KIRKLAND ALERT
July 2009

Data Security Legal Developments Complicate Compliance and Enhance Potential Legal Risks

Executive Summary

Three recent developments in data security law underscore the evolving and complicated legal patchwork applicable to businesses that handle personal information about individuals.

First, Nevada has codified the entire Payment Card Industry Data Security Standard ("PCI DSS"), which imposes various requirements on certain businesses that handle sensitive credit and debit card information. Nevada has also strengthened its existing encryption requirements for businesses that collect or transmit personal information of individuals. Both aspects of the Nevada law will likely impose costly and complex obligations on businesses. The codified PCI DSS in particular has the potential to create ambiguous and shifting legal requirements.

Second, Maine has amended its data breach notification statute to impose a specific deadline for notification: no greater than seven (7) days after law enforcement officials have determined that notification will not compromise an on-going criminal investigation.

Finally, retailer TJX recently entered into a settlement with 41 states, agreeing to pay $9.75 million in connection with a data breach that affected approximately 50 million individuals. This amount is in addition to the reported $100 million in breach-related costs that TJX has already incurred.

Nevada's PCI DSS and Data Encryption Law

Effective January 1, 2010, Nevada law will require all companies that conduct business in Nevada and that accept payment cards (including credit and debit cards) to meet the "current version" of the PCI DSS. The PCI DSS establishes extensive requirements designed to safeguard payment card information, such as the account number, security code, expiration date, magnetic strip data, and PIN.

Minnesota was the first state to codify portions of the PCI DSS. Nevada's codification goes further, however, codifying the entire PCI DSS. Nevada has thus turned the private regulatory scheme into law. Additionally, the new Nevada law appears to automatically incorporate future versions of the PCI DSS, which is updated approximately every two years by a private body.

In addition to codifying the PCI DSS, the new Nevada law strengthens data security requirements for businesses that do not accept payment cards. Nevada law already requires the encryption of certain personal information transmitted electronically over any system other than a business' secure internal network. Nevada's newly-amended law imposes two additional encryption requirements on most all businesses:

First, businesses subject to the law must encrypt certain personal information contained on electronic storage devices – such as laptops, cell phones, PDAs, and disk drives – whenever those devices are moved outside the "logical or physical controls" of the business.

Second, the encryption technology used to safeguard the personal information must have been adopted by an established standards setting body (including but not limited to the National Institute of Standards and Technology). The encryption technology must render the personal information indecipherable in the absence of associated cryptographic keys, the safeguarding of which is also subject to certain guidelines.

Maine's Notification Requirement Deadline

Under Maine's current data breach notification law, businesses are required to notify Maine residents in the event that their personal information is subject to unauthorized access. Such notification can be delayed, however, if it would compromise an on-going criminal investigation.

Effective September 11, 2009, Maine law will require businesses that experience a data security breach to notify affected residents within seven (7) days once law enforcement determines that notification will not compromise any on-going criminal investigation.

Businesses subject to Maine's law must be prepared to quickly undertake the notification within the time permitted, which may require close coordination with any outside vendor hired to administer the notification process. The seven-day period may impact other aspects of the business' incident response strategies, tactics, and obligations as well.

TJX Settlement with State AGs

As mentioned above, retailer TJX recently settled with attorneys general and state consumer protection agencies in 41 states, agreeing to pay a total of $9.75 million for TJX's failure to prevent an alleged data breach. This amount is in addition to the reported $100 million that TJX has paid already in breach-related expenses.

The TJX settlement serves as a reminder to all businesses that breakdowns in information security can have significant consequences and can lead to costly litigation with private litigants and governments. The Federal Trade Commission and state attorneys general continue to express a strong interest in enforcing data security laws and standards against businesses, as demonstrated by a portion of the TJX settlement being dedicated to fund future state enforcement actions.

Conclusion and Recommendations

We recommend that companies evaluate whether and how the new data security laws in Nevada and Maine relate to business practices. To the extent necessary, businesses should update their relevant policies, procedures, and technologies. Businesses should also remain vigilant regarding how these new laws impact existing and future contractual relationships and risk allocation with business partners, especially vendors and service providers that assist in the handling of sensitive personal information.

Should you have any questions about the matters addressed in this Alert, please contact the following Kirkland & Ellis author or the Kirkland & Ellis attorney you normally contact:

Seth Traxler
Kirkland & Ellis LLP
300 North LaSalle
Chicago, IL 60654
www.kirkland.com/straxler
+1 (312) 862-2241