BCLP. Client Intelligent

Insights

DATA BREACH LITIGATION PREPARATION: WHAT ARE THE REQUIREMENTS FOR PAYMENT CARD BREACHES?

Feb 11, 2020

As of January 1, 2020, California became the first state to permit residents whose personal information is exposed in a data breach to seek statutory damages between $100-$750 per incident, even in the absence of any actual harm, with the passage of the California Consumer Privacy Act ("CCPA"). The class actions that follow are not likely to be limited to California residents, but will also include non-California residents pursuing claims under common law theories. A successful defense will depend on the ability of the breached business to establish that it implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information held. The more prepared a business is to respond to a breach, the better prepared it will be to defend a breach lawsuit. To help our clients prepare for the CCPA, Bryan Cave Leighton Paisner is issuing a series of data security articles to empower organizations to focus on breach readiness.

Unique Issues Relating to Payment Card Breaches

Additional considerations should be analyzed when an organization is affected by a breach involving payment card information (*e.g.,* debit or credit cards). According to one study, the retail, hospitality, food and beverage, and health care industries are most vulnerable to attacks involving payment card information, whether through a physical card reader or through e-commerce.[1] If your organization accepts payment cards, and card information is the subject of a data breach, you may have additional obligations to notify your payment processor, merchant bank, or the payment card brands.

Visa and Mastercard cards are processed through a four-party system. Visa and Mastercard enter into licensing arrangements with various financial institutions called "issuing banks" that issue payment cards to cardholders. The issuing bank collects payment from the cardholders through their monthly payment card statements or via withdrawal from their bank account where debit cards are used. Retailers or merchants who accept Visa or Mastercard contract with other financial institutions called "merchant banks." Merchant banks and retailers in turn typically enter into contracts with payment card processors to process the card transaction and collect payment from a cardholder's issuing bank.

In the four-party system, the merchant banks have contracts with Visa or Mastercard and agree to follow Payment Card Industry Data Security Standards (PCI DSS). A merchant bank will typically have a separate contract with a merchant (directly or through a payment processor) that, in turn, requires the merchant to indemnify the merchant bank if there is a data breach and Visa or Mastercard imposes a liability assessment on the bank or processor. Accordingly, an organization impacted by a payment card breach usually is required to notify its merchant bank or payment processor within 24 hours of discovering the breach. The merchant bank is then required to notify Visa or Mastercard.

The Payment Card Industry has set forth a specific set of guidelines that often are incorporated in the various payment card contracts and must be followed in the event of a suspected incident involving payment card data. An organization should review both its contracts with the merchant bank or payment processor and the PCI rules on breach notification to ensure compliance. The PCI rules may require that the merchant retain, at its own cost, a PCI-certified forensic investigator to investigate the breach and determine whether the merchant's security systems were in compliance with PCI requirements.

Tip: An organization may wish to retain, through its legal counsel, a private forensic investigator to do its own parallel investigation, since the PCI investigator is required to report its findings to the payment card brands. The private investigator will provide the organization with the ability to contest the PCI investigator's findings.

Discover and American Express transactions are processed through a three-party system. Discover and American Express typically contract directly with a merchant who accepts those cards. In the event of a breach involving those brands, the merchant should consult its contracts with Discover and American Express and any regulations issued by those brands and follow all notification requirements. Generally, notification is required to be made to the brands immediately or within 24 hours.

Merchants should be advised that the brands may request or require prior review of any breach notification letters that will be sent to affected consumers.

BCLP is working with clients to assess – and mitigate – risks by putting in place the policies, procedures, and protocols needed to address data security breach issues.

---

1. Trustwave Holdings, Inc., Trustwave Global Security Report (2019)

RELATED PRACTICE AREAS

- Data Privacy & Security
- California Consumer Privacy Act

MEET THE TEAM

Linda C. Hsu

Los Angeles

linda.hsu@bclplaw.com
+1 310 576 2192

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2024 Bryan Cave Leighton Paisner LLP.