Payment Card Industry (PCI)
Data Security Standard

PFI Preliminary Incident Response Report

Template for PFI Preliminary Incident Response Report

Version 2.1

September 2016

Document Changes

Date	Version	Description
August 2014	1.0	To introduce the template for submitting PFI Preliminary Incident Response Report
July 2016	2.0	Added additional reporting to include the case number, client/PFI/acquiring bank contact information, details regarding the last assessment, type of business entity, third-party service providers and card brands that may be potentially affected. Clarified that all times/dates must be in GMT. Changed "Compromised Entity" to "Entity Under Investigation" throughout the document. Also includes minor corrections and edits made for clarification and/or format.
September 2016	2.1	Errata change to remove case number

Instructions for the Template for PFI Preliminary Incident Response Report

This reporting template provides reporting tables and reporting instructions for PFI Companies to use, and should be completed fully. This can help provide reasonable assurance that a consistent level of reporting is present among PFI Companies. Do not delete any sections or rows of this template, but feel free to add rows as needed.

Use of this Reporting Template is mandatory for all PFI Preliminary Incident Response Reports.

PFI Preliminary Incident Response Report

Contact Information

Client	
▪ Company name:	
▪ Company address:	
▪ Company URL:	
▪ Company contact name:	
▪ Contact phone number:	
▪ Contact email address:	
Acquiring Bank(s) *Additional rows may be added to accommodate multiple acquirers.*	
▪ Company name:	
▪ Company address:	
▪ Company contact name:	
▪ Contact phone number:	
▪ Contact email address:	
▪ Has the acquirer(s) been notified?	
PFI Company	
▪ Company name:	
▪ Company address:	
▪ Company URL:	

PFI Employee	
▪ Employee name:	
▪ Employee phone number:	
▪ Employee email address:	

Brand Acceptance

Brand	Accepted?
▪ Visa	□ Yes □ No
▪ MasterCard	□ Yes □ No
▪ Discover	□ Yes □ No
▪ American Express	□ Yes □ No
▪ JCB	□ Yes □ No
▪ Other	□ Yes □ No
▪ *If other, identify* other brand acceptance.	

Note: All dates and/or times must be in GMT throughout the entire report.

Question	**Response**		
▪ Name of Entity Under Investigation			
▪ Date of last AOC or SAQ		Qualified Security Assessor Company (if applicable)	
▪ Type of business entity	□ Merchant (brick and mortar, e-commerce, or both)	□ Acquirer processor	□ Encryption Support Organization (ESO)
	□ Prepaid issuer	□ Issuer processor	□ Payment application vendor
	□ Issuer	□ ATM processor	□ Payment application reseller
	□ Acquirer	□ Third-party service provider (webhosting; co-location; integrator reseller) Identify type of service provider:	
▪ Date investigation started			
▪ Is forensic investigation being done onsite or remotely?	□ Onsite □ Remote		
▪ Evidence of a breach?	□ Yes □ No		
▪ First confirmed date that the intruder or malware entered the network			
▪ Date of malware sample submission for analysis			
▪ Scope of forensic investigation *(e.g., single or numerous locations; how systems/networks were determined for acquisition, remote vs onsite)*			

▪ Type of data impacted (e.g., full track, CID, CAV2, CVC2, CVV2, encrypted or clear-text PINs, PIN blocks, EMV cryptograms)		
▪ Window of system vulnerability		
▪ Initial thoughts on attack vector		
▪ Is the security breach ongoing or has it been contained?	□ Ongoing □ Contained	
▪ If contained, how has it been contained?		
▪ Date of containment		
▪ Estimated date of investigation completion		
▪ Identify all third-party service providers (i.e., web-hosting, reseller/integrator, POS vendor). *(add more rows as needed)*	**Name of third-party service provider**	**Purpose**
▪ Other comments		

PFI Company Attestation of Independence

Signatory hereby confirms the following:

1. This investigation is being 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 PFI Preliminary Incident Response 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 PFI Preliminary Incident Response 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:*

PFI Preliminary Threat Indicator Information

Complete the table below with the following detailed threat indicator information, as much as is available at the time of the PFI Preliminary Incident Response.

- 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)**	