

Data & Information Security

Security Policies

Washington Continues the Trend of Encryption and Payment Card Laws

Contributed by Melissa J. Krasnow, Dorsey & Whitney LLP

Washington is the third state to enact an encryption law and a payment card law.¹ Massachusetts and Nevada enacted encryption and payment card laws, and Minnesota and Nevada enacted payment card laws. The Washington law takes effect July 1, 2010 and applies to any data breach occurring on or after this effective date.

Data Breach

Under the law enacted in Washington state, a data breach is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.² Personal information means an individual's name, together with any of the following elements, when both the name and element are not encrypted: (i) Social Security Number, (ii) Washington driver's license number or identification card number or (iii) account number, credit card number, or debit card number, together with any required security code, access code, or password permitting access to their financial account.³

Applies to Business, Processor, and Vendor

The law applies to a business that (i) processes more than six million credit card and debit card transactions annually and (ii) provides, offers, or sells goods or services to Washington residents. These generally are merchants that have the highest level of compliance obligations among businesses that process credit cards.

This law also applies to a processor that directly processes or transmits account information for or on behalf of another person as part of a payment processing service (other than the business described above) and a vendor that (i) manufactures and sells software or equipment designed to process, transmit, or store account information or (ii) maintains account information that it does not own.

Account information means: (i) the full, unencrypted magnetic stripe of a credit card or debit card; (ii) the full, unencrypted account information contained on an identification device; or (iii) the unencrypted primary account number on a credit card or debit card or identification device, plus cardholder name, expiration date, or service code, if not encrypted.

Encrypted means enciphered or encoded using standards reasonable for the breached business or processor, taking into account the business or processor's size and the number of transactions processed annually.

Liability for Data Breach

A business or processor is liable to a financial institution for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards incurred by the financial institution to mitigate potential current or future damages to its credit card and debit card holders resulting from a data breach (even if the financial institution has not suffered a physical injury) if: (i) a business or processor fails to take reasonable care to guard against unauthorized access to account information in its possession or under its control and (ii) this failure is found to be the proximate cause of a data breach. The prevailing party is entitled to reasonable attorneys fees and costs incurred in connection with the legal action.

A vendor is liable to a financial institution for the foregoing damages: (i) to the extent that the damages were proximately caused by the vendor's negligence and (ii) if the claim is not limited or foreclosed by another provision of law or by a contract to which the financial institution is a party.

Encryption

A business, processor, or vendor is not liable if: (i) the account information was encrypted at the time of the data breach or (ii) the business, processor, or vendor was certified compliant with the payment card industry data security standards, as adopted by the payment card security standards council (including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.) and in force at the time of the data breach. The payment card industry data security standard include requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures and are intended to help organizations proactively protect consumer account data.

A business, processor or vendor will be considered compliant if its payment card industry data security compliance was validated by an annual security assessment and this assessment took place no more than one year before the time of the data breach (for this purpose, this security assessment of compliance is nonrevocable).

Conclusion

Because the July 1, 2010 compliance deadline is approaching, a business, processor or vendor that could be subject to this law should start assessing their compliance with this law.

Ms. Krasnow is a Partner in the Minneapolis office of Dorsey & Whitney LLP. For additional information, please visit www.dorsey.com/krasnow_melissa/. She may be reached at krasnow.melissa@dorsey.com.

-
- 1 Wash. H.B. 1149.
 - 2 RCW 19.255.010(4).
 - 3 RCW 19.255.010(5).

Legal Topics:

[Consumer Information](#)

[Data & Information Security](#)

[Network Security](#)

[Notification](#)

[Privacy & Information](#)

[Privacy Policies & Notices](#)

[Security Policies](#)

[Security Policies](#)

[Technology Law](#)

[Website Security](#)

Industry Topics:

[Chief Privacy Officer](#)

[Data Management](#)

[Information Security](#)

[Disclaimer](#)

The discussions set forth in this report are for informational purposes only. They do not take into account the qualifications, exceptions and other considerations that may be relevant to particular situations. These discussions should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. The opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content contained in this report and do not make any representation or warranty as to its completeness or accuracy.

©2010 Bloomberg Finance L.P. All rights reserved. Bloomberg Law Reports[®] is a registered trademark and service mark of Bloomberg Finance L.P.