

Can a PFI Company perform subsequent PFI investigations for the same entity?

PCI SSC FAQ | Article 1444 | August 2024

PFI Companies must adhere to the independence requirements of the PFI program as defined in the PFI Qualification Requirements and PFI Program Guide. Whether a PFI Company can conduct a PFI investigation more than once on the same entity will depend on circumstance. For example; if during an investigation the PFI Company carried out work which impacted the PCI DSS compliance status of the entity, and the entity subsequently identifies or suspects a breach, that PFI Company may not be able to satisfy the independence requirements for a subsequent investigation.

Each payment brand has their own rules when a PFI must be engaged, and merchants should consult their compliance-accepting entity (acquirer and/or the payment brands) concerning any issues which may influence a PFI Company's ability to perform an independent investigation, including instances where there is continuation of breach/re-breach after a PFI Final Report has been issued.'

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

Source: <https://www.pcisecuritystandards.org/faqs/1444/>