ALSTON&BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM APRIL 22, 2013

Breach Investigations, Part 2: Understanding the Role of the PFI in Payment Card Breaches

By Kim Peretti

This article is the second in a four-part series describing some of the challenges to conducting breach investigations in response to increasingly sophisticated attacks. In Part 1, entitled Right-Sizing the Data Breach Investigation and published with *Law360* on March 26, 2013, we provided an overview of the evolving advanced cyber threat landscape and the three common breach response scenarios (internal investigations to fix technical problems, investigation to assess payment card exposure, and investigations to determine compliance with state data breach notification statutes). This Part 2 takes a closer look at responses involving payment card breaches—both because of their unique nature and their potentially grave implications. The third article will discuss both the need for, and requirements of, an "enterprise impact" investigation in appropriate circumstances. Finally, the fourth article will present hallmarks of an effective enterprise impact investigation.

Many of the highly visible data breaches of the last decade have involved unauthorized access into systems where the criminal actor targets customer credit and debit card numbers that are either stored in databases or transmitted across the wires as part of financial transactions. These types of breaches are prevalent, in large part, because of the flourishing criminal underground (known as "carding") that has created a black market for the theft and resale of stolen card numbers, which criminals use for financial gain. Companies that experience breaches involving payment cards are subject to a set of industry rules formulated by a governing body comprised of the major payment card brands. These rules dictate the response that must be taken by the compromised entity and limit the role of the victim company in this response. While there may be many positive aspects of this process, it should be noted that the intended purpose of these investigations is to minimize potential fraud losses to exposed cards and determine compliance with industry rules related to data security. Companies should be mindful that the dictated response may not necessarily include all of the activities necessary to investigate, assess, and address the broader impact of the breach to the enterprise.

I. PFI Investigations

Entities that store, process or transmit cardholder data, such as credit and debit card numbers, are required to comply with a set of industry security standards published and managed by the Payment Card Industry (PCI)

Security Standards Council (PCI SSC).[1] In addition to promulgating a set of data security standards (PCI DSS),[2] the PCI SSC has developed a set of industry rules governing responses to payment card data breaches. These rules, known collectively as the Payment Card Industry Forensic Investigator (PFI) program, were intended to replace the programs established by the individual card brands.[3] The rules require an entity to notify the affected card brands (e.g., Visa, Mastercard) in the event of a compromise to a company's system that exposes cardholder account information to third parties.[4] After notification to the brands, the brands may require the compromised entity to engage a PFI to conduct an independent forensic investigation.[5] PFIs are specially trained and qualified forensic investigators that must be approved by the PCI SSC. At a minimum, PFIs must be Qualified Security Assessors, or individuals specially trained in payment card compliance with the PCI DSS. Once approved as a PFI, the company will be included on a PFI list on the PCI SSC website and able to be selected by entities subject to a payment card breach. As of the date of this article, there are 18 companies on this list.[6]

While the compromised entity separately engages the PFI and is responsible for all fees and expenses associated with the PFI's investigation, the PFI conducts the investigation on behalf of the third-party card brands and with their direct involvement. Under PFI rules, each of the payment card brands are responsible for "defining requirements regarding the use of PFIs and the disclosure, investigation, and resolution" of the security incident, which affords them wide latitude in directing and controlling key aspects of the data breach response process.[7] In contrast, PFI rules attempt to minimize involvement of the victim company in the response, stating outright that the company is not to control or direct the investigation.[8]

One key aspect of any forensic investigation is the documentation of the event with an investigation report. Breach investigations are necessarily messy. Until the investigation is over, the facts of how the compromise occurred, how many systems were compromised, what was on those systems and could potentially be exposed, whether and how much data was taken out of the environment and whether the security incident is ongoing are likely to be under constant flux. Indeed, at the end of the investigation, while there may be some facts not in dispute, many are subject to interpretation and guided by assumptions (hopefully based on deep and broad experience) of the investigator of who the bad actors are, their motives and what types of tactics, methods and

---

1 The Council is comprised of five founding global payment brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

2 The PCI DSS consist of a set of 12 security requirements and sub-requirements that provide a baseline of technical and operational requirements designed to protect cardholder data. For a library of relevant PCI DSS documents, *see* https://www.pcisecuritystandards.org/security_standards/documents.php.

3 *Payment Card Industry PCI Forensic Investigator Program Guide, Version 1.0*, September 2010 (hereinafter "PFI Program Guide").

4 The term "compromise" refers to a process that exposes cardholder account information to third parties, placing cardholders at risk of fraudulent use. Appendix C: Glossary of Terms, *PFI Program Guide*.

5 *What To Do If Compromised, Visa Inc. Fraud Control and Investigations Procedures, Version 3.0*, May 2011, p. 9.

6 https://www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php.

7 Visa separately states in its incident response guidance that it "has the right to engage a PFI to perform a forensic investigation as it deems appropriate." *What To Do If Compromised, Visa Inc. Fraud Control and Investigations Procedures, Version 3.0*, May 2011, p. 22.

8 Appendix A: Forensic Investigation Guidelines, PFI Program Guide. To ensure compromised entities fully understand this limitation, the PFI rules further require that the company acknowledge and agree in its contract with the PFI that "the investigation is being carried out as part of the PFI Program, that all PFI Report investigation shall be shared with affected Payment Card Brands throughout the investigation and that the *investigation is not to be directed or controlled in any way by the Compromised Entity.*" *Id.*

techniques the particular bad actors often employ. Certainly, because these investigations can be as much art as science, in any investigation with multiple investigators, there will likely be varying interpretations of key facts.

In payment card breaches, the PFI rules afford the payment card brands direct and significant involvement in the reporting component of the response process. PFIs are required to produce both a preliminary and final incident response report to the card brands, as well as, upon request, all investigatory work papers and report drafts.[9] Templates for these reports are provided as part of the PFI program.[10] Importantly, one section in the Final Incident Report template is entitled "PCI DSS Compliance Status."[11] This section requires the PFI to "check" whether each of the 12 basic security requirements under the PCI DSS were in place at the time of the incident and whether that particular control contributed to the security breach. Thus, what companies may not realize at the outset of this process is that the investigator they hire will not only be conducting an investigation to determine the risk of payment card exposure from the data breach, but also assessing the company's compliance with the PCI DSS. Obviously, an inquiry into and documentation of a company's noncompliance with the PCI DSS can have significant and unfavorable consequences for the organization, such as providing a basis for regulator inquiries and class actions and other types of litigation, and removal from the card brands' lists of approved entities to store, process and transmit cardholder data, among other consequences.

Moreover, if the company disagrees with any of the findings of the PFI, it has little ability to dispute the facts documented by the PFI prior to unfavorable facts being turned over to third parties. PFI rules require the contract to specifically provide the PFI with the authority to deliver all final and draft reports and PFI work papers to the card brands *at the same time* as the reports are sent to the victim company.[12] Essentially, victim companies can comment on the draft and final reports (and theoretically do not have to approve the report), but any facts regarding the investigation with which the victim company fundamentally disagrees will be part of the documentation and provided, at a minimum, to some external parties. In contrast, the PFI rules provide the card brands with greater input and control with respect to the documentation of the security incident, including approval rights over all PFI reports and the ability to reject any report that does not conform to all applicable requirements, such as templates and use of proper scoping methodology.[13] Given that, as stated above, forensic facts in complex, technical investigations can be subject to interpretation, the company's diminished role in the process can prove to be an unexpected obstacle in working with what is sometimes believed to be an independent investigator engaged to determine the true nature and scope of the data breach.

---

9 *PFI Program Guide*, p. 6. Provide a preliminary forensic report to Visa within five (5) business days from the onsite review. Provide a final forensic report to Visa within ten (10) business days from the completion of the review. Visa compromised document, p. 22. App A: Forensic Investigation Guidelines, *PFI Program Guide*.

10 *See Report Templates and Aids for PFI Investigations*, November 2012, available at https://www.pcisecuritystandards.org/security_standards/documents.php.

11 *Id.*

12 *PFI Program Guide*, Appendix A: Forensic Investigation Guidelines.

13 *PFI Program Guide*, p. 7.

II. The Case for a Parallel, Company-Directed Investigation

As detailed in Part I of this series, sophisticated criminal actors—including those committing payment card breaches—often compromise hundreds of systems within a single company's environment. Such actors have the capability to conduct targeted, well-orchestrated, prolonged and repeat attacks on businesses. Given the potential for a far-reaching compromise and the deep level of access obtained by the criminals in payment card intrusions, companies need to be mindful that a PFI response may not necessarily include all of the activities necessary to assess and address more holistic risks for the enterprise. The critical point here is that the PFI's investigation is technically limited to the card processing environment and its investigation may fall well short of the entire story of the breach.

Some questions left unanswered by a PFI-focused investigation could be: Were the perpetrators solely interested in card data? What other types of information might the perpetrators have been targeting? What was the full scope of the compromise as it relates to environments other than the PCI environment? Were financial controls impacted? Was the company's sensitive data, intellectual property and client data impacted by the breach? While these questions may surface in the investigation, they are not the focus of the PFI and are often left unanswered.

Indeed, if the breach expanded beyond the payment card environment and targeted information other than payment card data, the company would not want the PFI to broaden its investigation. By way of example, if the financial controls were impacted, the company would not want that fact in a non-privileged document circulated to multiple third parties at the same time as it was reviewed by the company. A similar situation would exist if key research and development plans or customer contracts were exposed. Clearly, even if the victim company could require the PFI to conduct a broader investigation under the PFI rules, there are obvious reasons why it would not want to pursue this course. Data breach investigations, similar to other types of internal investigations, can—and often do—reveal certain sensitive information that the organization should attempt to protect, to the extent possible, by the attorney-client privilege.

This confluence of factors—PFI-focused investigation on cardholder environment, lack of meaningful process to dispute key facts, possible broader impact to enterprise from the incident, need to protect sensitive aspects of the investigation by the attorney-client privilege—demonstrate the need for a company to engage a non-PFI forensic investigator to conduct an independent, company-directed investigation when appropriate. This investigation would be conducted under privilege (i.e., at the direction of in-house or outside counsel) and focused on conducting an investigation to determine the full impact of the breach to the enterprise. Of course, the increased cost of hiring an additional investigator and challenges in coordination of multiple parties can be hindrances to this process. However, especially when dealing with advanced threat actors, the benefits of two sets of eyes on facts subject to interpretation, as well as at least one set aimed at determining the enterprise impact, can go a long way in minimizing the risk posed by advanced criminal actors who may attempt to revisit the enterprise for further exploitation, as well as that posed by regulators and class-action plaintiffs probing into details of the company's response.

This article was previously published by ***Law360.***

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com | alstondatabreach.com