Global Data Privacy and Security Team

Bryan Cave's Global Data Privacy and Security Team has responded to hundreds of data security breaches and routinely help clients, before a breach happens, analyze and improve upon their ability to respond to a breach if (or when) one occurs.

For more Information Contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
T: +1 202 508 6000

One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302-5386 USA
T: +1 303 444 5955

Courtney K. Stout
Associate
courtney.stout@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
T: +1 202 508 6076

To join Bryan Cave's data privacy and security distribution list visit Bryan Cave Data Matters.

BRYAN CAVE

Charging Retailers For Data Breaches: Credit Card Breaches At A glance

For most retailers credit cards are the primary form of the payments that they receive. Accepting credit cards, however, carries significant data security risks and potential legal liability. In addition to the normal repercussions of a data security breach – i.e., reputation damage, the risk of class action litigation, and the risk of a regulatory investigation – if a retailer's credit card system is compromised the retailer may be contractually liable to its payment processor, it's merchant bank, and ultimately the payment card brands (e.g., VISA, MasterCard, and American Express). In many cases that contractual liability surpasses any other financial obligation that arises from the breach.

The following provides an overview of credit card data breaches:

The number of separate contractual penalties, fines, adjustments, fees and charges that the credit card brands may assess upon a retailer.[1]	Largest number of credit card numbers impacted in a single breach in 2014 or 2015.[2]	Percentage of data breach class actions that relate to credit card data.[3]
26	**56** MILLION	**73%**

Factors retailers should consider when preparing to respond to a credit card data breach:

- ☑ Does your payment processing agreement cap or limit your contractual liability in the event of a data breach?
- ☑ Does your payment processing agreement cap or limit your processor's liability in the event that they suffer a data breach?
- ☑ Do you have a contractual obligation to notify your payment processor or merchant bank in the event of a possible security breach?
- ☑ Have the vendors of your point of sale equipment provided you with appropriate indemnification in the event of a breach caused by their equipment?
- ☑ Is a reporting structure, and contact information, included in your incident response plan?
- ☑ Are there any deficiencies identified in your organization's latest "Report on Compliance."
- ☑ If you have cyber-insurance are there any exclusions that would impact its coverage for credit card related breach costs?
- ☑ If you have cyber-insurance is there a sub-limit for PCI related liabilities?
- ☑ Do you have a contractual relationship in place with a forensic investigator that is certified by the Payment Card Industry (a "PFI")?
- ☑ Do you have a contractual relationship in place with a forensic investigator that is independent of the Payment Card Industry?

[1] American Express Merchant Regulations (April 2014); Discover Merchant Operating Regulations (April 2014); MasterCard Security Rules and Procedures (Feb. 2015); Visa Service Rules (April 2015).
[2] Privacy Rights Clearinghouse (last viewed June 2015).
[3] Bryan Cave 2015 Data Breach Litigation Report available at http://www.bryancavedatamatters.com (search whitepapers).