Responding to a Data Breach

A How-to Guide for Incident Management

Preparing for the worst is the best defense. This guidance will help merchants and service providers in the event of a data breach by outlining how to plan in advance for incident response and how and when a Payment Card Industry Forensic Investigator (PFI) can be engaged to assist.

Only PFIs listed on the PCI SSC website are approved to provide specific forensic investigation services.

A data breach now costs organizations an average total of $3.8 million (over €3.3 million). Is your business prepared to mitigate a compromise and its impact on your bottom line and reputation? Research shows that having an incident response team in place can provide significant savings[1].

PREPARING FOR THE WORST IS THE BEST DEFENSE

IMPLEMENT AN INCIDENT RESPONSE PLAN

Criminals are relentless; as a result the payment industry has seen many cardholder data breaches. Your organization needs to prepare for the worst by ensuring effective incident-management controls are in place. PCI DSS Requirement 12.10 is key in this effort: It requires entities to "Implement an incident response plan. Be prepared to respond immediately to a system breach." Guidance in this PCI DSS requirement notes that such a plan should be "thorough, properly disseminated, read, and understood by the parties responsible"; and include proper testing at least annually to ensure the process works as designed and to mitigate any missed key steps to decrease exposure.

Implement an incident response plan. Be prepared to respond immediately to a system breach.

LIMIT DATA EXPOSURE

Limiting data exposure and minimizing data loss while preserving evidence is a must. For example, make sure you know how to isolate a system without simply powering it off. Turning it off may make investigation more difficult and remove answers you need. See "Working with your PFI" (page 3) for more information on evidence preservation.

NOTIFY BUSINESS PARTNERS

Alert necessary parties immediately. Have a plan and ensure contact information of these parties is regularly validated. This plan will include payment card brands, acquirers (merchant banks), and any other entities that might require notification, whether by contract or law.

MANAGE THIRD-PARTY CONTRACTS

Ensure all contracts with third-party service providers, hosting providers, Integrators and Resellers, and other relevant parties sufficiently address incident-response management. Contracts should include specific provisions on how evidence from those environments will be accessed and reviewed, such as allowing your PFI access to the environments.

IDENTIFY A PFI

Some PFIs offer their services on retainer; you may want set up such an agreement so that you have a PFI company ready to call if you need them. But remember... PFIs must meet strict independence requirements—so you cannot use the same company you are already using for other PCI services, even if that company is also a PFI.

$3.8 MILLION
(MORE THAN €3.3 MILLION)
The average total cost of a data breach

1: Source: 2015 Cost of Data Breach Study: Global Analysis

PCI Security Standards Council

ENGAGING A PAYMENT CARD INDUSTRY FORENSIC INVESTIGATOR (PFI)

WHEN TO ENGAGE A PFI

If a cardholder data breach has occurred or is suspected, the payment brands may require an independent forensic investigation to be completed by a PCI-listed PFI*. You'll need to understand their role and engage effectively with the PFI should an investigation be necessary.

Acquirers and the payment brands all have their own rules and thresholds for when a PFI must be engaged, and you must contact them in order to make this determination. See Payment Brand Resources (page 3) for more on how to contact your acquirer or payment brand.

WHAT TO EXPECT FROM YOUR PFI AFTER A DATA BREACH

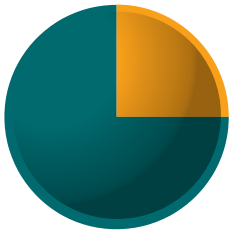
Perhaps your acquirer notified you of a suspected breach or you detected it and contacted the acquirer or payment brands yourself. Either way, you may be required to engage the services of a PFI. Understanding the role of a PFI and how to engage effectively is vital for successful incident management. Keep in mind the following considerations when selecting a PFI:

- PFIs are required to be independent of the entity they are investigating. When choosing a PFI, make sure your company has no other relationships with them. For example, if your Qualified Security Assessor (QSA) also happens to be a PFI, they cannot perform your investigation. Other forensic investigators (i.e., non-PFIs) or any other outside consultants (legal counsel, etc.) hired by or representing your company must not interfere with the PFI's investigation. The PFI must perform their own investigation and cannot accept reports from outside consultants.
- PFIs provide a 24x7x365 first level of phone and incident response for the regions in which they operate and must be able to initiate an investigation within five business days of an agreement being signed. Choose a PFI listed for the region in which you think the data loss has originated.
- The investigation will be supervised by a Lead Investigator and may be conducted remotely or onsite. If the investigation is remote, the PFI will give detailed instructions on how to securely transfer evidence for examination in the PFI's laboratory environment.
- The PFI looks at your environment from a different perspective than your QSA, Internal Security Assessor (ISA), or even your own self-assessment efforts. As such, what may have been defined as the PCI DSS or cardholder data environment (CDE) scope previously may need to be extended for the PFI investigation to find the root cause of the intrusion. The PFI will determine the scope of the investigation and the relevant sources of evidence.
- Your PFI will perform extensive investigation and reporting in order to understand what happened in your environment, and you can expect to receive a PFI Preliminary Incident Response Report and a PFI Final Incident Report (both on the PCI SSC's mandatory reporting template), which will also be provided to your acquirer (if you have such a contract) and the payment brands.
- For the vast majority of investigations, the PFI will not perform a full PCI DSS assessment, however the PFI will report as to whether there were deficiencies in requirements observed during their investigation. Understand: This does not constitute a full PCI DSS assessment; nor is a lack of findings evidence of PCI DSS compliance.
- If a PIN compromise is suspected, the PFI will perform a PIN-security and key-management investigation and a PCI PIN security assessment.

WHAT SUPPORT WILL A PFI PROVIDE?

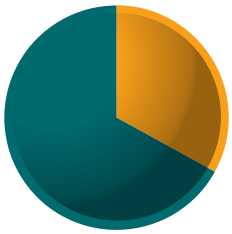
Based on their findings, the PFI will make recommendations on how your organization should prioritize containment and secure cardholder data. Those recommendations are intended to complement your internal incident response plan, and it is important that they are implemented as soon as possible to reduce the risk of further data loss—or even a second breach.

Based on their findings, the PFI will make recommendations on how your organization should prioritize containment and secure cardholder data.



ONLY 25%

of UK businesses believe their organisation could detect a data breach at any time*



ONLY 33%

of UK businesses rated their organisation as very good or excellent at detecting and containing breaches*

* Source: 2015 State of Data Security Intelligence study

PCI Security Standards Council

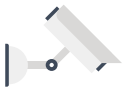
WORKING WITH YOUR PFI

To complete a thorough and effective investigation, the PFI will require access to data, facilities, and people. This may also include access to third-party service providers who store, process, or transmit cardholder data on your behalf or who can otherwise affect the security of the cardholder data environment–e.g., website hosting providers.

When a breach occurs or is suspected, it is critical to preserve the evidence. It is very tempting to reboot all devices, clear up log files, remove any suspect software, and generally try to recover as quickly as possible. Of course, everyone wants to "stop the bleeding" and prevent any more data being compromised. However, careful preservation of evidence is vital both in finding the root cause of the breach and in identifying the perpetrators. Digital evidence is easily contaminated, and maintaining a robust chain of custody is crucial to achieving a good investigation result.

EVIDENCE PRESERVATION

1. Do not access or alter compromised system(s)–i.e., *don't log on at all* to the compromised system(s) and change passwords; do not log in as ROOT. To avoid losing critical data, it is highly recommended the compromised system not be used.
2. Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (i.e., unplug network cable).
3. Preserve all evidence and logs–i.e., original evidence, security events, web, database, firewall, etc. Ensure the integrity of the evidence is not impacted by any tools used in the collection and analysis process.
4. Document all actions taken, including dates and individuals involved.



FACILITIES

The PFI will determine what facilities need to be visited and/or reviewed, and it is important that the compromised entity understands access to the facilities may provide vital insight into what actually happened. As mentioned earlier, this access can be particularly tricky when facilities include third-party service providers. Proactive work with these parties is important to ensure that a PFI has the needed access to the third party site, whether physical or remote, in order to adequately conduct the investigation.

PEOPLE

Ensure that appropriate employees–e.g., CTOs, network administrators, IT security managers–are available to meet with the PFI in a timely manner. Employees should be open, honest, and have an understanding of the role of the PFI. The PFI is not there to apportion blame; they want to find out what has happened and help the organization recover **quickly**.

FEEDBACK

PFIs are required to give their customers a feedback form, which can be submitted directly to PCI SSC. PFIs are subject to a quality assurance program operated by PCI SSC, and all feedback is welcome as input to this process.

PAYMENT BRAND RESOURCES

- Visa EU: Data Compromise Procedures
- Visa, Inc: Data Compromise Procedures
- MasterCard: Account Data Compromise Best Practices
- American Express: Data security is good business
- JCB
- Discover: Network Data Security, email

USEFUL REFERENCES

- The PCI SSC Documents Library
- Supplement for PCI Forensic Investigators
- PFI Program Guide
- A Guide to Forensic Readiness for Organisations, Security Advisors and Lawyers
- ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence
- CERT Incident Management
- ACPO Good Practice Guide for Digital Evidence
- Best Practices for Victim Response and Reporting of Cyber Incidents, Cybersecurity Unit, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice