Insert tab here:

Security Breach Notifications

(Arial Narrow)

The 2009 Hospitality Law Conference

February 9-11, 2009 - Houston, Texas

Focusing on worldwide legal, safety, & security solutions

Course Evaluation

Security Breach Notifications, the Law, and Your Brand
Scott Brown, Attorney, *Skadden, Arps, Slate, Meagher, & Flom LLP*

For each question circle the answer that comes closest to your opinion

1-strongly disagree 2-disagree 3-neutral 4-agree 5-strongly agree

This program was presented in a lively, stimulating way	1	2	3	4	5
The content was interesting and informative	1	2	3	4	5
The information presented will be useful to me	1	2	3	4	5

- **What other topics in this area should we consider for next year?**

- **Other Comments?**

Your comments will ensure a successful program next year. Thank you.
Please place this form in the designated box located in each session.

Scott Brown

Counsel
Skadden, Arps, Slate, Meagher & Flom LLP

Mr. Brown’s principal areas of practice include domestic and trans-border mergers and acquisitions, commercial contracts, litigation, and counseling involving copyrights, trademarks, patents, the rights of publicity and privacy, and data security. Mr. Brown is also well-versed in the legal issues involved in creating, substantiating and disseminating advertising and marketing materials, and he often reviews and pre-clears advertising copy.

Mr. Brown's transactional and commercial contract experience includes structuring and negotiating the development, apportionment and transfer of intellectual property rights in the context of domestic and trans-border mergers and acquisitions, divestitures, joint ventures, franchises, strategic alliances and other commercialization opportunities in the United States and abroad. He also has handled the intellectual property aspects of numerous securities offerings, corporate finance matters, and bankruptcy filings.

On the litigation front, Mr. Brown has successfully prosecuted and defended copyright, trademark, trade dress, unfair competition, publicity and privacy, trade secret, breach of contract, false advertising, and data security matters in state and federal trial and appellate courts. Many of the cases he has worked on are matters where one or both parties sought preliminary and permanent injunctive relief, in addition to substantial monetary damages. Mr. Brown has also successfully represented several claimants in domain name administrative proceedings brought under the Uniform Domain Name Dispute Resolution Policy.

Mr. Brown also has substantial experience counseling clients on the clearance and protection of their intellectual property rights.

Over the years, Mr. Brown has worked with a broad spectrum of clients, from growth-stage companies to some of the largest U.S. and foreign corporations, as well as private equity firms and investment banks.

An avid reader and frequent speaker and author, Mr. Brown reads, lectures and writes regularly about topics related to intellectual property, the rights of publicity and privacy, and data security.

Security Breach Notifications, The Law, and Your Brand:

Ten Tips to Protect Your Company and Reputation

Scott Brown
February 9, 2009

Skadden

Presenters

- Scott Brown, Counsel, Skadden, Arps, Slate, Meagher, & Flom LLP
- I have a broad practice, which includes counseling involving data security.
- I have dealt with data security for many years and in many contexts, including in mergers and acquisitions, commercial contracts, and in litigation.
- I have worked with a broad spectrum of clients, from growth-stage companies to some of the largest U.S. and foreign corporations, many of whom have sought my advice on data security issues.

Skadden

What constitutes a data security breach?

- Unauthorized acquisition of and access to "personal information"
- "personal information" is commonly defined as an individual's name in combination with said individual's:
  - social security number; or
  - driver's license or state identification number; or
  - account number or credit or debit card number in combination with any access code or password that would permit access to such individual's financial account.

Skadden

How do data breaches occur?

- Lost and stolen laptops
- Hacking
- Old fashioned theft (breaking and entering)
- Disclosure of data upon fraudulent representations
- Dishonest insiders
- Human error

Skadden

3

Tip one

Identify and Assess Existing Regulations and Standards

- Identify, analyze, and understand existing federal and state laws and regulations, as well as applicable professional standards, such as the Payment Card Industry Data Security Standards, and how they impact your organization.

Skadden

4

What various federal laws govern notice?

- The Financial Modernization Act of 1999 (a/k/a the Gramm-Leach-Bliley Act) (applies to financial institutions)
- Telecommunications Act of 1996 (applies to telecommunications carriers)
- United States Health Insurance Portability and Accountability Act of 1996 (a/k/a HIPAA) (applies to those in the healthcare industry)
- The Veterans Benefits, Health Care, and Information Technology Act of 2006 (applies to the Veterans Administration Secretary and related private sector service providers)
- The Privacy Act of 1974 (As clarified by the Office of Management and Budget memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information;" applies to federal agencies)

Skadden

5

What various state laws govern notice?

- Arizona
- Arkansas
- Alaska **(7/1/09)**
- California
- Colorado
- Connecticut
- Delaware
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Iowa
- Indiana
- Kansas
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina (7/1/09)
- Tennessee
- Texas
- Utah
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- Wyoming
- District of Columbia
- Puerto Rico
- Virgin Islands

Skadden

6

What about Europe?

- two directives currently govern data security in the European Union:
  - Directive 95/46/EC, which concerns the protection of an individual's personal data (the "Data Protection Directive"), and
  - Directive 2002/58/EC, on privacy and electronic communications (the "Privacy and Electronic Communications Directive").
- neither contains a requirement to inform or notify consumers or regulators of a breach.
- N.B., there is a "Communication on the Review of the EU Regulatory Framework for Electronic Communications Networks and Services" that proposes a breach notification system, but it has not yet been accepted or implemented.

Skadden

7

PCI Data Security Standards

- Install and maintain a firewall configuration to protect personal information; and
- Do not use vendor-supplied defaults for system passwords or other security parameters; and
- Protect stored personal information; and
- Encrypt transmission of personal information across open, public networks; and
- Use and regularly update anti-virus software; and
- Develop and maintain secure systems and applications; and
- Restrict access to personal information by business "need to know"; and
- Assign a unique ID to each person with computer access to personal information; and
- Restrict physical access to cardholder data; and
- Track and monitor all access to network resources and cardholder data; and
- Regularly test security systems and processes; and
- Maintain a policy that addresses information security.

Skadden

8

Complying with state law

- What constitutes a data security breach under state law?
- When is notice required?
- Who should be notified?
- What form should the notice take?
- What must the notice say/not say?
- When should the notice go out?

Skadden

9

Examples of what constitutes a data security breach under the laws of various states

- California (standard followed by most states): unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a person or business.

Skadden

10

Examples of what constitutes a data security breach under the laws of various states (cont.)

- New Jersey (example of a state with an encryption safe harbor): unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable.

Skadden

11

Examples of what constitutes a data security breach under the laws of various states (cont.)

- Massachusetts (example of a variation on the general theme): the unauthorized acquisition or unauthorized use of unencrypted personal information or encrypted electronic personal information and the confidential process or key that is capable of compromising the security, confidentiality or integrity of that personal information that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth.

Skadden

12

Tip two

Assess Your Data Retention Systems

- Determine what information your company keeps, why it keeps it, and where the information is stored.
- Safely discard any unnecessary information.

Skadden

13

Tip three

Assess Employees' Access To Data

- Evaluate which employees have access to sensitive information.
- Limit that access where appropriate to mitigate the risk of intentional misuse or accidental disclosure of data.

Skadden

14

Tip four

Assess Your Potential Vulnerabilities

- Conduct a thorough assessment of your company's infrastructure to identify present internal and external risks and vulnerabilities, and catalog all prior security breaches resulting from accidental and intentional behavior.

Skadden

15

Tip five

Form a Data Security Team

- Data security is no longer solely the domain of information technology professionals.
- Assemble a data security team to develop, oversee, implement, and administer your company's plan.
- To effectively protect your brand, data security must be a joint priority for management, legal counsel, public and media relations, and customer services professionals.

Skadden

16

Tip six

Design a response plan

- Design a plan for responding to a data security breach before it happens.
- Put your company's response plan in writing and distribute it to all relevant persons.
- Incorporate physical, technical and administrative security measures into your plan.

Skadden

17

Breach Investigation Checklist

- Examine the nature and extent of the breach (e.g., follow the trail to establish what hardware and/or data files have been compromised):
  - How many customers are at risk; and
  - What type of account information is at risk (e.g., account number, magnetic-stripe data, expiration date, cardholder name, cardholder address, PIN data, CVV2 or CVC2 data, etc.); and
  - What is the timeframe of personal information that was potentially compromised?
- Was the potentially-compromised information encrypted in whole or in part?
  - If the information was encrypted, did the intruders gain access to the encryption keys?
  - Has your technology been compromised? (If so, special handling required.)
- What has been done to contain the breach?

18

Skadden

Who must be notified under state laws?

- Law enforcement
- Affected consumers
- States' Attorneys General
- Various state agencies (e.g., New York State Office of Cyber Security and Critical Infrastructure Coordination)
- Consumer reporting agencies (e.g., Experian, TransUnion, Equifax)

19

Skadden

Who else may need to be notified?

- Visa, Mastercard, American express
- payment processors (e.g., Chase Paymentech, Fiserv, Metavante)
- Sponsoring banks (e.g., Fifth Third Bank)
- Your Customers (if you are a vendor)
- Entities providing services to your organization
- The market

20

Skadden

What form can the notice to affected consumers take under various state laws?

- written form:
  - Can be electronic (consistent with federal statutes governing electronic records and signatures)
- some statutes permit telephonic notification.
- Nearly all statutes contain "substitute notice" provisions for cases in which the company can demonstrate a significant cost associated with notification, where the number of individuals to be notified is significant, or if the company lacks sufficient contact information to notify individuals.
  - Substitute notification typically requires all of the following: (i) email, if the company has an email address, and (ii) conspicuous posting of the notice on the company's website and (iii) notification via major statewide media.

Skadden

21

What must the notice to affected consumers say under Massachusetts law?

- The notice must include:
  - the consumer's right to obtain a police report; and
  - how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and
  - any fees required to be paid to any of the consumer reporting agencies.
- The notification shall not include the nature of the breach or unauthorized acquisition or use, or the number of residents of the Commonwealth affected.

Skadden

22

What must the notice say under other states' laws?

- Describe the security breach in general terms; and
- Provide contact information for the company making the notification; and
- Include a description of the categories of information that were, or are reasonably believed to have been, breached; and
- Provide a general description of what the company has done to protect data from further security breaches; and
- Provide a telephone number where further assistance and information can be obtained; and
- Remind recipients of the need to remain vigilant for incidents of fraud and identity theft.

Skadden

23

When should the notice go out?

- **Massachusetts:** "as soon as practicable and without unreasonable delay when such person knows or has reason to know of a breach of security."
  - There is no hard and fast rule on the number of business days
- **California**, **New Jersey** and **New York** (as examples of other jurisdictions): "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement . . . or any measures necessary to define the scope of the breach and restore the reasonable integrity of the data system."
  - There is no hard and fast rule on the number of business days

Skadden

24

Tip seven

Periodically Revise Your Data Security Plan

- To maintain effectiveness over time, periodically review and revise your company's data security plan to reflect changes in risk, trends, security vulnerability, and the business environment in which your company operates.

Skadden

25

Tip eight

Know Your Obligations to Other Companies

- Review existing business contracts to determine your company's obligations to safeguard the information it acquires from other companies.
- Assess any potential liability to other parties for a data breach, such as clients that provide you with sensitive information.

Skadden

26

Tip nine

Monitor Third Parties

- Carefully select, audit, and supervise third-party service providers and vendors with access to sensitive information.
- Limit (and eliminate where possible) the amount of data provided to vendors.
- Incorporate data security standards in your contracts and indemnification provisions where appropriate.

Skadden

27

Tip ten

Consult with Knowledgeable Experts

- While these tips should be a useful starting point, in this constantly-changing area there is no substitute for careful examination of each company's unique circumstances with the participation of management, information technology personnel and knowledgeable counsel.

Skadden

28

Questions?

Skadden

29

Scott Brown
617-573-4800
scott.brown@skadden.com

Skadden

30