Payment Card Industry (PCI)
Data Security Standard

PFI Preliminary Incident Response Report

Template for PFI Preliminary Incident Response Report

Version 1.0

August 2014

Document Changes

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

Instructions for the Template for PFI Preliminary Incident Response 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.

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

PFI Preliminary Incident Response Report

Question	Response
▪ Name of compromised entity	
▪ 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)	
▪ 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?	
▪ Estimated date of investigation completion	
▪ Other comments	

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:*

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)**	