



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

Template for PFI Final Incident Report

Version 1.0

August 2014

Document Changes

Date	Version	Description
August 2014	1.0	To introduce the template for submitting PFI Final Incident Report

Table of Contents

Document Changes	i
Instructions for the Template for PFI Final Incident Report	1
1. Contact Information and Executive Summary	1
1.1 <i>Contact information</i>	1
1.2 <i>Date and timeframe of assessment</i>	2
1.3 <i>Locations Reviewed</i>	2
1.4 <i>Executive Summary of Findings</i>	2
1.5 <i>PFI Attestation of Independence</i>	3
2. Background	4
2.1 <i>Background information</i>	4
3. Incident Dashboard	5
3.1 <i>Summary</i>	5
3.2 <i>Payment application information</i>	5
3.3 <i>Possible Exposure</i>	6
3.4 <i>Incident evidence and cause summary</i>	7
4. Network Infrastructure Overview	8
4.1 <i>Network diagram(s)</i>	8
4.2 <i>Infrastructure after the timeframe of the compromise</i>	8
5. Findings	9
5.1 <i>Third-party payment applications and remote access applications</i>	9
5.2 <i>Third-party service providers</i>	9
5.3 <i>Changes made to the compromised entity's computing environment after the identification of compromise</i>	10
5.4 <i>Timeline of events</i>	10
5.5 <i>General Findings</i>	11
5.6 <i>Unauthorized access and/or transfer of data</i>	11
5.7 <i>Compromised systems/hosts</i>	12
5.8 <i>No conclusive evidence of a breach</i>	12
6. Compromised Entity Containment Plan	13
6.1 <i>Containment actions completed</i>	13
6.2 <i>Containment actions planned</i>	13
7. Recommendation(s)	14
7.1 <i>Recommendations for the entity</i>	14
7.2 <i>Other recommendations or comments</i>	14

Appendix A: PCI DSS Overview15
 A.1 PCI DSS Summary..... 15
 A.2 PCI DSS Overview..... 16

Appendix B: Threat Indicator Information19
 B.1 Threat Indicator Summary 19

Appendix C: List of Attack Vectors/Intrusion Root Causes/Contributing Factors.....20

Appendix D: List of Investigation Definitions for Final Incident Reports22

Instructions for the Template for PFI Final Incident 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 C.

Use of this Reporting Template is mandatory for all PFI Final Incident Reports. Where use of the remote incident report is indicated, use of that Reporting Template is mandatory for completion of the Remote Incident Report.

1. Contact Information and Executive Summary

1.1 Contact information

Client	
▪ Company name:	
▪ Company address:	
▪ Company URL:	
▪ Company contact name:	
▪ Contact phone number:	
▪ Contact e-mail address:	
PFI Assessor Company	
▪ Company name:	
▪ Company address:	
▪ Company website:	
PFI Assessor	
▪ Assessor name:	
▪ Assessor phone number:	
▪ Assessor e-mail address:	

1.2 Date and timeframe of assessment

▪ Date of PFI engagement	
▪ Date forensic investigation began	

1.3 Locations Reviewed

Identify all locations visited or forensically reviewed:

Location(s)	Onsite Investigation	Remote Investigation
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>

1.4 Executive Summary of Findings

▪ Summary of environment reviewed <i>Details must be documented under "Findings" section below.</i>	
▪ Was there conclusive evidence of a breach?	<input type="checkbox"/> Yes <input type="checkbox"/> No
<i>If yes (there is conclusive evidence of a breach), complete the following:</i>	
▪ Date(s) of intrusion	
▪ Cause of the intrusion <i>List applicable attack vectors as per Appendix C.</i>	
▪ Has the breach been contained?	<input type="checkbox"/> Yes <input type="checkbox"/> No
▪ <i>If yes, specify how the breach has been contained.</i>	
▪ Is there evidence the cardholder data environment was breached? <i>Provide reasons for Yes or No under "Findings" section below</i>	<input type="checkbox"/> Yes <input type="checkbox"/> No

If no (there is no conclusive evidence of a breach), complete the following:

▪ Were system logs available for all relevant systems?	<input type="checkbox"/> Yes <input type="checkbox"/> No
▪ Were network logs available for all relevant network environments?	<input type="checkbox"/> Yes <input type="checkbox"/> No
▪ Did the available logs provide the detail required by PCI DSS Requirement 10?	<input type="checkbox"/> Yes <input type="checkbox"/> No
▪ Were the log files in any way amended or tampered with prior to your investigation starting?	<input type="checkbox"/> Yes <input type="checkbox"/> No
▪ Were changes made to the environment prior to your investigation starting?	<input type="checkbox"/> Yes <input type="checkbox"/> No
▪ Was data pertaining to the breach deleted prior to your investigation starting?	<input type="checkbox"/> Yes <input type="checkbox"/> No
▪ Please provide reasons why the evidence is inconclusive.	

1.5 PFI Attestation of Independence

Signatory confirms that the independence requirements described in Section 2.3 of the *QSA Validation Requirements, Supplement for PFIs* were met during this investigation.

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

2. Background

2.1 Background information

<ul style="list-style-type: none"> ▪ Type of business entity 	<input type="checkbox"/> Merchant (brick and mortar, e-commerce, or both)	<input type="checkbox"/> Acquirer processor	<input type="checkbox"/> Encryption Support Organization (ESO)
	<input type="checkbox"/> Prepaid issuer	<input type="checkbox"/> Issuer processor	<input type="checkbox"/> Payment application vendor
	<input type="checkbox"/> Issuer	<input type="checkbox"/> ATM processor	<input type="checkbox"/> Payment application reseller
	<input type="checkbox"/> Acquirer	<input type="checkbox"/> Third-party service provider (webhosting; co-location)	
<ul style="list-style-type: none"> ▪ Number of locations 			
<ul style="list-style-type: none"> ▪ Parent company (if applicable) 			
<ul style="list-style-type: none"> ▪ Franchise or corporate-owned 			

3. Incident Dashboard

3.1 Summary

▪ Date when potential compromise was identified			
▪ Method of identification	<input type="checkbox"/> Self-detection	<input type="checkbox"/> Common point-of-purchase	<input type="checkbox"/> Other
▪ <i>If other</i> , describe the method of identification			
▪ Window of application, system, or network vulnerability			
▪ Window of intrusion			
▪ Malware installation date(s), if applicable			
▪ 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				
Payment Application Information:	Payment Application Name	Version Number	Install Date	Is Application PA-DSS Listed?
▪ At the time of the breach				<input type="checkbox"/> Yes <input type="checkbox"/> No
▪ Current payment application				<input type="checkbox"/> Yes <input type="checkbox"/> No
Software that stored the CID, CAV2, CVC2, CVV2, or track data:				
<i>This information must be supplied if CID, CAV2, CVC2, CVV2 or track data has been stored.</i>				
Name of Software	Version Number	Vendor name (or state, "in house")		

3.3 Possible Exposure

<ul style="list-style-type: none"> Type of data exposed (Check applicable data elements) 	<input type="checkbox"/> Cardholder name	<input type="checkbox"/> Encrypted or clear-text PINs	<input type="checkbox"/> PAN
	<input type="checkbox"/> Cardholder address	<input type="checkbox"/> Expiry date	<input type="checkbox"/> Track 2 data
	<input type="checkbox"/> Track 1 data	<input type="checkbox"/> CID, CAV2, CVC2, CVV2	<input type="checkbox"/> PIN Blocks
Brand Exposure:			
Brand	Brand Exposure?		Number of cards exposed (both live system space and unallocated space)
<ul style="list-style-type: none"> Visa 	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<ul style="list-style-type: none"> MasterCard 	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<ul style="list-style-type: none"> Discover 	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<ul style="list-style-type: none"> American Express 	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<ul style="list-style-type: none"> JCB 	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<ul style="list-style-type: none"> Other 	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<ul style="list-style-type: none"> If other, identify other brand exposure. 			
<ul style="list-style-type: none"> Total number of cards exposed (both live system space and unallocated space) 			
<ul style="list-style-type: none"> Were cryptographic keys at risk? 			<input type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> If yes, document the type of cryptographic keys at risk. 	Issuer-Side Cryptographic Keys		Acquirer-Side Cryptographic Keys
	<input type="checkbox"/> Issuer working keys (IWK)		<input type="checkbox"/> Acquirer working keys (AWK)
	<input type="checkbox"/> PIN-verification keys (PVK)		<input type="checkbox"/> POS, ATM, EPP PIN-encryption keys
	<input type="checkbox"/> PIN generation keys		<input type="checkbox"/> POS, ATM, EPP key-encrypting keys (KEKs)
	<input type="checkbox"/> Master derivation keys (MDK)		<input type="checkbox"/> Remote initialization keys
	<input type="checkbox"/> Host-to-host working keys		<input type="checkbox"/> Host-to-host working keys
	<input type="checkbox"/> Key-encrypting keys (KEKs)		<input type="checkbox"/> Key-encrypting keys (KEKs)
	<input type="checkbox"/> Switch working keys		<input type="checkbox"/> Switch working keys
<input type="checkbox"/> Other		<input type="checkbox"/> Other	
<ul style="list-style-type: none"> If other is indicated, please describe. 			

<ul style="list-style-type: none"> Were Card Validation Codes or Values at risk? <ul style="list-style-type: none"> <input type="checkbox"/> Yes <input type="checkbox"/> No 		
<ul style="list-style-type: none"> If yes, document the type of Card Validation Codes or Values at risk 	Magnetic-Stripe-Based Security Features	Printed Security Features
	<input type="checkbox"/> CAV – Card Authentication Value (JCB payment cards)	<input type="checkbox"/> CID – Card Identification Number (American Express and Discover payment cards)
	<input type="checkbox"/> CVC – Card Validation Code (MasterCard payment cards)	<input type="checkbox"/> CAV2 – Card Authentication Value 2 (JCB payment cards)
	<input type="checkbox"/> CVV – Card Verification Value (Visa and Discover payment cards)	<input type="checkbox"/> CVC2 – Card Validation Code 2 (MasterCard payment cards)
	<input type="checkbox"/> CSC – Card Security Code (American Express)	<input type="checkbox"/> CVV2 – Card Verification Value 2 (Visa payment cards)

3.4 Incident evidence and cause summary

<ul style="list-style-type: none"> Logs that provided evidence 	<input type="checkbox"/> Firewall logs	<input type="checkbox"/> Web server logs	<input type="checkbox"/> Wireless connection logs
	<input type="checkbox"/> Transaction logs	<input type="checkbox"/> Hardware Security Module (HSM) logs	<input type="checkbox"/> Anti-virus logs
	<input type="checkbox"/> Database queries	<input type="checkbox"/> File-integrity monitoring output	<input type="checkbox"/> Security event logs
	<input type="checkbox"/> FTP server logs	<input type="checkbox"/> Intrusion-detection systems	<input type="checkbox"/> Network device logs
	<input type="checkbox"/> System login records	<input type="checkbox"/> Remote-access logs	<input type="checkbox"/> Web proxy logs
<ul style="list-style-type: none"> Suspected cause summary and list of attack vectors (See “List of Attack Vectors” at Appendix C.) <p><i>Insert (or attach) brief case summary. Detailed findings should be included in the “Findings” section of the report.</i></p>			
<ul style="list-style-type: none"> Is card data still at risk? 	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<ul style="list-style-type: none"> If yes, please describe the residual risk. 			
<ul style="list-style-type: none"> Law enforcement report date 			
<ul style="list-style-type: none"> Law enforcement report case number 			
<ul style="list-style-type: none"> Law enforcement contact name 			
<ul style="list-style-type: none"> Law enforcement contact phone number 			
<ul style="list-style-type: none"> If the case has not been reported to law enforcement, please 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)>

4.2 Infrastructure after the timeframe of the compromise

<ul style="list-style-type: none"> ▪ Were there any infrastructure components implemented or modified after the timeframe of the compromise? 	
<ul style="list-style-type: none"> ▪ If yes, please describe 	

5. Findings

5.1 Third-party payment applications and remote access applications

<ul style="list-style-type: none"> Identify any third-party payment application(s), including version number 	
<ul style="list-style-type: none"> 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? 	<input type="checkbox"/> Yes <input type="checkbox"/> No
<ul style="list-style-type: none"> 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. 	
<ul style="list-style-type: none"> 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 Changes made to the compromised entity's computing environment after the identification of compromise

Identify any and all changes made to the compromised entity's computing environment after the identification of compromise, including the specific dates. Include any and all forensic evidence supporting changes made to networks, systems and POS components.

<ul style="list-style-type: none"> Payment Application Vendor 			
<ul style="list-style-type: none"> Reseller/IT support that manages payment application/network 			
Payment Application Information:			
	Specific date of change	Version Number	Install Date
<ul style="list-style-type: none"> At the time of the breach 			
<ul style="list-style-type: none"> Current payment application 			
Software that stored the CID, CAV2, CVC2, CVV2, or track data:			
<i>This information must be supplied if CID, CAV2, CVC2, CVV2 or track data has been stored.</i>			
	Name of Software	Version Number	Vendor name (or state, "in house")
<ul style="list-style-type: none"> Software that stored the CID, CAV2, CVC2, CVV2, or track data 			

5.4 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

5.5 General Findings

<i>Describe all relevant findings related to:</i>	
▪ Firewalls	
▪ Infrastructure	
▪ Host	
▪ Personnel	
▪ Other	
<i>Identify specific dates related to changes to the:</i>	
▪ Network	
▪ System	
▪ Payment Application	
▪ Personnel	
▪ Other	

5.6 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?	<input type="checkbox"/> Yes <input type="checkbox"/> No
▪ <i>If yes, describe what deleted data was recovered.</i>	

5.7 Compromised systems/hosts

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

Identified compromised systems/hosts	Functionality

5.8 No conclusive evidence of a breach

If there was no conclusive evidence of a breach indicated at 1.4, Executive Summary of Findings, complete the following:

<ul style="list-style-type: none"> Provide detailed analysis and feedback regarding the inconclusive case 	
<ul style="list-style-type: none"> Provide the PFI's opinion as to the reason for the forensic investigation being inconclusive 	

6. Compromised Entity Containment Plan

6.1 Containment actions completed

Document what the entity has done to contain the incident, including date(s) of containment.

Containment action completed	Date(s) of containment

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 containment

Appendix A: PCI DSS Overview

To assist in identifying where compromised entities failed to fully adhere to the PCI DSS, PFIs 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 potentially compromised entity.

A.1 PCI DSS Summary

<ul style="list-style-type: none"> Type of business entity 	<input type="checkbox"/> Merchant (brick and mortar, e-commerce, or both)	<input type="checkbox"/> Acquirer processor	<input type="checkbox"/> Encryption Support Organization (ESO)
	<input type="checkbox"/> Prepaid issuer	<input type="checkbox"/> Issuer processor	<input type="checkbox"/> Payment application vendor
	<input type="checkbox"/> Issuer	<input type="checkbox"/> ATM processor	<input type="checkbox"/> Payment application reseller
	<input type="checkbox"/> Acquirer	<input type="checkbox"/> Third-party service provider (webhosting; co-location)	
	<input type="checkbox"/> Other (describe):		
<ul style="list-style-type: none"> Summary statement for findings, including factors that caused or contributed to the breach. (For example, memory-scraping malware, remote access, SQL injection, etc.) 			
<ul style="list-style-type: none"> Indicate the version of the PCI DSS used for this part of the investigation (2.0 or 3.0). 			
<ul style="list-style-type: none"> Did the entity utilize any advanced payment technology at the time of the compromise—e.g., end-to-end encryption or tokenization? 	<input type="checkbox"/> Yes <input type="checkbox"/> No		
<ul style="list-style-type: none"> 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.

* “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).

** A “Yes” response to “In Place” is only applicable for fully assessed requirements.

*** A “Partial Yes” response is applicable even if requirement was not fully assessed under the PCI DSS but initial investigation findings suggest that some or part of the requirement(s) are “in place.”

PCI DSS Requirement	Was Requirement Fully Assessed?*		In Place				Cause of breach?			Contribute to breach?			Findings/Comments (Required)
	Yes	No	Yes**	Partial Yes***	No	Unknown	Yes	No	Unknown	Yes	No	Unknown	
Build and Maintain a Secure Network													
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Protect Cardholder Data													
Requirement 3: Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Requirement	Was Requirement Fully Assessed?*		In Place				Cause of breach?			Contribute to breach?			Findings/Comments (Required))
	Yes	No	Yes**	Partial Yes***	No	Unknown	Yes	No	Unknown	Yes	No	Unknown	
Requirement 4: Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Maintain a Vulnerability Management Program													
Requirement 5: Use and regularly update anti-virus software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6: Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Implement Strong Access Control Measures													
Requirement 7: Restrict access to cardholder data by business need-to-know	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8: Assign a unique ID to each person with computer access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 9: Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

PCI DSS Requirement	Was Requirement Fully Assessed?*		In Place				Cause of breach?			Contribute to breach?			Findings/Comments (Required)
	Yes	No	Yes**	Partial Yes***	No	Unknown	Yes	No	Unknown	Yes	No	Unknown	
Regularly Monitor and Test Networks													
Requirement 10: Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 11: Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Maintain an Information Security Policy													
Requirement 12: Maintain a policy that addresses information security	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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
	Hash Type and Value	IP Address(es)	Registry Settings
	Domain	Domain Time of Lookup	System Path
	Targeted E-mail Address(es)	Additional data (as needed)	

Appendix C: 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 D: List of Investigation Definitions for Final Incident 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. <i>If available, include date(s) when entity installed a patch or an upgrade to no longer retain prohibited data.</i>
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: <ul style="list-style-type: none"> ▪ Removal of malware or rebuilt of compromised systems ▪ Compromised 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	<ol style="list-style-type: none"> 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.