PCI 取证调查 – 高效应对支付产业潜在的数据泄露

作者：atsec 张力

关键词：PFI、数据泄露、CPP、PCI、入侵、日志分析

atsec information security

Tel +86-10-53056681
Fax +86-10-53056678

www.atsec.com

目录

1 引言

获知入侵者可能已经进入您的系统并窃取了敏感数据，这无疑对于业务可靠持续发展和技术的稳定性都是一个巨大的冲击。您不仅仅感到被攻击者所侵犯，甚至对即将到来的调查和处置感到焦虑。在支付卡行业，数据泄露事件的影响远远超出了短时间内的损害，故而任何涉及持卡人数据的疑似或确认泄露事件，都必须经过一个严格的流程，即 PCI 取证调查（PFI：PCI Forensics Investigation）。作为 PCI DSS 合规相关的另一个 PCI 体系，PFI 既是针对安全事件的诊断，也是通往修复和恢复的必经之路。

理解 PCI 取证调查的要求，对已经遭遇潜在泄露的企业至关重要，且对于任何处理持卡人数据的组织来说，从防患于未然角度出发也是必要的。了解 PFI 流程有助于企业制定更完善的事件响应计划、实施更强有力的预防措施，并全面理解自身的合规义务。

本文旨在帮助支付产业各类组织了解当疑似数据泄露发生时，如何有序、规范地开展 PCI 取证调查，并简要介绍了 atsec 作为 PCI 安全标准委员会的授权委员会（SSC：Security Standards Council）认可的 PFI 机构的服务和方法论。

2 什么是 PCI 取证调查（PFI）？

PFI 体系是 PCI DSS 合规框架的重要组成部分。PCI DSS 标准要求 12.10 明确规定，组织必须制定并实施应急响应计划，以应对系统泄露事件。在疑似或确认发生安全事件时，要求必须有相应的流程来支持和响应必要的取证调查，以确定事件的影响并制定补救计划。根据 PCI SSC 的《PFI Program Guide》，当发生安全事件时，受影响实体可能需要依据适用的行业规则通知收单银行和相关支付卡品牌，并须聘用经 PCI SSC 认证的 PFI 来调查安全事件、确定根本原因并向相关方报告。

PFI 虽然不执行与 QSA 同等深度的 PCI DSS 合规评估，但会在调查过程中报告所发现的 PCI DSS 合规缺陷。PFI 调查报告中的判断、结论和发现必须完全基于调查中获取的事实证据，并反映 PFI 公司的独立判断。

PCI 取证调查（PFI）是通过严格规范且有记录的分析及调查技术，识别、收集、检查和保存数字证据的系统性操作过程。该调查方法将定义范围内的证据收集、解析和关联工作，与对组织整体合规状况的全面评估相结合，查明攻击者如何进入系统、涉及哪些系统、数据泄露的范围和深度。其主要目标是识别过去或当前的未经授权或异常的迹象，确定适用的监管和法律合规要求，并评估业务影响和风险。

3 哪些组织需要进行 PFI？

PFI 的适用范围涵盖支付产业链中的各类组织。根据 PCI SSC 的定义，“受调查实体”（Entity Under Investigation）是指“处理、存储或传输持卡人数据，且根据行业规则需要进行 PFI 调查的商户、服务提供商、金融机构或其他实体”。

具体而言，以下类型的组织均可能需要进行 PFI 调查：

商户（Merchants）：包括实体零售商户（面对面交易）、电子商务商户（线上交易）以及通过虚拟支付终端进行交易处理的商户。无论规模大小，一旦发生或疑似发生持卡人数据泄露，商户都可能被要求聘请 PFI 进行调查。该要求适用于所有 PCI DSS 合规验证类型（商户 1-4 级）和所有 SAQ（Self-

Assessment Questionnaire）类型，即使是使用 SAQ A 的小型商户，如果遭遇泄露，也可能需要进行取证调查。

服务提供商（Service Providers）：包括支付网关、支付处理商、第三方支付平台等为代表持卡人处理、存储或传输数据的组织。当服务提供商发生或疑似发生数据泄露事件时，调查范围需要识别并包含所有第三方连接，包括受影响的商户及其收单机构。

收单机构（Acquirers）：与商户有合同关系、负责处理支付卡交易的金融机构。收单机构在发现商户可能存在数据泄露时，会要求商户聘请 PFI 进行调查。

金融机构（Financial Institutions）：处理支付卡交易的其他金融机构。

此外，组织也可以主动邀请 PFI 公司执行独立的取证调查，以发现事件发生的原因，追踪事件的源头，并进行必要的整改和措施。

组织在以下情况下必须启动 PCI 取证调查：

- **已确认的数据泄露：**任何已知持卡人数据被未经授权的人员访问、窃取或泄露的事件。
- **疑似泄露：**有证据表明可能存在对持卡人数据环境的未授权访问的情况。
- **卡品牌通知：**当支付卡品牌或收单银行基于欺诈模式或其他指标要求进行调查时。
- **法规要求：**某些司法管辖区规定在特定类型的安全事件发生后必须进行调查。

调查必须由经 PCI SSC 认可的合格取证调查机构（PFI：PCI Forensics Investigator）执行，比如 atsec。PFI 的执行应涵盖特定要素：泄露时间线、受影响系统、受损数据范围、攻击途径和修复要求。

4 银行或卡品牌是如何知道数据泄露的？

如果您的合作银行或收单机构联系了您，您的组织很可能被识别为一个“共同购买点”（CPP: Common Point-of-Purchase）。当支付品牌（如 Visa、MasterCard、American Express、Discover、JCB 和银联）分析欺诈性卡片活动的报告时，如果发现多张被盗用的卡片曾在同一商户或同一服务提供商的系统环境中被使用，这些组织就会被列入 CPP 报告。基于这份报告，您的收单机构或卡品牌将会与您取得联系。

此时，数据泄露的原因是不得而知的，您需要聘请一家经 PCI SSC 认可的 PFI 机构来调查此次泄露事件，并告知您为保障支付卡环境安全所需采取的措施。

注：当多个欺诈交易被报告给支付卡品牌并确定源自同一位置即“共同购买点”时，便会启动 CPP 调查。“共同购买点”称为 CPP，即卡片在被欺诈性使用之前最后一次成功授权的位置。该位置可能发生了持卡人数据泄露。

5 为什么要配合调查？

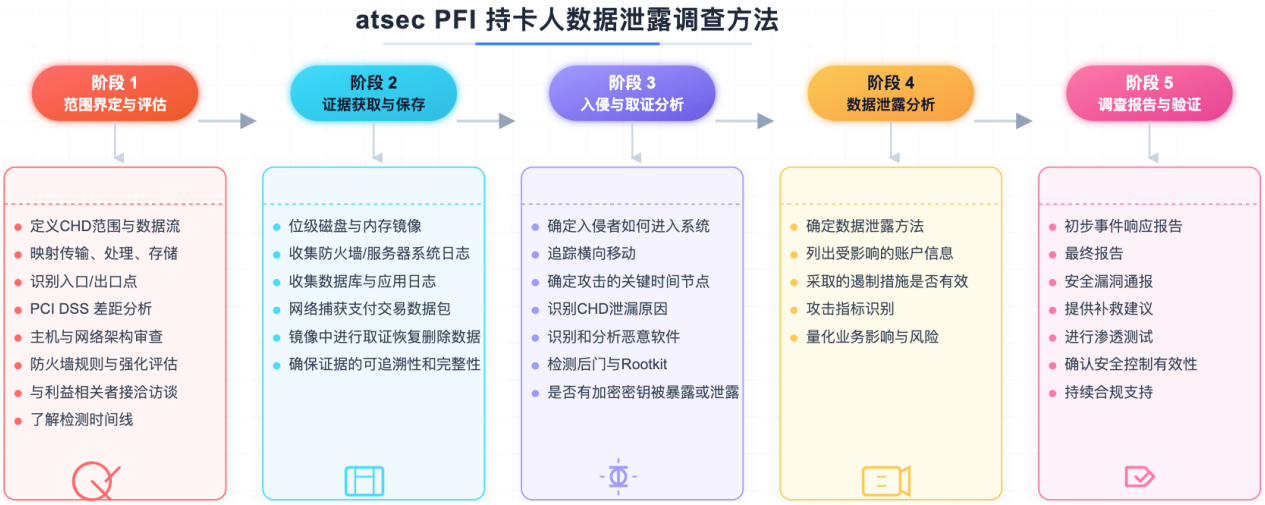
及时配合调查符合您的最大利益。任何延误都可能导致损害扩大，并增加您可能需要支付的相关罚款和费用。大多数卡品牌要求在发现疑似泄露事件后 24 小时内通知收单机构。您很可能会被卡品牌通过收单机构处以罚款，阻碍调查的推进可能会导致罚款金额增加。

您的支付系统现在很可能是一个“犯罪现场”，如果您的计算机系统继续运行，可能会破坏或污染证据，而这些证据恰恰有助于确定系统被入侵的时间、地点和方式。

此外，PCI SSC 明确指出，PFI 调查完成后必须出具最终报告。未能完成调查和报告可能导致进一步的合规问题，包括罚款、交易费用增加，甚至可能被暂停卡处理权限。

6 atsec PFI 的结构化方法

atsec PFI 采用一种结构化的方法来调查疑似的持卡人数据泄露事件，流程如下图所示：



具体步骤详细说明参见下述章节。

6.1 范围界定与合规性评估

确定调查的范围，绘制持卡人数据流图，并评估组织的安全和合规状况。

具体工作包括：

- **范围界定**：评估所有外部和内部连接点，包括各相关场所的网络接入点，以及第三方服务提供商的连接。适当的网络分段可以显著缩小泄露范围并降低调查复杂性。
- **持卡人数据流映射**：识别组织内持卡人数据的流向，确定数据在何处处理、存储和传输。
- **合规态势评估**：评估组织当前的 PCI DSS 合规状态，识别合规差距。
- **潜在调查位置识别**：包括持卡人数据存储位置、未经授权的访问点等。
- **网络访问控制评估**：检查被入侵系统与相邻网络之间的访问控制措施。
- **受影响支付卡品牌识别**：确定哪些卡品牌可能受到影响。

6.2 证据获取与保存

使用具有法律效力的取证技术收集数字证据，以确保其完整性和可采性。

具体工作包括：

- **证据获取**：使用开源、商业和专有取证工具从客户系统环境中获取证据。系统的证据收集包括从受影响系统获取日志文件、网络捕获、磁盘镜像和内存转储等。
- **在线分析**：分析系统内存、恶意软件、入侵时间线、文件和日志。
- **数据恢复**：从硬盘镜像中进行取证恢复，尝试从未分配磁盘空间、文件松弛区和隐藏文件中恢复已删除但尚未被覆盖且未加密的数据。
- **证据保全**：所有潜在电子证据必须在适合法庭审查和分析的平台上进行保全，维护严格的证据链记录，确保证据的可追溯性和完整性。

6.3 入侵与取证分析

分析收集到的证据，以重建攻击过程、识别攻击者的行为并确定数据泄露情况。此阶段可能随着新信息的出现需要额外的证据收集。

具体工作包括：

- **攻击路径重建**：确定入侵者如何进入系统、在系统内如何移动。
- **恶意软件分析**：识别和分析恶意软件，包括其功能、行为和数据捕获方式。
- **攻击时间线构建**：确定攻击的关键时间节点（入侵时间、数据窃取时间、恶意软件激活时间等）。
- **根本原因分析**：确定导致数据泄露的根本原因。
- **漏洞窗口确定**：确定系统漏洞的可被利用时间窗口。
- **加密密钥评估**：确定是否有加密密钥被暴露或泄露。

atsec 在 PFI 调查中采用的取证工具类别包括但不限于：

工具类别	主要用途与调查目标
磁盘与存储介质取证工具	对存储设备进行无损镜像采集，校验数据完整性；支持文件系统解析、已删除文件恢复，为分析提供可靠证据副本。
物理内存捕获与取证分析工具	捕获易失性内存，提取进程、内核模块、网络连接和加密密钥；重点用于检测无文件恶意软件、内存驻留后门及 Rootkit，还原内存级攻击痕迹。
网络流量取证分析工具	抓取并解析网络数据包，进行深度协议检测与会话重组；用于识别命令控制通信、数据外泄通道及横向移动路径。
持卡人数据与敏感信息扫描工具	通过模式匹配和校验算法扫描文件、数据库及日志中的主账号 PAN（Primary Account Number）等敏感数据，用于快速定位数据泄露范围。
日志聚合与关联分析工具	采集各类系统及安全日志，通过时序关联分析还原完整攻击链；识别初始入侵、权限提升及敏感数据访问等关键节点。
恶意代码静态与动态分析工具	对可疑文件进行反编译、反汇编提取特征，并在沙箱中动态执行监控行为；用于分析木马、Webshell 等，指导后续大规模排查。
综合性安全与取证工具集	集成系统信息收集、漏洞探测、密码恢复及数据恢复功能；快速获取系统基线，验证已知漏洞并辅助恢复关键证据。

取证分析技术手段：

- 文件、应用、网络和系统事件活动时间线分析。
- 已分配磁盘扇区、文件和目录的分析（用于恢复已删除数据），未分配文件系统空间分析。

- 文件系统二进制文件和可执行文件的深入分析（查找篡改或滥用痕迹）。
- 从损坏或无法使用的介质中恢复数据。
- 检查所有可能的位置（包括生产环境、备份、开发环境、测试环境等），确定持卡人数据是否被存储。
- 检查恶意软件输出日志，验证持卡人数据是否被捕获和存储。
- 审查各类日志：服务器应用日志、事务日志、排错日志、异常或错误文件、防火墙日志、防病毒日志、IDS/IPS 日志、Windows 事件日志、远程访问日志。

6.4 数据泄露分析

评估数据泄露的范围和方式，以支持违规通知和风险评估。

具体工作包括：

- **受影响账户识别**：确定每个受影响的卡品牌可能受影响的账户总数。
- **受影响账户清单**：列出受影响的账户信息。
- **数据曝光时间确定**：确定账户数据在系统上存储了多长时间，以及交易日期。
- **数据泄露方式确认**：确认持卡人数据是否不再存在风险或已从环境中移除。
- **遏制措施验证**：验证组织已采取的遏制措施是否有效。
- **攻击指标识别**：识别恶意工具包、恶意 IP 地址、匿名中继地址等威胁指标。如识别出威胁指标，PFI 必须通过安全渠道向受影响的支付卡品牌提交样本。
- **受影响支付卡品牌通知**：识别并通知受影响的支付卡品牌。
- **对于服务提供商**：需要确认并在最终报告中记录数据泄露与第三方服务提供商事件相关。

6.5 调查报告与验证

提交调查结果、建议和验证信息，以结束调查并改善安全状况。

具体工作包括：

- **初步事件响应报告**（Preliminary Incident Response Report）：在接案后 5 个工作日内交付，包含事件的初步评估、数据泄露的根本原因、泄露的范围和影响、事件时间线以及已收集的取证物证汇总。技术关键点在于速度与准确性的平衡——调查人员需在 5 天内完成初步的磁盘镜像采集、内存捕获和日志筛选，形成方向性结论，为后续深度调查指明路径。
- **最终报告**（Final Report）：该报告在调查完成后 10 个工作日内交付，要求得出完全基于事实证据的确定性结论。报告提供全面的根本原因分析，呈现经多源证据交叉验证的完整攻击时间线，并通过网络拓扑明确描述攻击者的攻击路径。调查范围需完整覆盖磁盘镜像、物理内存转储、网络流量、系统日志及恶意代码样本等全证据链，对账户数据类型（PAN、磁条数据、CVV/CVV2、PIN/PIN Block 等）进行详尽识别与分类，明确区分“环境中存在”与“实际泄露”的数据范围。PFI 还须对遏制措施的有效性进行独立验证，并系统化报告调查中发现的 PCI DSS 合规缺陷，将技术发现映射到具体合规要求。
- **安全漏洞通报**：调查过程中发现的任何安全暴露点或重大漏洞，在发现后第一时间通知客户。
- **合规验证**：验证持卡人数据是否已不再面临风险，安全控制措施是否已到位并正常运行。
- **持续合规支持**：调查完成后，协助组织持续满足 PCI DSS 合规要求。
- **对于无定论的调查**：提供详细分析和反馈，说明调查无定论的原因及发现问题的改善意见。

7 业务关系与责任

需要了解的是，根据卡品牌的不同，责任和赔付义务可能有所不同。最终对于取证结果的处置方法和业务层面的决策由卡组织和被评估机构沟通过协商决定，PFI 取证机构作为服务机构通过所获取的证据，以及上述技术方法进行原因分析，出具中立的取证报告。

通常来讲，收单机构和卡组织直接相连，收单机构有直接的责任确保商户和/或相关服务提供商 PCI DSS 的合规。

对于服务提供商和支付网关而言，情况可能更为复杂。服务提供商可能与多个收单机构、多个卡品牌以及众多下游商户存在业务关系。一旦服务提供商发生数据泄露，可能波及大量下游商户。

8 需要什么样的修复措施？

atsec 的 PFI 取证人员会在取证报告中为您提供具体的修复建议，并在整个取证过程中就如何提高信息安全防护与您深入沟通。

根据取证调查确认的情况，商户或服务提供商的验证级别的严格性可能会提升，您可能需要在至少 12 个月内满足更严格的 PCI DSS 验证要求，也即要求独立的 QSA（Qualified Security Assessor）公司的评估人员执行第三方的合规评估工作，而不能仅仅通过自评估 SAQ 实现合规。

完成取证调查工作后，您的第一步应该是确定内部谁来主导这个过程，这个人应具备一定的技术能力，能够理解或解读 PCI DSS 指南。

如果您使用外部 IT 服务提供商，请不要假设他们具备 PCI DSS 知识或已围绕 PCI DSS 指南构建您的支付环境。外包 IT 服务提供商同样需要符合 PCI DSS 要求，他们应能够提供相应的合规证明文件。

最佳实践建议：

- 维护全面的日志记录：确保持卡人数据环境中的所有系统生成详细日志，并集中收集和保留日志至少一年。高质量的日志数据将显著提高调查效率和准确性。
- 建立事件响应程序：制定并定期测试包含取证调查要求的事件响应程序。包括 PFI 的联系信息和明确的上报流程。
- 实施网络分段：适当的网络分段通过明确定义哪些系统可能受到影响来限制泄露范围并降低调查复杂性。
- 定期漏洞评估：主动的漏洞管理有助于预防泄露，并在需要调查时提供安全态势的宝贵文档。
- 文档标准：维护最新的网络拓扑图、系统清单和数据流文档。这些信息可大幅减少调查时间和成本。
- 证据保存培训：培训 IT 人员正确的证据保存技术，避免在调查员到达前污染证据。

9 总结

PCI 取证调查代表了支付卡行业合规相关的一个关键且复杂的技术体系。没有任何组织希望出现潜在的疑似泄露，从而触发取证调查流程，故而我们建议所有支付卡产业的相关组织都能够实现 PCI DSS 合规，从而最大限度地减少潜在安全或者数据泄露事件的发生。另一个层面，atsec 建议支付卡产业内各个组织能够提前理解 PFI 流程，有助于制定有效的事件响应程序并实施更强的预防性安全措施。

成功应对取证调查要求的关键在于准备：维护全面的日志记录、与合格的 PFI 建立关系、确保持续的合规状态、以及制定经过测试的事件响应程序。在这些准备措施上投入的组织能够更好地最小化安全事件的影响和所需调查的复杂性。

一旦出现了疑似的数据泄露，取证调查成本高昂且复杂度较高，也是 atsec 建议组织实现 PCI DSS 合规做到在事前防患于未然的原因。而 PFI 工作依然在一旦发生潜在泄露时，识别安全漏洞和预防未来泄露方面发挥着重要作用。通过专业取证分析获得的见解往往带来显著的安全改进，从而加强整体 PCI 合规并降低长期风险。

atsec 是经支付卡产业安全标准委员会（PCI SSC）认可的 PCI 取证调查机构（PFI），目前在亚太、美国及加拿大地区执行 PFI 取证调查。atsec 的团队在支持各类组织（包括商户、支付网关、服务提供商和金融机构）处理持卡人数据泄露方面拥有丰富经验。如果您希望通过取证调查来确定事件的原因，或者已被要求聘请 PFI，atsec 随时准备提供协助。

请注意：根据独立性要求，执行 PCI QSA 合规评估的机构不应同时担任组织的 PFI 取证调查服务机构。然而，在 PFI 取证调查完成后，atsec 依然作为 QSA 可以协助您完成 PCI DSS 的合规。

参考文献

[1] PCI-DSS v4.0.1: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

[2] PFI Program Guide v3.3: https://docs-prv.pcisecuritystandards.org/Programs%20and%20Certification/PCI%20Forensic%20Investigator%20(PFI)/PFI_Program_Guide_v3.3.pdf

[3] PCI Guidance on responding to a Data Breach: https://www.pcisecuritystandards.org/documents/Responding_to_a_Cardholder_Data_Breach.pdf

[4] atsec website: https://www.atsec.com/