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

Template for Final PFI Report

Version 2.1

August 2017

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)

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.

Company Name	Name/Title	Date	Version	Description

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 should 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.

Definitions for certain terms in this template are provided at Appendix E.

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.

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:			
▪ 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
▪ 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)**
	☐	☐	☐	☐
	☐	☐	☐	☐

1.5 Executive Summary of findings

▪ Summary of environment reviewed *Details must be documented under "Findings" section below.*	
▪ Was there conclusive evidence of a breach[1]?	☐ Yes (see section 1.5.1 below) ☐ No (see section 1.5.2 below)

[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.*

1.5.1 If yes (there is conclusive evidence of a breach), complete the following:	
▪ Date(s) of intrusion	Refer to Section 3.1 "Summary" for this response. No further reporting is required here.
▪ Cause of the intrusion *List applicable attack vectors as per Appendix D.*	
▪ Has the breach been contained?	☐ Yes ☐ No (explain)
▪ *If yes*, specify how the breach has been contained.	
▪ Date of containment	
▪ Is there evidence the cardholder data environment was breached? *Provide reasons for Yes or No under "Findings" section below*	☐ 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 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			

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	
▪ Reseller/IT support that manages payment application/network	
▪ Is the reseller listed as a Qualified Integrator/Reseller (QIR)?	☐ 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, or track data:

This information must be supplied if CID, CAV2, CVC2, CVV2 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 breached or suspected to have been breached, 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 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.*

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 Possible exposure

Note: *An account is considered "at risk" if evidence indicates the account number was exposed (i.e., accessible to any unauthorized entity, process or source) during the incident under investigation. The at-risk timeframe refers to the period of time that accounts for this merchant were at risk during the incident under investigation*

▪ Type of data 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	☐ PIN Blocks
	☐ EMV Cryptograms		

Brand Exposure:

Brand	Brand Exposure?	Number of cards exposed			
		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				
▪ *If Other* or *"Maybe,"* identify other brand exposure.					
▪ 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
▪ If no, explain.		
▪ 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)

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 (See "List of Attack Vectors" at Appendix D.) *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 a network diagram(s) that includes the following.

- 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 diagram(s)>

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 (i.e., web-hosting, reseller/integrator, POS vendor).

Name of third-party service provider	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

▪ Identify any data accessed by unauthorized user(s)	
▪ Identify any data transferred out of the network by unauthorized user(s)	
▪ Identify any evidence of data-deletion from systems involved in a compromise	
▪ 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 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 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 are requested to submit a copy of Appendix A directly to PCI SSC via the portal. When completing this section do not include any information that identifies the Entity Under Investigation.

A.1 PCI DSS Summary

▪ 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
▪ Summary statement for findings, including factors that caused or contributed to the breach. (For example, memory-scraping malware, remote access, SQL injection, etc.)			
▪ Previously-assessed version of the PCI DSS completed by the entity.			
▪ Date of previous PCI DSS Assessment			
▪ 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 compromise, e.g., end-to-end encryption or tokenization?	☐ Yes ☐ No		
▪ *If yes,* provide details of the product/solution in use.			

A.2 PCI DSS Overview

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

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

[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) A requirement (e.g., Requirement 1) was only partially assessed under the PCI DSS; ***AND***

b) 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."*

[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.*

[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.*

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	
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	
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	
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	
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	

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)
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	
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	
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	
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	
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	
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	

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 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	

Appendix B: Threat Indicator Information

B.1 Threat Indicator Summary

Complete the following table with the following detailed threat indicator information.

- Indicator Types are host, application, and network signs associated with an intrusion. These may include Internet Protocol (IP) addresses, URLs, registry settings, filenames and locations, domain names, e-mail addresses, and network protocols.
- Action or kill-chain phase refers to the point in the attack cycle or intrusion the indicator is associated with. Examples are: Reconnaissance, Weaponization, Delivery, Exploitation, Command-and-control, and Exfiltration.
- For identified malicious IPs, include any information related to malicious IPs (e.g., part of hacker group, TOR, or anonymous relay addresses) in the description.

Copy the below table and add additional tables as needed for each exploit file. Optionally, if you would like to provide extended data on the exploits, complete this and then add a separate annex at the end of this report (with a reference noted in this section to the annex).

Indicator File	**Indicator Type**	**Date and Time**	**Action or kill-chain**
Description:			
	File Name	**Description/File Type**	**File Size**
	MD5 Hash Value	**IP Address(es)**	**Registry Settings**
	Domain	**Domain Time of Lookup**	**System Path**
	Targeted E-mail Address(es)	**Additional data (as needed)**	

Appendix C: Impacted Entities

Complete the required Excel spreadsheet for all entities which may have been impacted by this breach.

Note: *Merchants listed in Appendix C should be provided only to the respective acquirer of record.*

A complete "master list" should also be provided to each Payment Brand affected.

Appendix D: List of Attack Vectors/Intrusion Root Causes/Contributing Factors

This appendix is for informational purposes.

One or more of the attack vector types, Intrusion Root Causes, and Contributing Factors listed below are to be used in completing the "Cause of the Intrusion" at Executive Summary of Findings above.

Vector Type	Specifics
Host	Host – Auto login enabled
	Host – Local accounts are default/unsecured
	Host – Local accounts have weak passwords
	Host – No/limited system hardening
	Host – No/limited system logging
	Host – System allows insecure remote access
	Host – System contains PAN/track data
	Host – System has unrestricted network/Internet access
	Host – System interfaces with POS environment
	Host – System lacks anti-virus/anti-malware/HIPS
	Host – System not inventoried/accounted
	Host – System not patched/maintained
	Host – System runs high-risk/insecure applications
	Host – System runs non-standard/proprietary software
	Host – System used for personal reasons

Vector Type	Specifics
Network	Network – Default configurations in use
	Network – Default passwords in use
	Network – Default/common ports allowed or in use
	Network – Network accounts have weak passwords
	Network – No ACLs present/in-use
	Network – No anti-virus/anti-malware
	Network – No encryption
	Network – No firewall present
	Network – No ingress/egress filtering
	Network – No network segmentation
	Network – No secured remote access
	Network – No security monitoring
	Network – No separate POS environment
	Network – No/insufficient logging
	Network – Use of insecure protocols

Vector Type	Specifics
Remote Access	Remote Access – No monitoring/logging of remote access
	Remote Access – Out-dated/known vulnerable hardware/software in use
	Remote Access – Remote access forwarding allowed
	Remote Access – Remote access left permanently enabled
	Remote Access – Unrestricted remote access allowed
	Remote Access – Use of blackbox/proprietary hardware/software
Web Attack	Web Attack – Allocation of Resources Without Limits or Throttling
	Web Attack – Buffer Access with Incorrect Length Value
	Web Attack – Buffer Copy without Checking Size of Input (Classic Buffer Overflow)
	Web Attack – Cross-site Request Forgery (CSRF)
	Web Attack – Download of Code Without Integrity Check
	Web Attack – Improper Access Control (Authorization)
	Web Attack – Improper Check for Unusual or Exceptional Conditions
	Web Attack – Improper Control of Filename for Include/Require Statement in PHP Program (PHP File Inclusion)
	Web Attack – Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)
	Web Attack – Improper Sanitization of Special Elements used in an OS Command (OS Command Injection)
	Web Attack – Improper Sanitization of Special Elements used in an SQL Command (SQL Injection)
	Web Attack – Improper Validation of Array Index
	Web Attack – Incorrect Calculation of Buffer Size

Vector Type	Specifics
Remote Access	Remote Access – Use of default passwords/accounts
	Remote Access – Use of default/out-of-box configuration
	Remote Access – Use of insecure remote software (e.g., VNC)
	Remote Access – Use of known POS vendor defaults
	Remote Access – Use of weak passwords
Web Attack	Web Attack – Incorrect Permission Assignment for Critical Resource
	Web Attack – Information Exposure Through an Error Message
	Web Attack – Integer Overflow or Wraparound
	Web Attack – Missing Authentication for Critical Function
	Web Attack – Missing Encryption of Sensitive Data
	Web Attack – Race Condition
	Web Attack – Reliance on Untrusted Inputs in a Security Decision
	Web Attack – Unrestricted Upload of File with Dangerous Type
	Web Attack – URL Redirection to Untrusted Site (Open Redirect)
	Web Attack – Use of a Broken or Risky Cryptographic Algorithm
	Web Attack – Use of Hard-coded Credentials
	Web Attack – Failure to Preserve Web Page Structure (Cross-site Scripting)

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	a) 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 compromise?" b) 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.

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, 2017) 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, 2017-08-12
- In full. For example, August 12, 2017 or 12 August, 2017

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.*

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

- ISO8601 format. For example, 2017-08-12T16:59:48
- Date in full, timestamp in UTC. For example, August 12, 2017 16:59:48
- Date in full, timestamp using civil time indicating local time zone and UTC offset.
  For example, August 12, 2017 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, 2017 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).*

[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