2009 HOSPITALITY LAW CONFERENCE

Data Security in the Hospitality Industry

February 10, 2009

Presenters

- Scott Brown, Skadden, Arps, Slate, Meagher, & Flom LLP
- His principal areas of concentration include transactions, licensing, litigation, and counseling involving trademarks, copyrights, the rights of publicity and privacy, software, data security and domain names.
- 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.

Introduction

- State and federal legislation and Payment Card Industry Data Security Standards
- Specific measures that will help you assess your data security plans and implement industry “best practices”
- Q&A

Laws, Regulations and Standards

- "Every company has an obligation to its customers, affiliates, and employees to safeguard sensitive data."
  –Leslie Fair, Attorney, FTC Bureau of Consumer Protection
- Federal Statutes and Rules
- FTC Regulations
- State Laws
- Payment Card Industry: Data Security Standards

Federal Trade Commission Act, §5

- Charges the FTC with preventing “persons, partnerships, or corporations” from using “unfair or deceptive acts or practices in or affecting commerce.”
- There have been 23 data security enforcement actions filed to date.

Federal Trade Commission Act, §5

- Under the FTC Act, the FTC brings data security cases based on alleged:
  - **Deception** (e.g., Eli Lilly, Microsoft, Petco, Life is Good, ChoicePoint)
  - **Unfairness** (e.g., BJ's Wholesale Club, Reed Elsevier, Seisint, TJX)
- ChoicePoint's settlement included $10 million in civil penalties and $5 million in consumer redress.

Federal Trade Commission Act, §5

ValueClick media

BJ's

cardsystems
the power of the right solution

PREMIER Capital Lending

Reed Elsevier

GOAL FINANCIAL™

GUESS? U.S.A.

PETCO
Where the pets go.

DSW

Guidance SOFTWARE

AMERICAN UNITED
MORTGAGE CORPORATION
Your partner in home financing.

seisint™

Lilly

Life is good.

TOWER
Records • Video • Books

Microsoft

TJX
THE TJX COMPANIES, INC.

HospitalityLawyer.com

The Fair Credit Reporting Act

- The Fair Credit Reporting Act regulates the collection, dissemination, and use of consumer credit information.
- The Fair Credit Reporting Act also serves as the underlying basis for many other consumer credit laws and rights in the United States.

FCRA – Fair and Accurate Credit Transactions Act

- Designed to help consumers combat the growing crime of identity theft
- Requires businesses to protect customers' information:
  - Duty to truncate payment card information on receipts
  - Receipts may not include expiration date
  - Class actions have been brought (though none have been successful thus far) regarding the truncation of customer information on receipts.

FCRA – Red Flags Rule

- The Red Flags Rule addresses the detection and prevention of identity theft
- Requires identification, detection, and response to patterns, practices, and specific activities (“red flags”) that could indicate identity theft

FCRA – Red Flags Rule

- FTC enforcement deadline: **May 1, 2009!**
- FTC Consent Orders trend: requiring retailers and service providers to institute practices which mirror the requirements of the Red Flags Rule

FCRA – FTC Disposal Rule

- Consumer reports must be disposed of with care, **and so too must ALL sensitive data!**
- Care must be taken to protect against "unauthorized access to or use of" customer information.

FCRA – FTC Disposal Rule

- With respect to the Disposal Rule, the FTC has advised:

"those who dispose of <u>any</u> records containing a consumer's personal or financial information should take similar protective measures."

Financial Privacy Rule & Safeguards Rule

- These rules are not directly aimed at the hospitality industry, but present a prudent business standard that would be helpful to any business.

Financial Privacy Rule & Safeguards Rule

- **Financial Privacy Rule**
  - Requires a “clear and conspicuous disclosure” of your business’s privacy policy
  - What information will you share? With whom? How will it be disclosed? For how long will you keep the information?

Financial Privacy Rule & Safeguards Rule

- **Safeguards Rule**
  - Develop administrative, technical, and procedural safeguards to ensure the security and confidentiality of customer records and information

State Laws

- In the absence of an over-arching federal law, states are stepping in with data security laws.
- To date, 44 states, Washington D.C., Puerto Rico, and the Virgin Islands have breach notification statutes.

State Laws – Breach Notification Statutes

Alaska	Arizona	Arkansas	California	Colorado
Connecticut	Delaware	Florida	Georgia	Hawaii
Idaho	Illinois	Indiana	Iowa	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
Tennessee	Texas	Utah	Vermont	Virginia
Washington	West Virginia	Wisconsin	Wyoming	Washington D.C.
Puerto Rico	Virgin Islands			

State Laws – Breach Notification Statutes

- Breach Notification Laws include various provisions related to:
  - Internal breach notification policies
  - The method of notification
  - The timing of notification
  - The content of notification
  - The persons to whom you must give notice (*e.g.*, consumers, credit reporting agencies, governmental bodies, etc.)

State Laws – Cost Sharing

- To date, only Minnesota has passed a "cost-sharing" law, but several states have considered similar measures.
  - Texas
  - Connecticut
  - Illinois
  - Massachusetts

State Laws – Cost Sharing

- Minn. Stat. §325E.64:
  - Allows financial institutions to recover costs incurred by the breach of another business's security system.
  - Businesses out of compliance with Minnesota's data security law run the risk of exposure.

State Laws – Cost Sharing

- Under Minnesota's cost-sharing law (and other state bills which have been proposed), a business may have to reimburse a financial institution for the cost of:
  - The cancellation, closure, reopening or re-issuance of accounts;
  - Actions to stop payments or block transactions;
  - Refunds and credits made to a cardholder; and
  - Any costs relate to the notification of cardholders affected by the breach.

European Union & U.S.A. Safe Harbor Provisions

- European Union's Directive on Data Protection
  - Effective in 1998; imposes a (strict) standard of "adequacy" on privacy protection.

European Union & U.S.A. Safe Harbor Provisions

- Safe Harbor Policy
  - Approved jointly by the European Commission and the U.S. Department of Commerce.
  - Participation for U.S. Companies is voluntary.
  - Businesses which wish to participate must annually self-certify that they comply with the seven "Safe Harbor Principles."

European Union & U.S.A. Safe Harbor Provisions

- For organizations doing business in Europe, participation in the Safe Harbor Program:
  - is cheaper.
  - is more efficient.
  - is less risky.
  - is a good business practice, and a good marketing tool.

European Union & U.S.A. Safe Harbor Provisions

- *Cheaper*.
  - The seven Safe Harbor principles allow a business to tailor their application to the size and purpose of the business.
- *More efficient*.
  - Companies participating in the Safe Harbor will be deemed “adequate” and data flows to those companies will continue.

European Union & U.S.A. Safe Harbor Provisions

- *Less risky*.
  - Participation in the Safe Harbor subjects companies to U.S. jurisdiction, rather than the more comprehensive E.U. Directive.
- *Good business practice. A good marketing tool*.
  - The Department of Commerce keeps a publicly available list of businesses which comply with the Safe Harbor principles. Is your company on it?

European Union & U.S.A. Safe Harbor Provisions

- The seven Safe Harbor principles:
  - *Notice*
  - *Choice*
  - *Transfer to Third Parties*
  - *Access*
  - *Security*
  - *Data Integrity*
  - *Enforcement*

European Union & U.S.A. Safe Harbor Provisions

- Additionally, businesses protected by the Safe Harbor must publish a privacy policy, disclosing that they adhere to these seven “Safe Harbor” principles.

Going Forward – Best Business Practices

- Businesses are faced with:
  - Customer demands for data security
  - Competitive pressures to maintain an integrated and streamlined information processing system
  - Contractual obligations related to the protection and security of data
  - Ever-changing and often-cumbersome legal and regulatory requirements

Payment Card Industry Data Security Standards

- Who is subject to the Payment Card Industry Data Security Standards?
  - In a 2007 study, 71% of businesses surveyed were unsure of the policies and procedures related to the PCI Standards.
- What do these Standards require?
  - To be "PCI Compliant," your business must meet **12 requirements**.

Payment Card Industry Data Security Standards

- How can your business be sure it is compliant?
  - In a 2007 study, 92% of businesses surveyed relied on third-party vendors as a means of maintaining their required compliance.
- What are the penalties for non-compliance?
  - In 2008, Visa announced that it would levy monthly fines of $25,000 against non-PCI-compliant large merchants and $5,000 against non-compliant middle-sized merchants.

One Size Does Not Fit All.

- Make a “breach inventory.”
  - Take a historical view of your vulnerabilities.
- Tailor your program to suit your business’s unique security needs.
  - An assessment of your vulnerabilities from a historical perspective allows you to develop the proper security focus going forward.

Put Your Plan In Writing.

- Maintain a clear, complete security program.
- Distribute this program to all relevant people in your organization.
  - IT professionals
  - Management teams
  - Employees that will have access to any sensitive data
  - Any person who may, *at any point*, need access to this data

Put Your Plan In Writing.

- To pass FTC muster, your policies must be strong enough to be fair to your customers **AND** your business must adhere to the policies it sets out.

Cover Your Bases.

- Implement three measures of data security:
  - ***Physical***
  - ***Technical***
  - ***Administrative***

Cover Your Bases.

- *Physical*
  - Dispose of information carefully
  - Restrict and monitor access to information
  - Lock paper files
  - Block access to certain websites which can comprise your system's integrity
  - Carefully screen employees and vendors with access to sensitive information

Cover Your Bases.

- *Technical*
  - Install identity and access management software
  - Utilize firewalls
  - Encrypt, scramble, or remotely disable data
  - Install available software patches
  - Use “data wipe” software
  - Implement multi-factor remote access controls

Cover Your Bases.

- *Administrative*
  - Document your security policies and protocol
  - Provide periodic training and regular reminders of the protocol
  - Consistently enforce sanctions when protocol is breached
  - Remain up-to-date on current security risks and system vulnerabilities
  - Regularly (and safely) dispose of data that is no longer needed
  - Contractually require third-party vendors to maintain acceptable data security standards and practices

Review Your Plan Regularly.

- Update your plan to reflect changes in risks, trends, and security vulnerability.
- The government is working with the private sector to provide data security training, outreach, and support. Take advantage of these programs.
- Maintain detailed records of your company's experiences with and responses to data theft.

Employees Are Essential To Your Plan's Success.

- Employees are critical to your information security plan for 4 reasons:
  - Employees make mistakes.
  - Employees can be unaware (or untrained).
  - Employees can be the perpetrators.
  - Employees *have* personal information which your business may store.

Third Parties, Vendors & Outsourcing

- Carefully select and continually manage third-party vendors entrusted with sensitive data.
- Monitor the process by which information is exchanged between your business and such vendors.

Third Parties, Vendors & Outsourcing

- A recent FTC decision revealed the Agency's view that businesses should be supervising and adequately auditing third-party vendors, and will be held responsible for data lost in such vendors' custody.

Fail-Safe Plans Can Fail – Are You Ready?

- The best-laid plans…
- Any comprehensive data-security plan must include policies for responding to a data breach or system invasion.
- Such policies should take into account:
  - Responses which are commensurate with the degree of risk posed
  - Aggravating factors that heighten the risk of

Fail-Safe Plans Can Fail – Are You Ready?

- When formulating your business's response protocol, consider:
  - Assessing the nature and scope of the incident
  - Pinpointing the exact information accessed or misused (including, if possible, specifically which customers may be affected)
  - Appointing a person or group to oversee your business's efforts and serve as a primary contact for information exchange regarding the breach

Fail-Safe Plans Can Fail – Are You Ready?

- When formulating your business's response protocol, consider:
  - Notifying the appropriate division of federal, state or local law enforcement officials, and the institution that maintains the accounts
  - Launching the appropriate physical, technical, or administrative systems to quarantine the intrusion and prevent further access and loss
  - Preserving all appropriate records, logs or other evidence to aid in the recapture of information or prosecution of the infiltrator

Fail-Safe Plans Can Fail – Are You Ready?

- When formulating your business's response protocol, consider:
  - Notifying customers in accordance with the proper state breach security law(s)
  - Setting up a call center or website (if the size of the breach warrants it) to instruct customers and to respond to questions and concerns.

Conclusion

- Businesses must be concerned with protecting the information they collect and store.
  - Take an inventory.
  - Reduce what you keep; keep what you need.
  - Physically, electronically, and administratively safeguard sensitive information.
  - Dispose of information safely.

Conclusion

- Businesses must be concerned with protecting the information they collect and store.
  - Create a policy. Write it down. Review it.
  - Train your employees. Give frequent reminders. Enforce sanctions.
  - Carefully select, continually manage, and occasionally audit vendors.
  - If you have questions, call me.

Scott Brown

(617) 573-4800

scott.brown@skadden.com