Data Security: Risks, Compliance and How to be Prepared for a Breach

Presented by:

Sandy B. Garfinkel, Esq.

ECKERT SEAMANS
ATTORNEYS AT LAW

The Data Breach Reality: 2015

AshleyMadison.com (July 2015)

- Member site facilitating personal connections for the purpose of extramarital affairs
- Hackers gain access to names and profile info of members
- 39,000,000 records exposed
- Threat: "We will publish unless the site is shut down"

ECKERT SEAMANS
ATTORNEYS AT LAW

The Data Breach Reality: 2015

June 2015: Federal Office of Personnel Management Announces Data Breach

- **21.5 million people now believed to be affected**
- **Chinese government elements suspected**
- **Breach not limited to federal employees – family members' data was also exposed**

ECKERT SEAMANS ATTORNEYS AT LAW

The Data Breach Reality: 2015

Anthem (Feb. 2015)

Over 80,000,000 Consumers Affected

Information accessed:

residential addresses, birthdates, medical identification numbers, Social Security Numbers, email addresses

ECKERT SEAMANS ATTORNEYS AT LAW

The Data Theft Reality

- Hackers are ahead of the game; security technology cannot keep up
- Security industry sources:
  - 79% of all companies and organizations in the U.S. have had a data breach in the past two years

ECKERT SEAMANS
ATTORNEYS AT LAW

A Decade of Breaches

2005 to September 1, 2015

Number of reported breaches = 5,562

Number of records exposed = 818,746,307

Source: Identity Theft Research Center

ECKERT SEAMANS
ATTORNEYS AT LAW

Target Targeted

December 2013:

- **Target Hacked in Pre-Christmas Attack**
  - Up to 70 million Target customers affected
  - Customer names, credit/debit card numbers, card expiration dates, debit-card PINs and magnetic strip data
  - Also non-payment card info: phone numbers, e-mail addresses

ECKERT SEAMANS
ATTORNEYS AT LAW

SONY Pictures

- Blackmail-style threats made concerning release of film “The Interview”
- Hacker infiltrated system, stole and disseminated highly sensitive data
- State sponsored activity? Or disgruntled former employee?

ECKERT SEAMANS
ATTORNEYS AT LAW

How Quickly We Forget

Since Target:

- Home Depot
- JP Morgan Chase
- K-Mart

ECKERT SEAMANS
ATTORNEYS AT LAW

Notable Breaches

Home Depot
109,000,000 Records Stolen

JP Morgan Chase
83,000,000 Records Stolen

Sony Pictures Entertainment
47,000 Records Stolen

eBay
145,000,000 Records Stolen

ECKERT SEAMANS
ATTORNEYS AT LAW

Wyndham's Woes

- 2008, 2009, 2010: *Wyndham Worldwide* suffered 3 separate attacks on its central property management and reservations systems – approximately 45 individual hotels were hit, and about 800,000 credit card accounts were stolen

ECKERT SEAMANS
ATTORNEYS AT LAW

2014

1,541 separate incidents

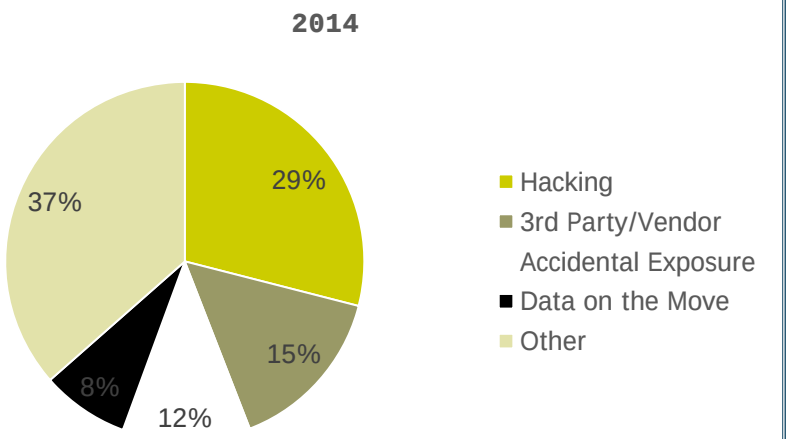
106 severe possibly even catastrophic*

Representing a 46% increase in data breaches from 2013

Source: Gemalto 2014 Breach Level Index Report

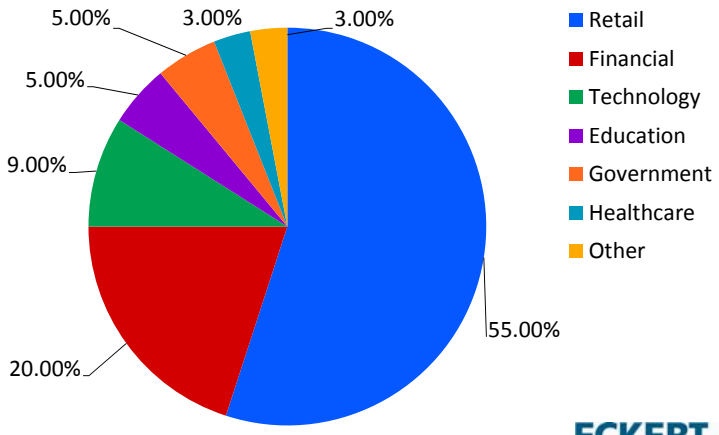
ECKERT SEAMANS
ATTORNEYS AT LAW

How is Data Getting Compromised?



ECKERT SEAMANS
ATTORNEYS AT LAW

Lost/Stolen Records



ECKERT SEAMANS
ATTORNEYS AT LAW

State Laws Generally Control Notification

- 47 States and the District of Colombia have data protection/notification laws
- PA Breach of Personal Information Notification Act, 73 P.S. § 2301 et seq.
- Congress has been considering multiple proposals for a federal data protection/notification law that may or may not preempt state laws
- As to certain specific types of data, federal laws and regs may control notification (e.g., HIPAA, HITECH)

ECKERT SEAMANS ATTORNEYS AT LAW

Typically Protected Data ("PII")

Credit/Debit Card Account Information (name of cardholder, account numbers, passwords)

- Bank or Financial Account Information (name of cardholder, account nos., passwords)
- Social Security Numbers
- Driver's License Numbers

ECKERT SEAMANS ATTORNEYS AT LAW

Protected Only In Certain States:

- Medical Information
- Health Insurance Information
- Biometric Data (fingerprint, voiceprint, retina image)
- Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names
- Digital signatures
- Parent's legal surname prior to marriage

ECKERT SEAMANS
ATTORNEYS AT LAW

Not Protected

- Publicly available information that is lawfully made available to the general public from Federal, State or local government records
- Information that an individual has consented to have publicly disseminated or listed (under some state laws only)

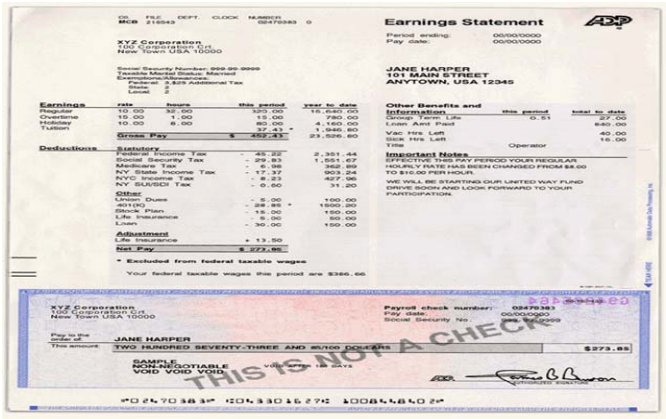
ECKERT SEAMANS
ATTORNEYS AT LAW

Paper Files Are Not Immune

- ***Misconception*** that data theft is always a high-tech attack on electronically stored information
- Paper files containing personal information can be just as vulnerable and are often the target of theft
- Some state laws are confined only to addressing electronic breaches, but a few specify that personal information stored in paper form is covered

ECKERT SEAMANS
ATTORNEYS AT LAW

Employee Data



ECKERT SEAMANS
ATTORNEYS AT LAW

Types of Protected Employee Information

- Personnel File
- Payroll File

ECKERT SEAMANS
ATTORNEYS AT LAW

Personnel Files

- Employment Application, which may include:
  - Name and address
  - Social Security Number
  - Possibly e-mail address
- Tax forms (W-2, W-4) will have Social Security Number
- If employment involves driving, possibly Driver License Number

ECKERT SEAMANS
ATTORNEYS AT LAW

Personnel Files (cont.)

- Employee Benefit Election Forms
  - Social Security Numbers for Employee and Family Members
    - Medical Information - may find its way into the file (e.g., workers' comp or disability claim)

ECKERT SEAMANS
ATTORNEYS AT LAW

Payroll File

- Tax forms (W-2, W-4) will have Social Security Number
- Direct Deposit Forms will include Bank Account Information
- If paycard payment system has been adopted, the file might include what would be considered Credit/Debit Card Information

ECKERT SEAMANS
ATTORNEYS AT LAW

Social Security Numbers

- Industry experts: Social Security Numbers are the most key piece of information exploited by identity thieves
- Social Security Numbers can be used to:
  - File false tax returns
  - Apply for new credit cards
  - Access financial accounts

ECKERT SEAMANS
ATTORNEYS AT LAW

Response & Notification

ECKERT SEAMANS
ATTORNEYS AT LAW

Which State's Law Applies?

- *The law of the state where the affected individual (cardholder, employee) resides is the law that governs notice* -- NOT the state where the merchant or employer is situated.
- This means that some merchants or businesses may have to comply with *many* state's laws when responding to a single breach

ECKERT SEAMANS
ATTORNEYS AT LAW

"Breach"

Example: PA's "Breach of Personal Information Notification Act" – defines breach as:

- *Unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.*

ECKERT SEAMANS
ATTORNEYS AT LAW

"Breach"

Example: Hawaii "Notification of Security Breaches" law:

- *(I) Unauthorized access to and acquisition of unencrypted or unredacted records or data (computerized, paper or otherwise) where the illegal use of the personal information has occurred, or is reasonably likely to occur and that creates a risk of harm to a person; OR*
- *(II) Unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key.*

ECKERT SEAMANS
ATTORNEYS AT LAW

Typical Breach Notification Act - When Breach Occurs, Who Must Issue Notification?

- An entity that maintains, stores or manages computerized data that includes personal information.
- A vendor that maintains, stores or manages computerized data on behalf of another entity must notify the entity on whose behalf the computerized data is maintained, stored or managed. The entity on whose behalf the computerized data is maintained, stored or managed must discharge the remaining notice duties.

ECKERT SEAMANS
ATTORNEYS AT LAW

Third Party Vendor Breaches

PAYTIME: 2014

- Outside payroll vendor
- Breach potentially compromised every customer account
- Information on both current and former employees
- Names, addresses, Social Security Numbers and other types of info
- Even though the third-party payroll vendor was in possession of the payroll information when it was exposed, the employer is the party responsible by law for issuing notifications to affected employees

ECKERT SEAMANS
ATTORNEYS AT LAW

Who Receives Notice:

- The individual (employee, cardholder, consumer)
- The entity on whose behalf a vendor maintains, stores or manages the data
- The nationwide credit reporting agencies must be notified; usually this is triggered if more than 1,000 individuals receive notice at one time
- Some statutes require a separate notice and/or copy of consumer notice to be sent to the state attorney general and/or a state consumer protection agency

ECKERT SEAMANS
ATTORNEYS AT LAW

Timing

Most state statutes require that notifications must be issued "*without unreasonable delay*."

- EXCEPTIONS
  - Notification may be delayed if a law enforcement agency determines that it will impede a criminal or civil investigation and the agency has so advised in writing. Notification is required after the law enforcement agency determines that it will no longer compromise the investigation or national or homeland security
  - Notification may be delayed to determine the scope of the breach and to restore the reasonable integrity of the data

ECKERT SEAMANS ATTORNEYS AT LAW

Changing State Law Landscape

- State Data Breach Notification laws change and evolve
- FLORIDA and IOWA amended their laws in 2014
- **Florida**:
  - 30 day deadline for notification from determination of a breach or reason to believe a breach occurred

ECKERT SEAMANS ATTORNEYS AT LAW

Content of Notice

Massachusetts

- Individual's right to obtain a police report
- How to request a security freeze and necessary information to be provided when requesting a security freeze and any required fees
- Notification (to residents) shall not include the nature of the breach or the number of residents affected by the breach

ECKERT SEAMANS
ATTORNEYS AT LAW

Consequences of Non-Compliance

- PA:
  - The attorney general may bring an action for unfair or deceptive trade practices under the PA Unfair Trade Practice Act & Consumer Protection Law (no private right of action for affected individual)
- CA:
  - Permits individual cause of action "to recover damages," also civil penalty for willful or intentional violation of up to $3,000 per violation

ECKERT SEAMANS
ATTORNEYS AT LAW

Private Claims – Class Actions

Most decisions by far:

Increased risk of identity theft is insufficient to confer standing.

- *In re Horizon Healthcare Services, Inc. Data Breach Litigation*, No. 2:13-cv-07418-CCC-JBC (D.N.J. Mar. 31, 2015)
- *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011)

ECKERT SEAMANS ATTORNEYS AT LAW

Private Claims – Class Actions

BUT:
Remijas v. The Neiman Marcus Grp. LLC (7th Circuit No. 14-3122, 8/3/15) – increased risk of identity theft is sufficient to create standing

AND:
Some companies choose to settle rather than litigate.

- Public relations
- Litigation costs savings

TARGET - $10,000,000 class action settlement fund established

ECKERT SEAMANS ATTORNEYS AT LAW

New Trend: Safe Destruction

July 1, 2014:

- **DELAWARE** passed a law governing safe destruction of records containing a consumer's personally identifiable information
- Requires commercial entities to shred, erase, or to otherwise destroy or modify the records to make the personal information entirely unreadable or indecipherable through any means
- Consumers actually harmed by violations of the law may file a civil action and seek treble damages

ECKERT SEAMANS
ATTORNEYS AT LAW

Federal Data Breach Law?

- Currently several different data breach bills pending before U.S. Congress
- Passage of a federal data breach law is likely to preempt state law – could result in greater consistency: (a) types of data protected, (b) pre-breach security standards and (c) response and notification requirements
- Critics of proposed laws: They weaken current consumer protections in some states

ECKERT SEAMANS
ATTORNEYS AT LAW

Personal Data Notification & Protection Act

- Designed to preempt state notification laws except regarding victim protection assistance
- "*Sensitive Personally Identifiable Information*" far more broad than most states' definitions of PII
- FTC primary enforcement authority; FCC and Consumer Financial Protection Bureau would also have roles
- 30 days from knowledge of the breach to issue notifications to consumers
- Approved by Congressional Committee in April 2015, but bill has stalled.

ECKERT SEAMANS
ATTORNEYS AT LAW

NEW FTC GUIDELINES

June 30, 2015:

Start with Security: A Guide for Business

1. Start with security (develop an appropriate, proactive cybersecurity plan)
2. Control access to data sensibly
3. Require secure passwords and authentication
4. Store sensitive personal information securely and protect it during transmission
5. Segment networks and monitor who's trying to get in and out

ECKERT SEAMANS
ATTORNEYS AT LAW

FTC Guidelines (Cont'd.)

6. Secure remote access to networks
7. Apply sound security practices when developing new products
8. Make sure service providers implement reasonable security measures
9. Put procedures in place to keep security current and address vulnerabilities that may arise
10. Secure paper, physical media, and devices

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

ECKERT SEAMANS
ATTORNEYS AT LAW

INCIDENT RESPONSE PLAN

- **Action Plan– detection, analysis, recovery and post-incident procedures**
- **Employee Policies & Procedures**
  - Limiting who has access
  - Protocols for transferring information
  - Working off-site
  - Confidentiality & Non-Disclosure Agreements and policies
  - Regularly purging information – document retention policies

ECKERT SEAMANS
ATTORNEYS AT LAW

INCIDENT RESPONSE PLAN

- Internal Procedures – detection, analysis, recovery and post-incident procedures
- Internal Resources – security incident response team (SIRT)
- External Resources
  - Legal
  - Security/Forensics
  - Public Relations
  - Law Enforcement

ECKERT SEAMANS
ATTORNEYS AT LAW

Cyber Insurance

- There <u>may be</u> some coverage under existing General Liability or D&O policies
- BUT: Stand-alone cyber insurance products are the new wave
- Not all cyber insurance is the same
- Some include program of incident response services: legal counsel, crisis management, forensic investigation and other resources

ECKERT SEAMANS
ATTORNEYS AT LAW

The End …?

Not by a longshot.

Stay tuned for:

- More high-profile data breach stories
- More legislative action by states and possibly the federal government
- More cyber threats and more defenses to respond to them

ECKERT SEAMANS
ATTORNEYS AT LAW

Questions?

Sandy B. Garfinkel, Esq.
(412) 566.6868 | sgarfinkel@eckertseamans.com

ECKERT SEAMANS
ATTORNEYS AT LAW