

# Is the expectation that any PFI investigation initiated must result in a PFI Final Report?

PCI SSC FAQ | Article 1571 | August 2024

---

Yes, a PFI Final Report is required. The expectation is that the PFI must complete the merchant's PFI Investigation and produce the Final PFI Report, with details of adequate evidence to support claims.

PCI SSC has received multiple inquiries on how to move forward on a third-party service provider case where the breach has been confirmed to have occurred and affected merchants, particularly where some affected merchants may have already begun their own PFI engagements. While there is no "one size fits all" response to such inquiry, PCI SSC can provide the following guidance to PFIs in determining next steps:

- When a PFI investigates a third-party service provider incident, scoping should include steps to identify and include any third-party connections as part of incident validation and assessment, including affected merchants and their sponsoring acquirers.
- In the example of a merchant for which a PFI has already completed the PFI Preliminary Incident Response Report and delivered it to each affected Participating Payment Brand before evidence that a third-party service provider was in fact responsible for the breach affecting the merchant is produced, PFIs are expected to fully complete a Final PFI Report for the merchant. The PFI is expected to complete the merchant investigation and provide confirmation and document in the final PFI report that the breach is related to the third-party service provider incident. It would be reasonable to explain what was investigated, at what point the PFI became aware of the findings for the third-party service provider, and to clearly communicate what was assessed at the merchant and report those findings (conclusive or inconclusive).
- Whether the same PFI Company did or did not assess the third-party service provider and the merchant may affect the level of reporting; if the same PFI Company assessed both, they would reasonably have access to more relevant data than a PFI Company who did not assess the third-party service provider but is assessing an affected merchant.
- Where a third-party service provider PFI investigation has identified affected merchants and no PFI has been engaged for any affected merchant, it is recommended to consolidate the merchant cases into the third-party provider case as a matter of efficiency instead of opening an individual merchant PFI if required by a different workstream or regulatory agency. While the final decision does not rest with the PFI, the PFI must consult with Participating Payment Brands and affected acquirers on how to proceed with the investigation.
- Where there is sufficient evidence, based on one or more merchant PFI investigation(s) that indicate the breach was caused by the third-party service provider, and the third-party service provider is not cooperative and/or has not engaged a PFI, the PFI

must inform the Participating Payment Brands and affected acquirers.

Payment Brand contact details are provided in FAQ #1142 How do I contact the payment card brands?

Source: <https://www.pcisecuritystandards.org/faqs/1571/>