ALSTON & BIRD

WWW.ALSTON.COM

CYBER ALERT ■

FEBRUARY 27, 2019

Retailers Beware: Navigating Through Assessments and Appeals from the Card Brands

By Jim Harvey, Kim Peretti, and Larry Sommerfeld

Some of the most highly publicized and scrutinized data breaches involve the theft of payment card data. In recent years, the payment card industry has implemented new technologies, most visibly EMV, in an effort to stem the tide of payment card data theft and fraud. Despite these efforts, such activity remains common.

Imagine making it through the life cycle of an incident response crisis. The company has devoted substantial resources to responding to and investigating the incident—perhaps through hiring both a payment card industry forensic investigator (PFI)[1] and privileged investigator, mitigating and remediating any vulnerabilities that may have led to the security incident or that may otherwise have been discovered during the investigation, and notifying the public and numerous state and possibly federal regulators. The company is also in the midst of defending any securities or class action lawsuits that may have been filed. After all this, correspondence arrives from various card brands raising the prospect of assessments ranging in the six or seven figures. In these circumstances, the company would be well-served to consider the process behind these assessments ahead of time, and certainly well before the investigation is complete, so that the company can respond appropriately.

Current Threat Landscape

Both point-of-sale malware (for use in attempted intrusions) and stolen payment card data (for use in fraudulent transactions) are readily available for sale in underground forums, and the theft of payment card data is big business for some of the most sophisticated and active cybercrime groups. According to the 2018 Verizon Data Breach Incident Report, point-of-sale and skimming incidents account for a significant portion of incidents in the retail sector and for over 90% of all incidents within the accommodation and food services sector. Cybercriminals continue to successfully target online transactions as well, such as by compromising systems and making unauthorized code modifications in payment applications.

[1] In an earlier client alert, "Breach Investigations, Part 2: Understanding the Role of the PFI in Payment Card Breaches," we discussed particular aspects of investigating payment card breaches, including the role of the PFI and strategies for companies to consider in such investigations.

Like many cyber intrusions, payment card breaches often begin with well-known hacking techniques, such as spear phishing, credential escalation, and installation of backdoors and malware. Nevertheless, payment card breaches tend to attract a disproportionate amount of public and regulatory scrutiny and litigation. In short, not only do point-of-sale "brick and mortar" breaches continue to occur despite advances in technology, but breaches involving e-commerce payment systems also continue to become increasingly more sophisticated.

Investigations of Payment Card Breaches

Companies that experience breaches involving payment cards are subject to a set of industry rules formulated by a governing body, the Payment Card Industry Security Standards Council (PCI SSC), composed of the major payment card brands. These industry rules, coupled with specific rules established by each card brand, dictate the response that a compromised company must take and limit the role of that company in its response. The purpose of these investigations, from the card brand perspective, is to minimize potential fraud losses to exposed cards, assist banks with a portion of any recovery for reissuance costs, and determine merchant compliance with industry rules related to data security.

Among other things, the PCI SSC has established the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS consists of 12 broad security requirements with numerous subrequirements that are meant to provide a baseline of technical and operational requirements designed to protect cardholder data. Separately, the card brands also maintain specific rules governing responses to payment card data breaches. These rules require companies to notify the affected card brands when discovering a compromise that exposes payment card information. After being notified, the card brands may require the compromised company to engage a specially trained and qualified forensics investigator, known as a PCI forensic investigator (PFI). PFIs must be approved by the PCI SSC. Once approved as a PFI, the forensics investigator will be included on a PFI list on the PCI SSC website. Currently, there are 20 companies listed.

Importantly, while the compromised company 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 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 PFI Companies and the disclosure, investigation, and resolution" of the security incident, which affords them a wide latitude in directing and controlling key aspects of the data breach response process. In contrast, PFI rules make clear that the compromised company is not to control or direct the investigation. The PFI rules require that the compromised 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 information shall be shared with affected Participating Payment [Card] Brands throughout the investigation and that the investigation is not to be directed or controlled in any way" by the compromised entity.

The PFI, in turn, is required to produce both a preliminary and final incident response report to the card brands that follow templates that are part of the PFI program. Within the final report, the PFI evaluates the compromised company's PCI DSS compliance status, opining on whether each of the 12 basic security requirements under the PCI DSS were in place at the time of the incident and whether each particular control

may have contributed to or caused the security breach. Critically, therefore, the PFI not only investigates and reports to the card brands the risk of payment card information being exposed due to the breach, but also undertakes a partial audit of the company's compliance with the PCI DSS.

A company that disagrees with any of the findings of the PFI has little ability to dispute the facts documented by the PFI before disclosure to the card brands. PFI rules require the contract with the compromised company 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 the reports are sent to the victim company. The card brands have approval rights over all PFI reports and the ability to reject any report that in their view does not conform to all applicable requirements.

In sum, a company suffering a compromise involving payment card information may be ordered to retain a PFI, but the PFI investigation is conducted under the control of the card brands and extends beyond the circumstances of the breach, entailing an evaluation of the company's compliance with the PCI DSS. For these reasons, companies may choose to engage a second forensics firm to conduct a parallel investigation under privilege and under their own control.

Assessment and Appeal

The PFI final report does not necessarily end the matter, since the card brands may seek to impose an assessment on the compromised company. Each card brand operates independently in this regard, with its own set of rules, and each card brand may levy its own potentially substantial assessment. And the card brands enjoy a wide latitude in interpreting their own rules and determining assessments. But while the card brands ultimately hold significant leverage in determining the amount and appropriateness of assessments, these assessments may be challenged.

Assessments are potentially triggered by a number of factors, generally boiling down to a finding by the PFI of a PCI DSS deficiency in combination with a sufficient number of cards at stake. So, for example, an assessment under Visa's Global Compromised Account Recovery (GCAR) program is triggered by an account data compromise (ADC) event—that is, an event in which Visa account data is at risk—when a list of specified criteria are met. Among these criteria are a violation of the PCI DSS, a high enough number of compromised cards, and an amount of operating expense recovery (e.g., the cost of reissuing cards). Mastercard and American Express potentially trigger assessments based on the occurrence of a security incident involving cardholder data and a specified number of cards.

Once triggered, assessments cover roughly three types. First, assessments include an amount based on a failure to abide by the PCI DSS. The PFI report template includes a section entitled "PCI DSS Compliance," where the PFI will set forth its list of PCI DSS deficiencies and will also include whether each may have caused or contributed to the breach. Importantly, even if a PCI DSS deficiency found by the PFI had nothing to do with the breach, the finding may still form the basis of an assessment. Companies should be aware that despite any records of compliance the company may have had in place, in most cases the PFI will nevertheless find some deficiency related to PCI DSS compliance.

Card companies next impose an assessment premised on operating losses, such as costs to issuers. These assessments are based on the number of cards at stake and may also be based on the types of cards and types of transactions, depending on the particular card brand at issue. The amount per card may further vary depending on the size of the issuer. For example, Mastercard's operational assessments range from $3.75 per card for a large issuer to $7.25 per card for a small one for each at-risk chip card. These calculations add up quickly and are often the source of the bulk of the assessment. Lastly, Mastercard's rules also provide that Mastercard may seek fraud recovery for fraud attributable to an ADC event.

Note that card brand rules provide for reductions or a safe harbor based on a company's use of certain advanced anti-fraud technologies, such as EMV. For example, Mastercard has safe harbors generally based on the extent to which a company's annual total transaction count was processed through terminals capable of processing both chip and magnetic strip transactions, among other technical requirements. The requirements for safe harbor qualification vary, and indeed, installing advanced technology such as EMV may not be enough to trigger a safe harbor, particularly if the card brand determines that the company processes transactions by swiping or manual entry, thus circumventing the anti-fraud technology.

There are also methods to challenge these assessments. In particular, both the Visa and Mastercard rules expressly provide for an appeal mechanism. Challenges must be based on the specific grounds identified within each set of card brand rules, as updated and as applied at the time of the breach. Of course, just as with the PFI and assessment processes, the card brands have a wide degree of discretion in this area, and their decision on appeal is final. And unlike in litigation, there is no public precedent to guide the arguments. Companies facing an assessment nonetheless have the opportunity to present their position and argue that the assessment was improper. To do so, and to help develop and navigate an appropriate and strategic response, they would be wise to consider, potentially with the benefit of counsel, the complexities of the rules and how to apply those rules to the specific circumstances of their particular case.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com
Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us: @AlstonPrivacy | www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, TX 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ 5th Floor ■ East Palo Alto, CA 94303-2282 ■ 650-838-2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333