

## Lose a Laptop? Practical Approaches to Navigating Breach Notification Laws

HIMSS Conference  
Chicago  
April 6, 2009

Diana J.P. McKenzie  
Partner and Chair – Information  
Technology Practice Group  
Neal, Gerber & Eisenberg LLP  
Office: (312) 269-8093  
Cell: (847) 370-1121  
dmckenzie@ngelaw.com  
[www.ngelaw.com](http://www.ngelaw.com)

© Neal, Gerber & Eisenberg LLP 2008, 2009

---

---

---

---

---

---

---

---

## The Breakdown

	TOTAL	HEALTH CARE
Lost / Stolen Media	20.7%	29.9%
Employee Theft	15.7%	16.5%
Accidental Disclosure	14.5%	10.3%
Hacking	13.9%	5.2%
Subcontractors	10.4%	15.5%
Other / Unknown	24.8%	22.7%

2

---

---

---

---

---

---

---

---

## Laws and Regulations

- FTC
- Federal security breach notification law
- State security breach notification laws
  - Apply when a security breach occurs involving personal information
  - Set forth requirements for when, how and in what circumstances to notify affected individuals of the breach

3

---

---

---

---

---

---

---

---

## Federal Security Breach Notification Law

### Stimulus Package – Data Security Breach Notification

- So far, “just” one law – American Recovery and Reinvestment Act of 2009
- Data Security Breach Notification Requirements
- Unsecured Protected Health Information
- Timing for Data Security Breach Notices

4

---

---

---

---

---

---

---

---

## Federal Security Breach Notification Law Continued

- Content of Data Security Breach Notices
- Methods for Giving Data Security Breach Notices
- Notice to DHHS

5

---

---

---

---

---

---

---

---

## Federal Security Breach Notification Law Continued

- Enhanced Civil Penalties and Enforcement
  - Increased Amounts
  - Victim Compensation
  - States Attorneys General Enforcement
- Clarified Criminal Coverage
  - Knowing Violations
  - Exposure for Employees and Other Individuals

6

---

---

---

---

---

---

---

---

## State Security Breach Notification Laws Important Distinctions

- Who the laws apply to
- What constitutes a security breach
- What constitutes personal information
- Who must be notified
- What must be disclosed
- How and when the notification must be sent
- How the law is enforced
- How to qualify for a safe harbor

7

---

---

---

---

---

---

---

---

## Who Do the Laws Apply To?

- Most states: only entities conducting business in the state
- Some states:
  - Entities who own or license information of state residents.
  - Only information brokers (Georgia and Maine)
  - Only state government (Oklahoma)
- Exemptions (in some states):
  - Compliance with federal or state regulations
  - Financial institutions
  - Government agencies
- All states: entities who *own or license* the personal data
  - Vendors who merely *maintain* the data are only obligated to notify the owner or licensee.

8

---

---

---

---

---

---

---

---

## What Constitutes a Security Breach?

- Most states: unauthorized *acquisition* that compromises personal data
  - May include missing data
- Some states:
  - Mere unauthorized *access* is sufficient
  - Data must be *materially* compromised
  - The acquisition must create risk of loss or injury

9

---

---

---

---

---

---

---

---

## What Triggers the Requirements?

- Half of the states: automatic notification upon discovery of breach
- Other half: after investigation to determine the likelihood of misuse or harm
  - Documentation / retention requirements

10

---

---

---

---

---

---

---

---

## What Is Personal Information?

- Most states—name (last and first or first initial) with:
  - Social security number;
  - Driver's license or ID card number; or
  - Information sufficient to get access to a financial account
- Some states:
  - Additional information also included
  - The name is not necessary
- Arkansas and California: medical information
- Exception: public information

11

---

---

---

---

---

---

---

---

## Must the Data Be Computerized?

- Most states: yes
- Six states: the data can be in any form (written, spoken, printed, electronic, etc.)

12

---

---

---

---

---

---

---

---

## Who Must Be Notified?

- **Most states:** affected residents of the state
- **Four states:** all affected individuals
- It is a good idea to notify *all* affected individuals, regardless of the law
- Could be employees (not just customers)
- Other agencies to notify (in some states):
  - Law enforcement
  - Consumer reporting agencies
  - Regulating state office
  - State attorney general's office

13

---

---

---

---

---

---

---

---

## What Must Be Disclosed?

- **Most states:** notice of the breach
- **Some states:** clear and conspicuous notice
- **Best Practices**
  - Be clear, direct and simple
  - Be honest and accept responsibility, but make it clear that you have control
  - Use an empathetic, but not apologetic, tone
  - Offer assistance and useful information
  - Use company (not attorney) letterhead

14

---

---

---

---

---

---

---

---

## How May the Notification Be Sent?

- **Written:** all states
- **Electronic:** all states, if individual consented to receive electronic communications
  - Limited in 13 states
- **Other methods:** telephone, fax, publication
- **Substitute notice:** all states, if cost exceeds some dollar amount or affected class is high
  - Usually \$250,000 or 500,000 individuals
  - E-mail, website and major media

15

---

---

---

---

---

---

---

---

### When Must the Notification Be Sent?

- Most States: in the most expedient time and manner possible, without unreasonable delay
  - Unless law enforcement requests a delay
  - Entity given time to restore data and determine scope
- Some States: Specific time limit

---

---

---

---

---

---

---

---

### How is the Law Enforced?

- Most States: Civil penalties
- Some States:
  - Private cause of action
  - Damages recoverable through Attorney General
  - Injunction and/or equitable relief

---

---

---

---

---

---

---

---

### What Safe Harbors Are Available?

- Encryption: all states
- Security policy: 29 states

---

---

---

---

---

---

---

---

## What to do if a Breach Occurs

- Secure the data from further breach
- Consider notifying the police
- Find out what data was accessed
- Conduct an investigation (documenting evidence)
- Provide *all* affected individuals with written, clear and conspicuous notification in the most expedient time possible.
- Notify other agencies, as required
- Consider offering free credit watch services
- Document all steps taken and people contacted

19

---

---

---

---

---

---

---

---

## How to Protect Yourself Beforehand

- Encrypt personal information
- Implement security measures
- Destroy personal records not in use
- Assess whether you need the personal information you collect and store
- Create an information security or privacy policy

20

---

---

---

---

---

---

---

---

## What to do if a Breach Occurs: Preservation of Evidence

- For evidence to be admissible, you must prove that it was not tampered
- Preserving digital evidence
  - Disconnect the system from the network, but do not shut it down
  - Don't open log files
  - Don't use the system (if possible)

21

---

---

---

---

---

---

---

---

## Data Protection Laws

- Duty to Safeguard Personal Information
- Disposal
- Collection and Retention Limits
- Transfer Notification
- Encryption requirements
- Employee training / monitoring requirements
- Merchant Liability

22

---

---

---

---

---

---

---

---

## The Security Policy

- Is it worth it?
  - Financial risk
  - Consumer trust and loyalty
- What to include
  - Collection / storage / disposal of information
  - Encryption / security requirements
  - Employee policies
  - Identification of "red flags"
  - Incident Response Plan

23

---

---

---

---

---

---

---

---

## The Future?

- California laws effective January 1, 2009
- Medical Record Breach Notification Law
  - Applies to breach of medical information
  - Must notify affected patients and state Dept. of Public Health within five days
- State Duty to Safeguard Medical Information
  - Private cause of action and civil penalties for unauthorized negligent or willful access, use or disclosure

24

---

---

---

---

---

---

---

---



25

---

---

---

---

---

---

---

---

## Questions

Diana J. P. McKenzie  
Partner and Chair, Information  
Technology Practice Group  
Neal, Gerber & Eisenberg LLP  
Office: (312) 269-8093  
Cell: (847) 370-1121  
dmckenzie@ngelaw.com  
***www.ngelaw.com***

26

---

---

---

---

---

---

---

---