

The Cyber Attack and Hacking Epidemic – A Legal and Business Survival Guide

**Practising Law Institute
January 9, 2012**

**Melissa J. Krasnow, Partner, Dorsey & Whitney LLP,
and Certified Information Privacy Professional**

SEC Guidance on Cybersecurity and Cyber Incident Disclosure

- Securities and Exchange Commission (SEC) guidance about public company disclosure of cybersecurity risks and cyber incidents:
 - not a rule, regulation or statement of the SEC
 - no disclosure requirement specifically refers to cybersecurity risks and cyber incidents
 - certain disclosure obligations may require discussion of cybersecurity risks and cyber incidents

SEC Guidance on Cybersecurity and Cyber Incident Disclosure

- risk factors (if among the most significant factors that make an investment in the company speculative or risky), for example:
 - aspects of the company’s business that give rise to material cybersecurity risks and the potential costs and consequences
 - description of material cyber incidents experienced by the company and the costs and other consequences

SEC Guidance on Cybersecurity and Cyber Incident Disclosure

- management’s discussion and analysis of financial condition and results of operations
- description of business (if materially affects its products, services, relationships with customers or suppliers or competitive conditions)
- legal proceedings (where a party to a material pending legal proceeding that involves a cyber incident)
- disclosure controls and procedures (where poses a risk to the company’s ability to record, process, summarize and report information required to be disclosed in SEC filings)
- financial statement disclosure

Legislative Response to Cyber Attacks and Breaches

- Cybersecurity legislation with critical infrastructure focus called for by the Obama administration
- Calls for national breach notification law
- Amendments to state breach notification laws (e.g., California, Illinois and Texas)

Massachusetts Privacy Regulation

- Covers an entity (regardless of whether in Massachusetts) with access to Massachusetts resident personal information (including name plus Social Security number, name plus driver's license number or name plus financial account number or credit or debit card number)

Massachusetts Privacy Regulation

- Requires an entity to implement a written information security program (WISP):
 - encryption of personal information transmitted wirelessly and stored on portable devices
 - third party service provider to an entity by contract provision must implement and maintain appropriate security measures for personal information (March 1, 2012 deadline for contracts entered into on or before March 1, 2010; effective for contracts entered into after March 1, 2010)
 - documentation of actions taken in response to incident involving a breach and mandatory post-incident review to make changes in business practices for protection of personal information

Massachusetts Privacy Regulation

- Reporting a breach to the Massachusetts attorney general (which is required under the Massachusetts breach notification law) could trigger an investigation of a reporting entity, including that the entity submit its WISP for review
- Massachusetts attorney general enforcement actions
- Other states have laws addressing security procedures (e.g., California) and encryption (e.g., Nevada)

PCI DSS

- Payment Card Industry Security Standards Council (PCI SSC) comprises payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.
- PCI SSC sets the Payment Card Industry Data Security Standard (PCI DSS) and works on a three-year lifecycle to update PCI DSS
- PCI DSS is the global data security standard for all entities that process, store or transmit cardholder data, consisting of 12 requirements

PCI DSS Requirements

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

PCI DSS Requirements

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel

PCI DSS Compliance and Validation

- Compliance is the continuous state of adhering to the standard
- Validation is a point-in-time event that attempts to measure and describe the level of adherence to the standard
- 21% of entities were found fully compliant at the completion of their initial report on compliance (2011 Verizon PCI Compliance Report)
- 11% of entities suffering payment card breaches were compliant with PCI DSS at the time of the breach based on the last official audit or self-assessment (2011 Verizon Data Breach Investigations Report)

Payment Card Brand Requirements and State Requirements Relating to PCI DSS

- Each payment card brand has its own program for compliance, validation levels and enforcement
- Minnesota, Nevada and Washington have laws addressing compliance with PCI DSS
- In March 2011 Massachusetts attorney general enforcement action, company is required to comply with PCI DSS and verify compliance with the Massachusetts attorney general's office