Payment Card Industry (PCI)
Data Security Standard
PFI Preliminary Incident Response Report

Template for PFI Preliminary Incident Response Report

Version 3.2

July 2021

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
August 2017	2.2	Added various clarification language and guidance notes throughout document Clarified reporting of dates and timestamps (Final PFI Report Appendix F) Clarified that Discover also includes Diners Club International
June 2019	3.0	Added section numbers for easier reference Clarified that containment must be validated by the PFI Added a field in section 3 for PFI to describe the state of containment
June 2020	3.1	Minor language updates for consistency with the *Final PFI Report* template v3.1 Added new template form for Appendix B indicators of compromise (available on PFI Portal)
June 2021	3.2	Clarified in the report instructions that delivery of the Preliminary Incident Response Report must be delivered no later than five (5) business days after engagement or beginning the PFI Investigation review, whichever occurs first. Added UnionPay to Accepted Card Brands throughout

Table of Contents

Instructions for the Template for PFI Preliminary Incident Response Report

This reporting template provides reporting tables and reporting instructions for PFI Companies to use. 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. The PFI Preliminary Incident Response Report must be completed by the PFI Company at the beginning of each PFI Investigation. Each completed Preliminary Incident Response Report must be delivered to each affected Participating Payment Brand, the applicable Entity Under Investigation, and such Entity's affected acquirer(s) (if the Entity Under Investigation is a merchant), in each case no later than five (5) business days after engagement or beginning the PFI Investigation of such Entity Under Investigation, whichever occurs first.

Note: *An investigation that begins as a PFI Investigation but does not conclude as a PFI Investigation requires the approval of all Participating Payment Brands.*

Definitions for certain terms in this template are provided at Appendix E of the *Final PFI Report* template. 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 of the *Final PFI Report* template.

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

PFI Preliminary Incident Response Report

1 Contact Information

Client	
Company name:	
Company address:	
Company URL:	
Company contact name:	
Company contact role or position:	
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:	

2 Brand Acceptance

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.	

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

3 Investigation Details

Question	Response		
Name of Entity Under Investigation			
Date of last AOC or SAQ		Qualified Security Assessor Company (if applicable)	
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
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			

Question	Response
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, CVN2 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 validated by the PFI as contained?	☐ Contained ☐ Ongoing ☐ Unknown
If contained, how has it been contained?	
If containment is ongoing or unknown, describe the state of containment. Include all containment activities that have occurred (for example, steps that the Entity Under Investigation has taken to contain the security breach). ***Note:*** *Distinguish and describe activities that have been validated by the PFI as well as any activities that have not yet been validated by the PFI.*	
Date of containment	
Estimated date of investigation completion	

Question	Response	
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		

4 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:*

5 PFI Preliminary Threat Indicator Information

Complete the required Excel spreadsheet (available on the Portal) with detailed threat indicator information related to the incident under investigation, as much as is available at the time of the *PFI Preliminary Incident Response* report.