) Additional rows may be added to accommodate multiple acquirers.			
Company name:			
Company address:			
Company contact name:			
Contact phone number:			
Contact e-mail address:			
Has the acquirer(s) been notified?			

PFI Company	
Company name:	
Company address:	
Company website:	
PFI Employee	
Employee name:	
Employee phone number:	
Employee e-mail address:	

1.2 Brand Acceptance

Indicate whether each card brand is accepted by the Entity Under Investigation. If card brands are not accepted by the Entity Under Investigation, provide applicable details in Section 3.4.

Brand	Accepted?
Visa	☐ Yes ☐ No
MasterCard	☐ Yes ☐ No
Discover (including Diners Club International)	☐ Yes ☐ No
American Express	☐ Yes ☐ No
JCB	☐ Yes ☐ No
UnionPay	☐ Yes ☐ No
Other	☐ Yes ☐ No
If *other, identify other brand acceptance.*	

1.3 Date and Timeframe of Assessment

Note: *Dates and timestamps must be reported in accordance with* Appendix F *throughout the report.*

Date of PFI Company engagement	
Date forensic investigation began	

1.4 Locations Reviewed

Identify all locations visited or forensically reviewed.

Note: *Scanned locations should be omitted from this section, but included in* Appendix C*.*

Total number of locations					
Number of locations reviewed					
Location(s)	**Onsite Investigation**	**Remote Investigation**	**Imaged (full)**	**Imaged (logical)**	**Other (describe)**
	☐	☐	☐	☐	☐
	☐	☐	☐	☐	☐
Describe any other source(s) of evidence (if applicable):					

1.5 Executive Summary of Findings

Summary of environment reviewed *Details must be documented in Section 5.*	
Was there conclusive evidence of a breach[1]? ***Note:*** *Whether or not conclusive evidence of a breach exists, in each case the PFI must complete* Appendix C*, consistent with the findings reported below.*	☐ Yes (complete only Section 1.5.1 below) ☐ No (complete only Section 1.5.2 below)
1.5.1 If *yes* (there is conclusive evidence of a breach), complete the following:	
Date(s) of intrusion	Refer to Section 3.1 for this response. No further reporting is required here.
Cause of the intrusion	
Has the breach been validated by the PFI as contained?	☐ Yes ☐ No (explain) ☐ Not Applicable (explain)
If *yes*, specify how the breach has been contained. ***Note:*** *Include only the containment actions that have been validated by the PFI here.* *All containment actions completed by the Entity Under Investigation (and/or their agents) should be detailed in Section 6.1.*	
Date of containment	

[1] For the purpose of PFI Investigations and reporting, "breach" is defined as unauthorized intrusion into or access, acquisition, use, disclosure, modification and/or destruction of data and/or systems.

Note: *A good-faith but unauthorized intrusion into or acquisition of personal information by a person or entity, or any employee, contractor, representative or agent thereof, solely for the lawful purposes of such person or entity, is not by itself considered a breach for purposes of the above definition, unless that personal information is then subject to other unauthorized intrusion, access, acquisition, use, disclosure, modification or destruction.*

Note: *The term "breach" (as defined above) is intended solely for purposes of this document and the PFI Program, and may be defined differently under or for purposes of applicable laws, statutes, regulations, or other legal requirements. PFI's should be familiar and comply with all applicable legal requirements, and nothing herein should be construed to suggest or imply anything to the contrary.*

Is there evidence the cardholder data environment was breached? *Provide reasons for Yes or No in Section 5.*	☐ Yes ☐ No
1.5.2 If *no* (there is no conclusive evidence of a breach), complete the following:	
Were system logs available for all relevant systems?	☐ Yes ☐ No
Were network logs available for all relevant network environments?	☐ Yes ☐ No
Did the available logs provide the detail required by PCI DSS Requirement 10?	☐ Yes ☐ No
Were the log files in any way amended or tampered with prior to your investigation starting?	☐ Yes ☐ No
Were changes made to the environment prior to your investigation starting?	☐ Yes ☐ No
Was data pertaining to the breach deleted prior to your investigation starting?	☐ Yes ☐ No
Provide reasons why the evidence is inconclusive.	

1.6 PFI Company Attestation of Independence

Signatory hereby confirms the following:

1. This investigation was conducted strictly in accordance with all applicable requirements set forth in Section 2.3 of the *Qualification Requirements for PCI Forensic Investigators*, including but not limited to the requirements therein regarding independence, professional judgment, integrity, objectivity, impartiality and professional skepticism;
2. This Final PFI Report accurately identifies, describes, represents and characterizes all of the factual evidence that the PFI Company and its PFI Employees gathered, generated, discovered, reviewed and/or determined in their sole discretion to be relevant to this investigation in the course of performing the investigation; and
3. The judgments, conclusions and findings contained in this Final PFI Report (a) accurately reflect and are based solely upon the factual evidence described immediately above, (b) reflect the independent judgments, findings and conclusions of the PFI Company and its PFI Employees only, acting in their sole discretion, and (c) were not in any manner influenced, directed, controlled, modified, provided or subjected to any prior approval by the subject Entity Under Investigation, any contractor, representative, professional advisor, agent or affiliate thereof, or any other person or entity other than the PFI Company and its PFI Employees.

Signature of PFI Employee ↑	Date:
PFI Employee Lead Investigator Name:	PFI Company:

2 Background

2.1 Background Information

Type of business entity	☐ Merchant: Card present (e.g., brick and mortar)	☐ Acquirer	☐ Third-party service provider (webhosting; co-location; integrator reseller) Identify type of service provider:
	☐ Merchant: Card not present (e.g., e-comm, MOTO, etc.)	☐ Acquirer processor	☐ Encryption Support Organization (ESO)
	☐ Prepaid issuer	☐ Issuer processor	☐ Payment application vendor
	☐ Issuer	☐ ATM processor	☐ Payment application reseller
Parent company (if applicable)			
Franchise or corporate-owned			

2.2 Account Data in the Environment Reviewed

Note: *The intent of this section is to identify account data present (for example, stored, processed, transmitted) in the Entity Under Investigation's environment, and/or account data accessible to the Entity Under Investigation (including any third parties that collect account data on the entity's behalf) during the incident under investigation as described in Section 1.5. This includes data collected by or accessible to third parties serving or operating on behalf of the Entity Under Investigation. This section does not indicate account data exposure.*

Data elements present *(Check applicable data elements)*	☐ Cardholder name	☐ Encrypted or clear-text PINs	☐ PAN
	☐ Cardholder address	☐ Expiry date	☐ Track 2 data
	☐ Track 1 data	☐ CID, CAV2, CVC2, CVV2, CVN, CVN2	☐ PIN Blocks
	☐ EMV Cryptograms	☐ Payment Tokens	☐ Track-equivalent data

Brand-specific Data Present:

Brand	Any data present?
Visa	☐ Yes ☐ No
MasterCard	☐ Yes ☐ No
Discover (including Diners Club International)	☐ Yes ☐ No
American Express	☐ Yes ☐ No
JCB	☐ Yes ☐ No
UnionPay	☐ Yes ☐ No
Other	☐ Yes ☐ No
If *other*, identify other brand data present:	
Were cryptographic keys present?	☐ Yes ☐ No

If *yes,* document the type of cryptographic keys found	**Issuer-Side Cryptographic Keys**	**Acquirer-Side Cryptographic Keys**
	☐ Issuer working keys (IWK)	☐ Acquirer working keys (AWK)
	☐ PIN-verification keys (PVK)	☐ POS, ATM, EPP PIN-encryption keys
	☐ PIN generation keys	☐ POS, ATM, EPP key-encrypting keys (KEKs)
	☐ Master derivation keys (MDK)	☐ Remote initialization keys
	☐ Host-to-host working keys	☐ Host-to-host working keys
	☐ Key-encrypting keys (KEKs)	☐ Key-encrypting keys (KEKs)
	☐ Switch working keys	☐ Switch working keys
	☐ Tokens	☐ Detokenization keys
	☐ Other	☐ Point-to-Point Encryption keys
		☐ Other
If *other* is indicated, describe:		
Were Card Validation Codes or Values found to have been present (i.e., storage, process, transmission, whether intentional or inadvertently) within the scoped investigation?	☐ Yes ☐ No	
If *yes,* document the type of Card Validation Codes or Values found:	**Magnetic-Stripe-Based Security Features**	**Printed Security Features**
	☐ CAV – Card Authentication Value (JCB payment cards)	☐ CAV2 – Card Authentication Value 2 (JCB payment cards)
	☐ CSC – Card Security Code (American Express)	☐ CID – Card Identification Number (American Express and Discover payment cards)
	☐ CVC – Card Validation Code (MasterCard payment cards)	☐ CVC2 – Card Validation Code 2 (MasterCard payment cards)
	☐ CVV – Card Verification Value (Visa and Discover payment cards)	☐ CVV2 – Card Verification Value 2 (Visa payment cards)
	☐ CVN – Card Verification Number (UnionPay payment cards)	☐ CVN2 – Card Verification Number 2 (UnionPay payment cards)

3 Incident Dashboard

3.1 Summary

Date when potential compromise was identified			
Method of identification	☐ Self-detection	☐ Common point-of-purchase	☐ Other
If *other*, describe the method of identification			
Window of application, system, or network vulnerability			
Window of intrusion			
Malware installation date(s), if applicable		Malware family:	
Date(s) of real time capture, if applicable			
Date(s) that data was transferred out of the network, if applicable			
Window of payment card data storage			
Transaction date(s) of stored accounts			

3.2 Payment Application Information

Payment Application Vendor	***3.2.1***
Reseller/IT support that manages payment application/network	***3.2.2***
Does the reseller/IT support employ a Qualified Integrator/Reseller (QIR) Professional listed on the PCI SSC list of Qualified Integrator/Reseller Professionals?	***3.2.3*** ☐ Yes ☐ No

Payment Application Information:	Payment Application Name	Version Number	Install Date	Last Patch Date	Is Application PA-DSS Listed?
At the time of the breach					☐ Yes ☐ No
Current payment application					☐ Yes ☐ No

Software[2] that transmitted or stored the CID, CAV2, CVC2, CVV2, CVN2, or track data:

This information must be supplied if CID, CAV2, CVC2, CVV2, CVN2 or track data has been transmitted or stored. List all applicable software, to include those with a legitimate need to transmit or store and those without a legitimate need to transmit or store.

Name of Software	Version Number	Vendor name (or state, "in house")

[2] Include software and add-on components (for example, extensions, plug-ins)

3.3 Payment Terminal Information

Note: *If PIN block or PIN data was compromised or suspected to have been compromised, a PIN-security and key-management investigation and a PCI PIN-security assessment is required. A current version of the PIN Security Requirements Report template is available as Appendix G of this Final PFI Report template and must be completed by a PFI Company upon completion of each PFI Investigation in cases where PIN block or PIN data was compromised.*

Payment Terminal Information:	Product Name	Version Number	Install Date	Is Payment Terminal Listed?
At the time of the breach				☐ Yes ☐ No
Current payment terminal				☐ Yes ☐ No

3.4 Data Elements Exposed (or possibly exposed)

Note: *A data element is considered "at risk" if evidence indicates the data element was exposed during the incident under investigation. For example, a data element was accessible to the Entity Under Investigation or any unauthorized entity, process or source during the incident under investigation. The at-risk timeframe refers to the period of time these data elements were at risk for this Entity Under Investigation during the incident under investigation.*

Data elements exposed (or possibly exposed) (Check applicable data elements)	☐ Cardholder name	☐ Encrypted or clear-text PINs	☐ PAN
	☐ Cardholder address	☐ Expiry date	☐ Track 2 data
	☐ Track 1 data	☐ CID, CAV2, CVC2, CVV2, CVN, CVN2	☐ PIN Blocks
	☐ EMV Cryptograms	☐ Payment Tokens	☐ Track-equivalent data

Brand Exposure (or possible exposure):					
Brand	**Brand Exposure?**	**Cardholder Data Identified**			
		Malware Output Files Found within CDE	**Malware Output Files Found outside the CDE**	**Data Found within CDE**	**Data Found outside CDE**
Visa	☐ Yes ☐ No ☐ Maybe				
MasterCard	☐ Yes ☐ No ☐ Maybe				
Discover (including Diners Club International)	☐ Yes ☐ No ☐ Maybe				
American Express	☐ Yes ☐ No ☐ Maybe				
JCB	☐ Yes ☐ No ☐ Maybe				
Other	☐ Yes ☐ No ☐ Maybe				
UnionPay	☐ Yes ☐ No ☐ Maybe				
If "*Other*," identify other brand exposure:					
If "*Maybe*," describe the circumstances for each:					
Total number of cards exposed (both malware output file(s) and other data found)					
Is the above the total number of cards that are at risk?		☐ Yes ☐ No			
Explain, including how PFI determined no further cardholder data is at risk, if applicable:					
Were cryptographic keys at risk?		☐ Yes ☐ No			

If *yes,* document the type of cryptographic keys at risk	**Issuer-Side Cryptographic Keys**	**Acquirer-Side Cryptographic Keys**
	☐ Issuer working keys (IWK)	☐ Acquirer working keys (AWK)
	☐ PIN-verification keys (PVK)	☐ POS, ATM, EPP PIN-encryption keys
	☐ PIN generation keys	☐ POS, ATM, EPP key-encrypting keys (KEKs)
	☐ Master derivation keys (MDK)	☐ Remote initialization keys
	☐ Host-to-host working keys	☐ Host-to-host working keys
	☐ Key-encrypting keys (KEKs)	☐ Key-encrypting keys (KEKs)
	☐ Switch working keys	☐ Switch working keys
	☐ Tokens	☐ Detokenization keys
	☐ Other	☐ Point-to-Point Encryption keys
		☐ Other
If *other* is indicated, describe:		
Were Card Validation Codes or Values at risk?	☐ Yes ☐ No	
If *yes,* document the type of Card Validation Codes or Values at risk	**Magnetic-Stripe-Based Security Features**	**Printed Security Features**
	☐ CAV – Card Authentication Value (JCB payment cards)	☐ CAV2 – Card Authentication Value 2 (JCB payment cards)
	☐ CSC – Card Security Code (American Express)	☐ CID – Card Identification Number (American Express and Discover payment cards)
	☐ CVC – Card Validation Code (MasterCard payment cards)	☐ CVC2 – Card Validation Code 2 (MasterCard payment cards)
	☐ CVV – Card Verification Value (Visa and Discover payment cards)	☐ CVV2 – Card Verification Value 2 (Visa payment cards)
	☐ CVN – Card Verification Number (UnionPay payment cards)	☐ CVN2 – Card Verification Number 2 (UnionPay payment cards)

3.5 Incident Evidence and Cause Summary

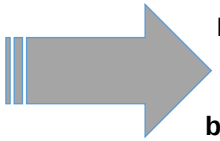
Logs that provided evidence	☐ Firewall logs	☐ Web server logs	☐ Wireless connection logs
	☐ Transaction logs	☐ Hardware Security Module (HSM) logs	☐ Anti-virus logs
	☐ Database queries	☐ File-integrity monitoring output	☐ Security event logs
	☐ FTP server logs	☐ Intrusion-detection systems	☐ Network device logs
	☐ System login records	☐ Remote-access logs	☐ Web proxy logs
Suspected cause summary and list of attack vectors *Insert (or attach) brief case summary. Detailed findings should be included in the "Findings" section of the report.*			
If the initial attack vector is a phishing email (compromised account credentials), confirm that the phishing email, with headers and link, has been included as an appendix to this report. ***Note:** If the phishing email has not been included, provide any information regarding efforts made to obtain the phishing email.*			
If breach is confirmed, is card data still at risk?	☐ Yes ☐ No		
If *yes,* describe the residual risk			
Law enforcement report date			
Law enforcement report case number (if available)			
Law enforcement contact name			
Law enforcement contact phone number			
If the case has not been reported to law enforcement, explain why			

4 Network Infrastructure Overview

4.1 Network Diagram(s)

Provide 1) network diagram(s) representing the time of breach and, 2) if changes occurred, network diagram(s) illustrating post-breach. Include the following in each diagram:

- Cardholder data sent to central corporate server or data center
- Upstream connections to third-party processors
- Connections to acquiring payment card brand networks
- Remote access connections by third-party vendors or internal staff
- Include remote access application(s) and version number
- Inbound/outbound network connectivity



Network security controls and components (network security zones, firewalls, hardware security modules, etc.)**<Insert network diagrams depicting the infrastructure at the time of the breach (or potential breach) and after the breach (or potential breach)>**

Note: *Network diagrams that do not fit on a single page without downsizing should be included as a separate attachment to the report.*

4.2 Infrastructure at the Time of the Breach or Potential Breach

Were there any infrastructure components implemented or modified after the timeframe of the breach?	
If *yes*, describe. Include any changes performed during *and* after the breach.	

5 Findings

5.1 Third-party Payment Applications and Remote Access Applications

Identify any third-party payment application(s), including version number	
Are there any upgrades/patches to the payment application(s) that address removal of magnetic-stripe data, card verification codes or values, and/or encrypted PIN blocks?	☐ Yes ☐ No
If *yes*, identify the payment application and the applicable upgrades/patches to the payment application that address removal of magnetic-stripe data, card verification codes or values, and/or encrypted PIN blocks	
Identify remote access application(s) used, including version number	

5.2 Third-party Service Providers

Identify all third-party service providers (e.g., web hosting, reseller/integrator, POS vendor, etc.).

Name of Third-party Service Provider	Third-party Service Provider alias (for use in Appendix A)	Purpose

5.3 Timeline of Events

Provide an attack timeline of events. Include relevant date(s) and activities as follows:

Date/Time Created	Activity (Brief Description)	Description of Evidence	System/File Evidence

5.4 General Findings

Describe all relevant findings related to:	
Networking technologies	
Infrastructure	
Host	
Personnel	
Other	
Identify specific dates related to changes to:	
Network	
System	
Payment Application	
Personnel	
Other	

5.5 Unauthorized Access and/or Transfer of Data

Describe any data accessed by unauthorized user(s)	
Describe any data transferred out of the network by unauthorized user(s)	
Describe any evidence of data-deletion from systems involved in a breach	
Was any deleted data recovered through forensic file recovery methods?	☐ Yes ☐ No
If *yes*, describe what deleted data was recovered.	

5.6 Breached Systems/Hosts

Complete the table for all breached systems/hosts (e.g., operating system, service pack/hotfix, application) with the corresponding functionality provided.

Identified Breached Systems/Hosts	Functionality

5.7 No Conclusive Evidence of a Breach

If there was no conclusive evidence of a breach indicated at 1.5, Executive Summary of Findings, complete the following:

Provide detailed analysis and feedback regarding the inconclusive case	
Provide the PFI Company's opinion as to the reason for the forensic investigation being inconclusive	

6 Containment Plan for the Entity Under Investigation

6.1 Containment Actions Completed

Document what the entity (and/or its agents) has done to contain the incident, including date(s) of containment.

Containment Action Completed	Completion Date(s)

6.2 Containment actions planned

Document what actions the entity (and/or its agents) plans to take to contain the incident, including planned date(s) of containment.

Containment Action Planned	Planned Date(s) of Completion

7 Recommendation(s)

7.1 Recommendations for the Entity

Document the recommendations made by the PFI Company for the entity. Order recommendations by priority level, with the highest priorities listed first.

Recommendations	Priority Ranking

7.2 Other Recommendations or Comments

Other recommendations or comments from the PFI Company	

Appendix A PCI DSS Overview

To assist in in identifying where breached (or potentially breached) entities failed to fully adhere to the PCI DSS, PFI Companies must submit a copy of *Appendix A* directly to PCI SSC via the Portal.

Note: *When completing this section do not include any information that identifies the Entity Under Investigation.*

QSA Employee who performed the technical review in accordance with the PFI Qualification Requirements:	
QSA Employee name:	
QSA Employee phone number:	
QSA Employee e-mail address:	

A.1 PCI DSS Summary

Type of business entity / payment channels	☐ Merchant: Card present; face-to-face (e.g., brick and mortar)	☐ Acquirer	☐ Third-party service provider (web hosting; co-location; integrator reseller) Identify type of service provider:
	☐ Merchant: Card not present ☐ e-comm ☐ MOTO	☐ Acquirer processor	☐ Encryption Support Organization (ESO)
	☐ Prepaid issuer	☐ Issuer processor	☐ Payment application vendor
	☐ Issuer	☐ ATM processor	☐ Payment application reseller
Was there conclusive evidence of a breach? ☐ Yes ☐ No			
Summary statement for findings, including factors that caused or contributed to the breach. (For example, memory-scraping malware, remote access, SQL injection, etc.)			
Was a PCI DSS Assessment performed prior to the incident under investigation?	☐ Yes ☐ No		

If a PCI DSS Assessment was performed prior to the incident under investigation:			
Date of previous PCI DSS Assessment (prior to the incident under investigation)		Version of PCI DSS used	
Describe any deficiencies or errors with how the environment was scoped for the previous PCI DSS Assessment			
How was the previous PCI DSS Assessment reported?	☐ ROC ☐ SAQ		
If applicable, QSA Company that performed the previous PCI DSS Assessment and attestation for the entity under investigation			
Was an Attestation of Compliance (AOC) issued to the entity within the 12 months prior to this investigation?	☐ Yes ☐ No		
If an SAQ was performed, which SAQ was used?	SAQ (e.g., A, B, C) SAQ version: ☐ NA		
Indicate the version of the PCI DSS used for this part of the investigation			
Did the entity utilize any advanced payment technology at the time of the breach, e.g., end-to-end encryption or tokenization?	☐ Yes ☐ No		
If *yes*, provide details of the product/solution in use, including but not limited to the product or solution used, the date(s) implemented, identify if the advance payment technology was implemented and functioning as designed, etc.			
Describe whether a third-party service provider caused or contributed to the incident under investigation. *Note: Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*			

A.2 PCI DSS Overview

Based on findings identified in the forensic investigation, indicate the compliance status for each of the PCI DSS requirements.

Note: *Since completion of a partial PCI DSS Assessment (e.g., SAQ or partial ROC) is not an indication of an organization's full compliance with PCI DSS, the PFI must perform appropriate testing and validation to verify the non-applicability of any PCI DSS requirements that have been previously de-scoped. For example, if an entity completed an SAQ (or QSA completed a partial ROC) the entity must be assessed against all applicable PCI DSS requirements – the PFI must perform testing and validation to verify the non-applicability of any PCI DSS requirements.*

Document all of the specific PCI DSS requirements and sub-requirements that were not in place at the time of the breach and thus may have contributed to the breach.

1. "Fully-assessed" is defined as an attestation by a QSA as part of the PFI Investigation, including a complete and thorough testing of all sub requirements, in line with the same level of testing required of the PCI DSS in accordance with completing a Report on Compliance (ROC).
2. A "Yes" response to "In Place" may only be used for fully assessed requirements. Fully assessed is defined as an attestation by a QSA as part of the PFI Investigation, including a complete and thorough testing of all sub-requirements, in line with the same level of testing required of the PCI DSS in accordance with completing a Report on Compliance (ROC).
3. A "Partial Yes" response to "In Place" may only be used when:
   - A requirement (e.g., Requirement 1) was only partially assessed under the PCI DSS; and
   - Investigation findings confirm that all sub-requirements that were assessed are "In Place."

   A response of "Partial Yes" does not indicate full compliance with PCI DSS. A "Partial Yes" must not be used if any sub-requirement of the PCI DSS was assessed and found not "In Place."
4. A "No" response to "In Place" must be used if, at any time, a requirement or sub-requirement was assessed and found not "In Place." A "No" responses to "In Place" must include a description of only what **was not** in place (and must not describe anything that **was** in place).
5. A "Not Assessed" response to "In Place" must be used if none of the sub-requirements, for a given requirement, were assessed.
6. "Cause of breach" – the failure of meeting a PCI DSS requirement has provided an attacker access or the ability to access cardholder data.

   A "Yes" response requires the PFI to report which PCI DSS sub-requirement(s) caused the breach. A "Yes" response must not be used if the results of the investigation are inconclusive.
7. "Contribute to breach" – a PCI DSS requirement or sub-requirement has not been met that likely was a contributing factor to the exposure, breadth of attack, and/or ease by which the attacker(s) gained access to the cardholder data environment. By itself, a

contributing factor is not the primary cause of the breach, but when combined with other unmet requirements/sub-requirements, it facilitated and/or contributed to the impact of the breach.

A "Yes" response requires the PFI to report which PCI DSS sub-requirement(s) contributed to the breach. A "Yes" response must not be used if the results of the investigation are inconclusive.

PCI DSS Requirement	Was Requirement Fully Assessed? 1	In Place	Cause of breach? 6	Contribute to breach? 7	Findings/Comments (must be completed for all Requirements)
Build and Maintain a Secure Network					
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					

PCI DSS Requirement	Was Requirement Fully Assessed? 1	In Place	Cause of breach? 6	Contribute to breach? 7	Findings/Comments (must be completed for all Requirements)
Protect Cardholder Data					
Requirement 3: Protect stored cardholder data	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					
Requirement 4: Encrypt transmission of cardholder data across open, public networks	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					

PCI DSS Requirement	Was Requirement Fully Assessed? 1	In Place	Cause of breach? 6	Contribute to breach? 7	Findings/Comments (must be completed for all Requirements)
Maintain a Vulnerability Management Program					
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					
Requirement 6: Develop and maintain secure systems and applications	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					

PCI DSS Requirement	Was Requirement Fully Assessed? 1	In Place	Cause of breach? 6	Contribute to breach? 7	Findings/Comments (must be completed for all Requirements)
Implement Strong Access Control Measures					
Requirement 7: Restrict access to cardholder data by business need-to-know	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					
Requirement 8: Identify and authenticate access to system components	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					
Requirement 9: Restrict physical access to cardholder data	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					

PCI DSS Requirement	Was Requirement Fully Assessed? 1	In Place	Cause of breach? 6	Contribute to breach? 7	Findings/Comments (must be completed for all Requirements)
Regularly Monitor and Test Networks					
Requirement 10: Track and monitor all access to network resources and cardholder data	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					
Requirement 11: Regularly test security systems and processes	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					
Maintain an Information Security Policy					
Requirement 12: Maintain a policy that addresses information security for all personnel	☐ Yes ☐ No	☐ Yes [2] ☐ Partial Yes [3] ☐ No [4] ☐ Not Assessed [5]	☐ Yes ☐ No ☐ Unknown	☐ Yes ☐ No ☐ Unknown	
Describe all applicable third party service provider roles or responsibilities for the Entity Under Investigation. Provide details where the third party may have caused or contributed to the breach. ***Note:*** *Do not disclose the service provider's identity – use the alias assigned in Section 5.2 "Third-party Service Providers."*					

Appendix B Threat Indicator Information

If Indicators of Compromise are available, a Threat Indicator Information spreadsheet (available on the Portal), with detailed information for all threat indicators related to the Incident Under Investigation, must be fully completed (both tabs) and submitted as part of the *Final PFI Report*.

Appendix C Impacted Entities

An Impacted Entities spreadsheet (available on the Portal), reflecting all entities that may have been impacted by this breach, must be fully completed (both tabs) in connection with each PFI Investigation.

Note: *As part of the Final PFI Report provided to each affected Payment Brand, the PFI must include a complete list of all impacted entities identified in the "Impacted Entities" tab of the Impacted Entities spreadsheet. As part of the Final PFI Report provided to each acquirer of record for a merchant identified in the "Impacted Entities" tab of the Impacted Entities spreadsheet, the PFI must include a list of all impacted entities identified therein for which that acquirer is the acquirer of record.*

Appendix D <Hold for future use>

Appendix E List of Investigation Definitions for Final PFI Reports

This appendix is for informational purposes.

Terminology	Description
Date(s) that data was transferred out of the network	The confirmed date(s) that data was transferred out of the network by the intruder or malware.
Date and version of POS installation(s)	Date(s) when the entity began using the POS application and version number. *If available, include date(s) when entity installed a patch or an upgrade to no longer retain prohibited data.*
Malware installation date(s)	The date(s) that malware was installed on the system, if applicable.
Date(s) of real-time capture	Date(s) that malicious code/malware, such as packet sniffer and/or key logger, was activated to capture payment card data on the network and system. Should also include date(s) that malware was de-activated.
Window of intrusion	First confirmed date that intruder or malware entered the system to the date of containment. Examples of containment include, but are not limited to: • Removal of malware or rebuilt breached systems • Breached system removed from the network • Blocking of malicious IPs on the firewall • Rotation of compromised passwords
Transaction date(s) of stored accounts	The date(s) of the transactions stored on the system.
Window of system vulnerability	1. The timeframe in which a weakness in an operating system, application, or network could be exploited by a threat to the time that weakness is properly remediated. It answers the question, "How long was the system at risk to a given breach?" 2. Overall time period that a system was vulnerable to attack due to system weaknesses—for example, lack of or poorly configured firewall, missing security patches, insecure remote access configuration, default passwords to POS systems, insecure wireless configuration.

Window of payment card data storage	1. The timeframe for which account or payment card data was being stored – this may include expired accounts and/or card data. It answers the question, "What is the date range of all accounts and/or payment card data stored, including expired account/payment card data?" 2. Overall timeframe of exposed account/card data. Note the *Window of payment card data storage* is not limited to the "at-risk timeframe" which refers to the period of time the account numbers were at risk (see Section 3.4 and FAQ 1448). The *Window of payment card data storage* includes the full date range (time window) of the actual accounts/card data that were exposed during the at-risk timeframe. Example: The at-risk timeframe is Jan 1 - Jan 31, 2021 (31 days). The unauthorized data disclosure includes account/payment card data dating back to March 2012. The *Window of payment card data storage* would be March 1, 2012 - January 31, 2021.

Appendix F Dates and Timestamps

For consistency with international standards the following date and timestamp formats must be used consistently throughout the report. Multiple formats (as described herein) are permitted within the same report as long as their use is constant. For example, ISO8601 format might be used in a tabular context (especially where space is at a premium) but if a date is referenced generally in a narrative, the full date (e.g., August 12, 2021) may be appropriate. Furthermore, if a specific event is referenced in the same narrative, a full ISO8601 representation may be appropriate. The key is consistency; dates and timestamps must be represented in a manner that can be easily translated and referenced as required.

Dates must be presented in one of the following formats:

- ISO8601[3] format (YYYY-MM-DD). For example, 2021-08-12
- In full. For example, August 12, 2021 or 12 August 2021

Timestamps must be presented in one of the following formats:

- Coordinated Universal Time[4] (UTC). For example: 16:59:48
- Civil time[5] (in full) with local time zone and UTC offset[6] indicated. For example, 09:59:48 PST UTC-07

Formats may be combined for clarity (examples below) but must adhere to the aforementioned formats:

- Coordinated Universal Time (UTC), including civil time (in full) with the local time zone and UTC offset included in parentheses directly afterward.
  For example: 16:59:48 (09:59:48 PST UTC-07)
- Civil time (in full) with the local time zone and UTC offset, including the converted UTC timestamp in parentheses directly afterward.
  For example: 09:59:48 PST UTC-07 (16:59:48)

Note: *If 12-hour clock convention is used for local timestamps, AM/PM indicators must be included.*

[3] http://www.iso.org/iso/home/standards/iso8601.htm
https://en.wikipedia.org/wiki/ISO_8601

[4] https://en.wikipedia.org/wiki/Coordinated_Universal_Time

[5] https://en.wikipedia.org/wiki/Civil_time

[6] https://en.wikipedia.org/wiki/UTC_offset

Timestamps with date information must be presented in one of the following formats:

- ISO8601 format. For example, 2021-08-12T16:59:48
- Date in full, timestamp in UTC. For example, August 12, 2021 16:59:48
- Date in full, timestamp using civil time indicating local time zone and UTC offset.
  For example, August 12, 2021 09:59:48 PST UTC-07
- Date in full, timestamp using civil time indicating local time zone and UTC offset with converted UTC timestamp in parentheses directly afterward.
  For example, August 12, 2021 09:59:48 PST UTC-07 (16:59:48)

Note: *If log file entries are referenced or provided as an attached to the report, the PFI must note any differences between the log entry dates/timestamps and UTC).*

Appendix G PCI PIN Security Requirements Report

A *PIN Security Requirements Report* 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.

Instructions for the Template for PFI PIN Security Requirements Report

This report template provides reporting tables and instructions for PFIs to use and must be completed fully. This helps provide reasonable assurance that a consistent level of reporting is present among PFIs. Do not delete any sections or rows of this template.

Use of this Report Template is mandatory for all PFI PIN Security Requirements Reports.

Requirement		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
Control Objective 1: PINs used in transactions governed by these requirements are processed using equipment and methodologies to ensure they are kept secure.								
1	All cardholder-entered PINs are processed in equipment that conforms to the requirements for secure cryptographic devices (SCDs). PINs must never appear in the clear outside of an SCD. A secure cryptographic device (SCD) must meet the requirements of a "Physically Secure Device" as defined in ISO 13491. This is evidenced by their being validated and approved against one of the following: • One of the versions of the PCI PTS standard, as members of Approval Classes EPP, PED, or UPT (collectively known as POI Devices) and Approval Class HSMs, or • FIPS 140-2 level 3 or higher	☐	☐	☐	☐	☐	☐	
2.	Cardholder PINs shall be processed in accordance with approved standards. • All cardholder PINs processed online must be encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double-length keys. • All cardholder PINs processed offline using IC card technology must be protected in accordance with the requirements in Book 2 of the EMV IC Card Specifications for Payment Systems and ISO 9654.	☐	☐	☐	☐	☐	☐	

Requirement		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
3.	For online interchange transactions, PINs are only encrypted using ISO 9564–1 PIN block formats 0, 1, 3 or 4. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.	☐	☐	☐	☐	☐	☐	
4.	PINs must not be stored except as part of a store-and-forward transaction, and only for the minimum time necessary. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged.	☐	☐	☐	☐	☐	☐	
Control Objective 2: Cryptographic keys used for PIN encryption/decryption and related key management are created using processes to ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.								
5.	All keys, key components and key shares must be generated using an approved random or pseudo-random process.	☐	☐	☐	☐	☐	☐	
6.	Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.	☐	☐	☐	☐	☐	☐	
7.	Documented procedures must exist and be demonstrably in use for all key-generation processes.	☐	☐	☐	☐	☐	☐	
Control Objective 3: Keys are conveyed or transmitted in a secure manner.								
8.	Secret or private keys shall be transferred by: • Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, SCD) using different communication channels, or • Transmitting the key in cipher text form Public keys must be conveyed in a manner that protects their integrity and authenticity. It is the responsibility of both the sending and receiving parties to ensure these keys are managed securely during transport.	☐	☐	☐	☐	☐	☐	

Requirement		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
9.	During its transmission, conveyance, or movement between any two locations or organizational entities, any single unencrypted secret or private key component or share must at all times be protected. Sending and receiving locations/entities are equally responsible for the physical protection of the materials involved. These requirements also apply to keys moved between locations of the same organization.	☐	☐	☐	☐	☐	☐	
10.	All key-encryption keys used to transmit or convey other cryptographic keys must be at least as strong as any key transmitted or conveyed.	☐	☐	☐	☐	☐	☐	
11.	Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.	☐	☐	☐	☐	☐	☐	
Control Objective 4: Key loading to HSMs and POI PIN-acceptance devices is handled in a secure manner.								
12.	Secret and private keys must be input into hardware (host) security modules (HSMs) and POI PIN-acceptance devices in a secure manner. • Unencrypted secret or private keys must be entered using the principles of dual control and split knowledge. • Key-establishment techniques using public-key cryptography must be implemented securely.	☐	☐	☐	☐	☐	☐	
13.	The mechanisms used to load secret and private keys – such as terminals, external PIN pads, key guns, or similar devices and methods– must be protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.	☐	☐	☐	☐	☐	☐	
14.	All hardware and access/authentication methods (e.g., passwords/authentication codes) used for key loading must be managed under the principle of dual control.	☐	☐	☐	☐	☐	☐	

Requirement		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
15.	The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured, and it can be ascertained that they have not been tampered with, substituted, or compromised.	☐	☐	☐	☐	☐	☐	
16.	Documented procedures must exist and be demonstrably in use (including audit trails) for all key-loading activities.	☐	☐	☐	☐	☐	☐	
Control Objective 5: Keys are used in a manner that prevents or detects their unauthorized usage.								
17.	Unique, secret cryptographic keys must be in use for each identifiable link between host computer systems between two organizations or logically separate systems within the same organization.	☐	☐	☐	☐	☐	☐	
18.	Procedures must exist to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.	☐	☐	☐	☐	☐	☐	
19.	Cryptographic keys must be used only for their sole intended purpose and must never be shared between production and test systems.	☐	☐	☐	☐	☐	☐	
20.	All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (e.g., PED) that processes PINs must be unique (except by chance) to that device.	☐	☐	☐	☐	☐	☐	
Control Objective 6: Keys are administered in a secure manner.								
21.	Secret keys used for enciphering PIN-encryption keys or for PIN encryption, or private keys used in connection with remote key-distribution implementations, must never exist outside of SCDs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.	☐	☐	☐	☐	☐	☐	

Requirement		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
22.	Procedures must exist and must be demonstrably in use to replace any key determined to be compromised, its subsidiary keys (those keys encrypted with the compromised key), and keys derived from the compromised key, to values not feasibly related to the original keys.	☐	☐	☐	☐	☐	☐	
23.	Keys generated using reversible key-calculation methods, such as key variants, must only be used in SCDs that possess the original key. Keys generated using reversible key-calculation methods must not be used at different levels of the key hierarchy. For example, a variant of a key-encryption key used for key exchange must not be used as a working key or as a Master File Key for local storage. Keys generated using a non-reversible process, such as key-derivation or transformation process with a base key using an encipherment process, are not subject to these requirements.	☐	☐	☐	☐	☐	☐	
24.	Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.	☐	☐	☐	☐	☐	☐	
25.	Access to secret and private cryptographic keys and key materials must be: • Limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use; and • Protected such that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component.	☐	☐	☐	☐	☐	☐	
26.	Logs must be kept for any time that keys, key components, or related materials are removed from storage or loaded to an SCD.	☐	☐	☐	☐	☐	☐	

Requirement		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
27.	Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key. ***Note:*** *It is not a requirement to have backup copies of key components or keys.*	☐	☐	☐	☐	☐	☐	
28.	Documented procedures must exist and are demonstrably in use for all key administration operations.	☐	☐	☐	☐	☐	☐	
Control Objective 7: Equipment used to process PINs and keys is managed in a secure manner.								
29.	PIN-processing equipment (e.g., POI devices and HSMs) must be placed into service only if there is assurance that the equipment has not been substituted or subjected to unauthorized modifications or tampering prior to the deployment of the device – both prior to and subsequent to the loading of cryptographic keys – and that precautions are taken to minimize the threat of compromise once deployed.	☐	☐	☐	☐	☐	☐	
30.	Physical and logical protections must exist for deployed POI devices.	☐	☐	☐	☐	☐	☐	
31.	Procedures must be in place and implemented to protect any SCDs—and ensure the destruction of any cryptographic keys or key material within such devices—when removed from service, retired at the end of the deployment lifecycle, or returned for repair.	☐	☐	☐	☐	☐	☐	

Requirement		In Place		Cause of breach?		Contribute to breach?		Forensic Findings
		Yes	No	Yes	No	Yes	No	
32.	Any SCD capable of encrypting a key and producing cryptograms (i.e., an HSM or key-injection/loading device) of that key must be protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of one or more of the following: • Dual access controls required to enable the key-encryption function. • Physical protection of the equipment (e.g., locked access to it) under dual control. • Restriction of logical access to the equipment.	☐	☐	☐	☐	☐	☐	
33.	Documented procedures must exist and be demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., POI devices supporting PIN and HSMs) placed into service, initialized, deployed, used, and decommissioned.	☐	☐	☐	☐	☐	☐	

PFI Company Attestation of Independence

Signatory hereby confirms the following:

1. This investigation was conducted strictly in accordance with all applicable requirements set forth in Section
2. of the Qualification Requirements for PCI Forensic Investigators, including but not limited to the requirements therein regarding independence, professional judgment, integrity, objectivity, impartiality and professional skepticism;
3. This Final PFI Report accurately identifies, describes, represents and characterizes all of the factual evidence that the PFI Company and its PFI Employees gathered, generated, discovered, reviewed and/or determined in their sole discretion to be relevant to this investigation in the course of performing the investigation; and
4. The judgments, conclusions and findings contained in this Final PFI Report (a) accurately reflect and are based solely upon the factual evidence described immediately above, (b) reflect the independent judgments, findings and conclusions of the PFI Company and its PFI Employees only, acting in their sole discretion, and (c) were not in any manner influenced, directed, controlled, modified, provided or subjected to any prior approval by the subject Entity Under Investigation, any contractor, representative, professional advisor, agent or affiliate thereof, or any other person or entity other than the PFI Company and its PFI Employees.

Signature of PFI Employee ↑	Date:
PFI Employee Name:	PFI Company: