

What is meant by "At-Risk Timeframe" and at risk referenced in the Final PFI Report?

PCI SSC FAQ | Article 1448 | September 2024

The At-Risk Timeframe refers to the period of time data elements, such as account data, were at risk for this Entity Under Investigation during the incident under investigation. A data element is considered at risk if evidence indicates the data element was exposed (i.e. per the Final PFI Report template v3.3, Section 3.4 "a data element was accessible to the Entity under investigation or any unauthorized entity, process, source, etc.") during the incident under investigation.

The "At-Risk Timeframe" as identified in the Final PFI Report template, Appendix C refers to the period of time during the incident under investigation when data was vulnerable. For example, consider a scenario where evidence (e.g., system/access logs) indicates that an unauthorized entity breached the cardholder data environment's security controls on 2024-04-14T18:30:00 and was discovered by the breached entity (who subsequently took the system offline to limit the exposure) 2024-04-17T07:15:00.

The at-risk timeframe is considered to have been from 6:30PM on April 14th when the breach occurred, through 7:15AM on April 17th when the breached system was taken offline (approximately 60 hours).

Further considering the scenario above, suppose the breached entity had several years' worth of data elements stored in the environment. In this case, regardless of how many data elements were exposed or how long they were stored, the at-risk timeframe:

- would not date back to the oldest data element stored, and
- only refers to the timeframe itself — the period of time the data elements were at risk (approximately 60 hours in this scenario).

For additional information please contact your case-specific Payment Brand representative.

Source: <https://www.pcisecuritystandards.org/faqs/1448/>