Best Practices for Protecting Data and Managing Data Breaches

June 30, 2011

Sheila A. Millar  
Partner  
Keller and Heckman LLP  
1001 G Street, N.W.  
Washington, DC 20001  
202-434-4143  
millar@khlaw.com

Tracy P. Marshall  
Partner  
Keller and Heckman LLP  
1001 G Street, N.W.  
Washington, DC 20001  
202-434-4234  
marshall@khlaw.com

Presenters

- **Sheila A. Millar** is a Partner at Keller and Heckman and counsels corporate and association clients on a range of consumer protection regulatory and public policy matters. Ms. Millar advises clients on privacy and security policies and programs, data breach responses, data transfers and cloud computing. She also counsels clients on privacy and regulatory compliance aspects of promotions, social media policies, website terms and online sales. Noted for her expertise on children’s issues, Ms. Millar has participated in Federal Trade Commission (FTC) workshops on children's privacy and advertising literacy.
Presenters

- **Tracy P. Marshall** is a Partner at Keller and Heckman LLP. She assists for-profit and non-profit clients with a range of business and regulatory matters. In the Internet, privacy, and advertising areas, Ms. Marshall provides counsel on e-commerce transactions and online promotions, privacy and data security policies and programs, and data breach management.

---

Preliminary Word

- This presentation provides information about the law. Legal information is not the same as legal advice, which involves the application of law to an individual's specific circumstances. The interpretation and application of the law to an individual’s specific circumstance depend on many factors. This presentation is not intended to provide legal advice.

- The information provided in this presentation is drawn entirely from public information. The views expressed in this presentation are the authors’ alone and not those of the authors’ clients.
Upcoming Webinars

- **July 14** -- Practical Tips for Avoiding Privacy Enforcement and Lawsuits
- **July 28** -- Toward Privacy by Design: Smart Grid and Other Technologies

The Issues

- Knowing how the data you collect is being used, stored, and secured, and who has access to it
- Identifying breaches
- Managing notifications to individuals, state agencies and consumer reporting agencies from a data breach incident
- Best practices
Agenda

- Setting the Scene
- Sector-Specific Federal Laws
- State Laws
- Major Data Breaches and the Aftermath
- Congressional Hearings and Legislation
- FTC and State Enforcement
- Best Practices

What Data is Collected and Stored

- First and last name
- Email address
- Mailing address
- Phone and/or fax number
- Credit card, financial account information
  - With or without PIN or access code
- Social Security Number
- Driver’s license number
- Health information
- Biometric data
Ways that Data is Compromised

- Hacking
- Phishing
- Lost or stolen laptop, PDA, portable memory device, hard drive, etc.
- Inadvertent disclosure
- Improper disposal
- Copying, forwarding, etc.
- Software problems

Identifying Breaches

- Intrusion detection
- Automatic software
- Unusual traffic
- Periodic audits
Sector-Specific Federal Laws

- **Health**
  - Health Information Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic and Clinical Health (HITECH) Act

- **Financial**
  - Gramm-Leach-Bliley Act

- **Credit**
  - Fair Credit Reporting Act (FCRA)
  - Fair and Accurate Credit Transactions Act (FACTA)
  - FTC Red Flags Rule

State Laws

- Data Breach Notification
- Data Security
- Social Security Numbers
- Records Destruction
- Consumer Protection
Patchwork of State Laws

- 46 states and District of Columbia have laws governing notification to residents whose personal information (PI) was or is believed to have been compromised
  - Many laws are based on the CA law, which was the first to be enacted
- Alabama, Kentucky, New Mexico, and South Dakota do not have data breach notification laws
Personal Information

- PI generally defined as first name/initial and last name plus
  - SSN
  - Driver’s license number
  - Credit card number with a PIN, access code, etc. that permits access
- A few laws also cover medical and health insurance information, biometric data, and fingerprints

Differences Among Laws

- Most laws apply to unencrypted computerized “personal information,” but some apply to all data, whether in paper or electronic form
- Different standards for whether incident is reportable
- Some states require specific content for notices
- Some states require that state agencies and CRAs be notified in addition to residents
  - Some agencies must be notified before residents
  - Some states have threshold (e.g., notify agency or and/or CRA if > 1,000 residents to be notified)
Notification to Individuals

- **Timing**
  - Most states require notification in most expedient time possible, without unreasonable delay
  - FL and OH: within 45 days

- **Type**
  - Written
  - Electronic
  - Telephone (some states)
  - Fax (some states)
  - Substitute Notice

- **Specific Content**
  - Approximately 15 states

State Data Security Laws

- Massachusetts requires all companies that store or maintain PI about a resident to implement a comprehensive written information security program, conduct security reviews, and implement employee training
  - PI tied to definition for breach notification purposes
  - Regulations set forth minimum requirements for the security program and minimum technical requirements for computer systems

- Several states require companies that acquire, own, or license PI about a resident to implement and maintain reasonable security procedures and practices to protect PI from unauthorized access, destruction, use, modification, or disclosure
Recent Data Breaches

- **Sony (April and May 2011)**
  - Names, addresses, email addresses, birth dates, passwords, and logins for > 100 million consumers

- **Epsilon (April 2011)**
  - Names and email addresses for > 60 million of its business customers’ clients

- **Texas Comptroller’s office (April 2011)**
  - Names, addresses, SSNs, dates of birth, and driver’s license numbers for 3.5 million residents on server accessible to the public

- **Citigroup (June 2011)**
  - Names, account numbers and email addresses of > 360,000 customers

- **Sega (June 2011)**
  - Names, birth dates, e-mail addresses and encrypted passwords for 1.3 million users
Aftermath of Sony and Epsilon Breaches

- Multiple lawsuits filed in U.S. federal courts
- Congressional hearings
- Federal data breach notification legislation introduced
- Sony’s estimated costs reportedly $170 million for data security remediation, customer services, and legal fees by the close of 2011 fiscal year
  - Includes credit monitoring and $1 million identity theft insurance policy per U.S. customer affected
- Global investigations ongoing

Sony Data Breach Lawsuits

- First lawsuit filed just days after notice of the breach; dozens of lawsuits filed in U.S. federal courts
  - Claims for monetary compensation and free credit card monitoring
  - Alleged that Sony failed to take reasonable care to protect, encrypt, and secure data and delayed breach notifications to consumers
  - Seeking class action status
- Most recent lawsuit alleged that Sony laid off several employees in network security unit just weeks before the breach and the company protected corporate data, but not consumer data
Aftermath of Texas Comptroller Breach

- Class action lawsuit filed in District Court
  - McClung v. Combs (April 29, 2011)
  - Seeks penalty of $1,000 for each victim, plus damages and attorney's fees
- Cost around $1.8 million
  - $1.2 million for notification letters
  - $300,000 for consulting services
  - $393,000 to set up call center for inquiries

Aftermath of Citigroup Breach

- Company criticized for delayed disclosure
- Company criticized for not offering one year of credit monitoring services
- Senator Robert Menendez (D-NJ) sent letter to Office of the Comptroller of the Currency requesting an investigation given the implications for financial industry security and the company's failure to immediately notify
Claridge v. RockYou

- N.D. Cal., Dec. 28, 2009
- RockYou suffered breach in 2009 that exposed unencrypted personal information for 32 million users
- Judge dismissed 5 of Plaintiff’s causes of action, but allowed breach of contract and negligence claims
Congressional Hearings

- **March 16, 2011: The State of Online Consumer Privacy**
  - Senate Committee on Commerce, Science, and Transportation

- **May 4, 2011: The Threat of Data Theft to American Consumers**
  - House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade
  - Epsilon and Sony declined to testify
  - FTC testified

- **June 2, 2011: Sony and Epsilon: Lessons for Data Security Legislation**
  - House Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade
  - Epsilon and Sony testified

- **June 15, 2011: Data Security and Breach Notification Legislation**
  - House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade
  - FTC testified

Federal Breach Notification Legislation

- **Data Accountability and Trust Act (H.R. 1707)**
  - Rep. Bobby Rush (D-IL)

- **Data Accountability and Trust Act (H.R. 1841)**
  - Rep. Cliff Stearns (R-FL)

- **Personal Data Privacy and Security Act of 2011 (S. 1151)**
  - Senator Patrick Leahy (D-VT)

- **Secure and Fortify Electronic Data Act (H.R. __)**
  - Rep. Mary Bono Mack (R-CA)
Data Accountability and Trust Act


- PI defined as name, address, or phone number plus SSN or driver’s license number or financial account/credit card number and security/access code
- Must notify individuals and FTC upon discovery of breach
- Specific methods and content for notices to consumers
- Exemption if no reasonable risk of ID theft, fraud, other unlawful conduct
- FTC to promulgate regulations regarding information security
- FTC to enforce violations as unfair or deceptive acts or practices
- State AGs can bring civil actions (except while FTC action pending)
- No private right of action
- Preempts state information security and breach notification laws

SAFE Data Act (H.R. ___)

Rep. Mary Bono Mack (R-CA) – Discussion Draft

- PI defined as first name/initial and last name, address, or phone number plus SSN or driver’s license number, passport #, military ID #, etc. or financial account number or credit or debit card number and security code, access code, password that permits access
- Must notify law enforcement officials within 48 hours after discovery
- Must notify FTC and affected individuals within 48 hours of completing breach assessment
- Specific methods and content for notices to individuals
- Exemption if no reasonable risk of ID theft, fraud, other unlawful conduct
- FTC to promulgate regulations regarding information security
- FTC to enforce violations as unfair or deceptive acts or practices
- State AGs can bring civil actions (except while FTC action pending)
- No private right of action
- Preempts state information security and breach notification laws
Personal Data Privacy and Security Act

S. 1151- Senator Patrick Leahy (D-VT)

- Sensitive Personally Identifiable Information (SPII) defined as
  - First name/initial and last name plus either SSN, driver’s license number, passport #, unique biometric data, unique account identifier, user name or routing code plus security code, access code, etc. or any two of home address or telephone number, mother’s maiden name, DOB
  - Financial account number or credit or debit card number plus security code, access code, pass code, etc.
- Notify consumers without unreasonable delay
- Notify CRAs if > 5,000 individuals to be notified
- Notify U.S. Secret Service and FBI in certain circumstances
- Describes content of notices
- Entities that collect, access, transmit, use, store, or dispose of SPII for 10,000 or more individuals must implement privacy and security program
- State AGs can bring civil actions (after consultation with U.S. AG)
- No private right of action
- Preempts state data breach notification laws

Obama Administration Proposal

- SPII includes any information or compilation of information, in electronic or digital form that includes first and last name plus any two of:
  - home address or telephone number, mother’s maiden name, or DOB
  - SSN, driver’s license, passport number, etc.
  - unique biometric data
  - unique account identifier, financial account number, credit or debit card number, electronic identification number, user name, routing code
- Covers entities that use, access, transmit, store, dispose of or collect SPII of > 10,000 individuals during any 12-month period
- Must notify without unreasonable delay (not to exceed 60 days)
- Notification not required if no reasonable risk of harm
- Must notify CRAs if > 5,000 individuals to be notified
- FTC to enforce violations as unfair or deceptive acts or practices
- State AGs can bring civil actions (except while FTC action pending)
- Preempts state data breach notification laws
FTC Enforcement

- Bureau of Consumer Protection Division of Privacy and Identity Protection oversees matters pertaining to consumer privacy, credit reporting, identity theft, and information security
- Division enforces Section 5 of the FTC Act, FCRA, Red Flags Rule, GLB Act, etc.
- Since 2001, FTC has brought 34 cases charging businesses with failing to protect consumers’ personal information
Recent FTC Settlements

- **Ceridian Corporation** and **Lookout Services**
  - Failure to employ reasonable and appropriate security measures to protect the sensitive and personal information of consumers, in violation of Section 5(a) of the FTC Act
  - Companies must maintain a comprehensive information security program to protect the security, confidentiality, and integrity of personal information collected from or about consumers
  - Companies must obtain independent, third party security audits every other year for 20 years

FTC Twitter Settlement

- Hackers gained administrative control of Twitter between January and May of 2009 due to lapse in data security
- Company barred for 20 years from misleading consumers about security and privacy protections
- Company must maintain comprehensive information security program; assessed by auditor every other year for 10 years
MA Data Breach Settlement

- MA Attorney General settlement with the Briar Group, LLC, owner and operator of several Boston-area bars and restaurants, over breach of credit card information for tens of thousands of consumers
- Lawsuit filed in MA Superior Court alleging that hackers gained access to the Briar Group’s computer systems in April 2009 and misappropriated customer data; malcode not removed until December 2009
- Settlement Terms
  - Pay $110,000 in civil penalties
  - Comply with MA data security regulations
  - Comply with Payment Card Industry Data Security Standards
  - Establish and maintain an enhanced network security system
Map the Data

- What type of personal information is collected
- How is it collected
- Where and how is it stored
- Who has access
- Identify and assess reasonably foreseeable risks and safeguards

Service Providers

- Review provider’s data security practices; compare with company’s
- Visit facilities
- Contractually require providers to implement and maintain appropriate security measures
- Contractually require providers to notify company in the event of any security incident
Employees

- Create company awareness
- Establish policies for storage, access, and transport of records
- Designate and train employees
- Conduct background checks
- Require confidentiality agreements
- Limit access to those with a need to know
- Implement disciplinary measures for violations
- Prevent terminated employees from accessing records

Data Security

Physical
- Store paper documents, files, CDs, disks, tapes, etc. in a locked cabinet
- Limit access to offices, cabinets, computers, networks where data stored
- Log off computers, lock cabinets and offices when not in use

Electronic
- Run security software, anti-virus and anti-spyware programs
- Employ encryption, firewalls, and Secure Sockets Layer (SSL) technology
- Secure Wi-Fi networks
- Use “strong” passwords to control access
- Regularly change passwords
- Use intrusion detection systems, monitor traffic to detect breaches
Laptop Security

- Restrict use
- Only store sensitive information on laptops if necessary
- Store laptops securely
- Employ encryption
- Adopt remote erasure features

Data Breach Response Plan

- Identify scope of breach
- Understand applicable laws
  - How laws are triggered
  - Who must be notified
  - When must they be notified
  - How must they be notified
Data Breach Response Plan

- Adopt written breach response plan
- Determine available remedies (e.g., free credit monitoring, insurance) and under what circumstances they will be offered
- Identify law enforcement, state agency, CRA contacts

Data Breach Response Plan

- Identify individual(s) responsible for implementing response plan
- Establish target timeline for internal investigations and response
- Consider proactive outreach to FTC
- Prepare FAQs
  - Press
  - Consumers
Breach Response Plan

- Document actions taken in response to a breach
- Anticipate regulatory investigations, litigation in the wake of a major breach

Questions?

www.khlaw.com
Washington, D.C. ● Brussels ● San Francisco ● Shanghai
Upcoming Webinars

- **July 14** -- Practical Tips for Avoiding Privacy Enforcement and Lawsuits
- **July 28** -- Toward Privacy by Design: Smart Grid and Other Technologies

All webinars will be held from 11:00 a.m. – 12:30 p.m. ET

Thank you!

Sheila A. Millar  
Partner  
Keller and Heckman LLP  
1001 G Street, N.W.  
Washington, DC 20001  
202-434-4143  
millar@khlaw.com

Tracy P. Marshall  
Partner  
Keller and Heckman LLP  
1001 G Street, N.W.  
Washington, DC 20001  
202-434-4234  
marshall@khlaw.com