The Current State of the Law: Data Privacy and Security

Presented by:

Sandy B. Garfinkel,
Eckert Seamans Cherin & Mellott, LLC

March 7, 2017

ECKERT SEAMANS
ATTORNEYS AT LAW

DATA SECURITY

The confidentiality, availability, and integrity of data.

Includes all practices and processes to ensure data is not used or accessed by unauthorized parties.

DATA PRIVACY

The appropriate collection and use of data.

ECKERT SEAMANS
ATTORNEYS AT LAW

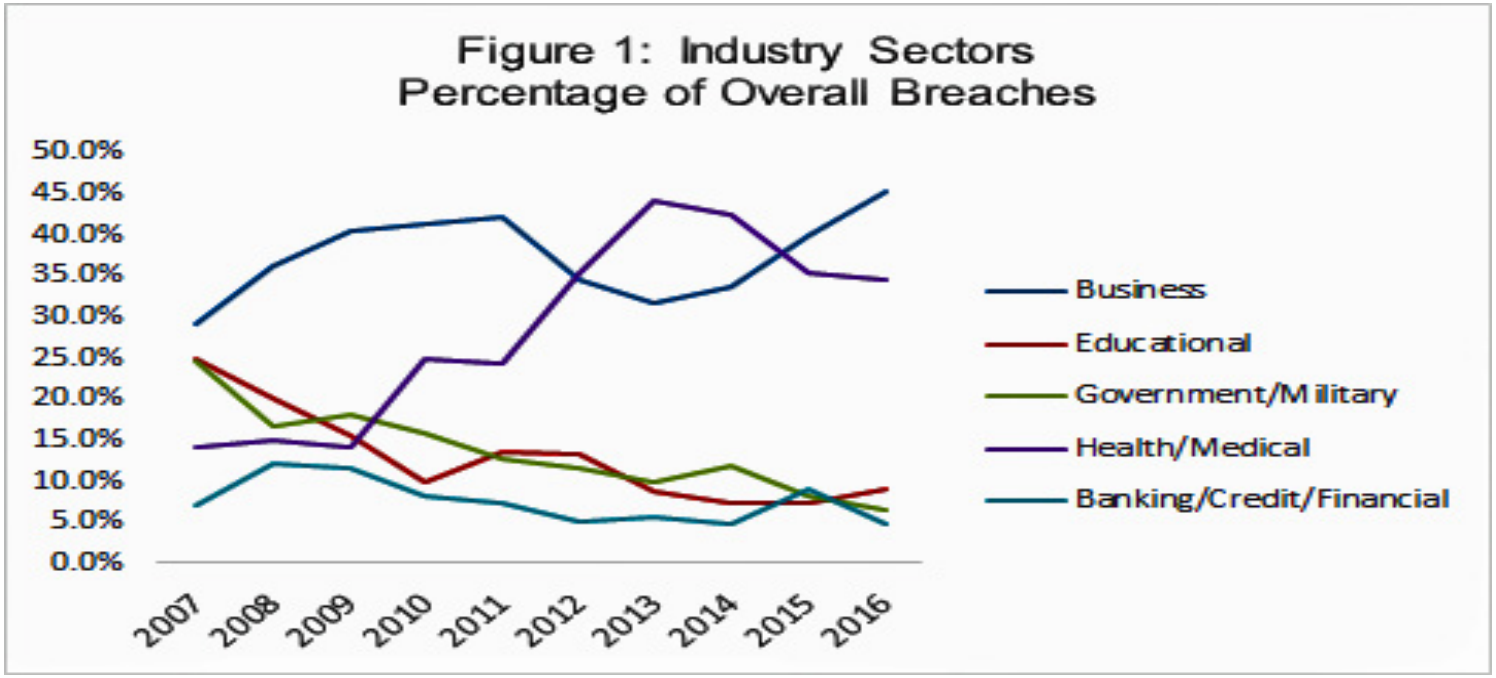
2016 – A Big Year For Breaches

- U.S. data breaches tracked in 2016: **1,093**
- Data Breaches Increased by 40% in 2016
- Business sector had the highest number of data breach incidents, with 494 reported, representing 45.2 percent of the overall number of breaches

Source: Identity Theft Resource Center

ECKERT SEAMANS
ATTORNEYS AT LAW

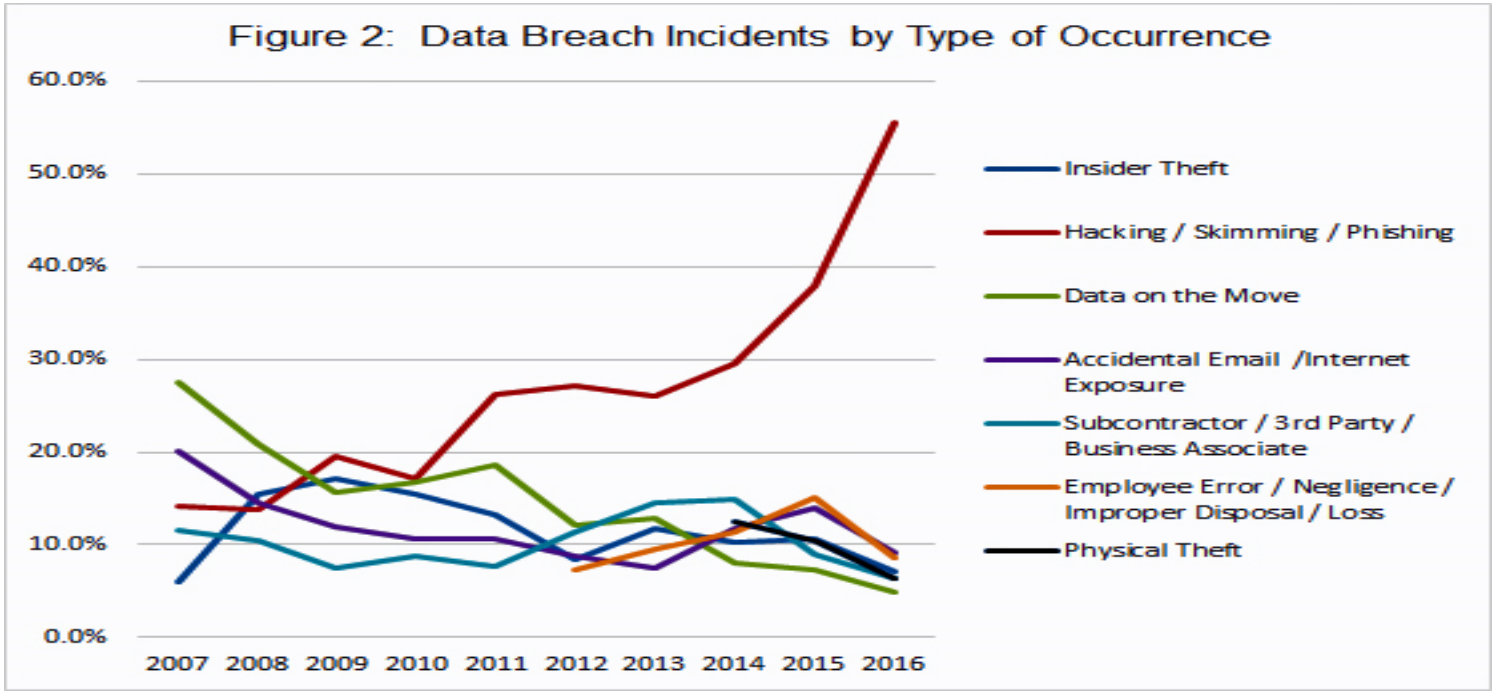
Breaches by Industry - 2016



Source: Identity Theft Resource Center

ECKERT SEAMANS
ATTORNEYS AT LAW

How is Data Getting Compromised?



Source: Identity Theft Resource Center

ECKERT SEAMANS
ATTORNEYS AT LAW

Yahoo!: The Biggest Breach Yet?

Two separate incidents -

- Occurred in 2014, reported September 2016, affected over 500 million user accounts
- Occurred in 2013, reported December 2016, affected over 1 billion user accounts
- names, email addresses, telephone numbers, encrypted or unencrypted security questions and answers, dates of birth, and encrypted passwords

ECKERT SEAMANS
ATTORNEYS AT LAW

DATA SECURITY AND PRIVACY LAWS

ECKERT SEAMANS
ATTORNEYS AT LAW

Federal Laws

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Fair Credit Reporting Act (FCRA)
- Children's Online Privacy Protection Act (COPPA)

ECKERT SEAMANS
ATTORNEYS AT LAW

State Laws Generally Control Notification

- 47 States and the District of Colombia have data protection/notification laws
- Notification timing, content and triggers may differ from state to state
- Congress has considered 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

Enforcement Agencies

- Federal Trade Commission
- Consumer Financial Protection Bureau
- Federal Communications Commission
- U.S. Dept. of Health & Human Services
- State Attorneys General

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

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

What is a "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

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

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
- Notification may be delayed to determine the scope of the breach and to restore the reasonable integrity of the data
- **Trend**: Within 30-45 days of knowledge of the incident

ECKERT SEAMANS
ATTORNEYS AT LAW

Private Claims – Class Actions

- Most decisions so 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

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

Spokeo, Inc. v. Robins, 136 S.Ct. 1540 (2016) FCRA, Standing:

1. injury-in-fact requirement - plaintiff must show he suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."
2. Violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact

ECKERT SEAMANS
ATTORNEYS AT LAW

SETTLEMENTS OF DATA BREACH AND DATA PRIVACY ACTIONS

ECKERT SEAMANS
ATTORNEYS AT LAW

Settlements of Data Breach And Data Privacy Class Actions

- Most companies choose to settle rather than litigate.
  - Public relations / reputational harm
  - Litigation costs savings
  - Risks of fines, penalties and awards

ECKERT SEAMANS
ATTORNEYS AT LAW

Target Corp.

In re: Target Corporation Customer Data Security Breach Litigation, No. 14-2522 (U.S. Dist. Court, Dist. of Minnesota)

"**If You Shopped at Target from November 27 through December 18, 2013 or Received Notice That Your Personal Information Was Compromised, You Could Get Money from a Data Breach Settlement."**

- $10 Million Settlement Fund
- Up to $10K per claim
- To banks with MasterCard $39 million and Visa $67 million
- **BUT …**

ECKERT SEAMANS
ATTORNEYS AT LAW

February 2017:

- One person objected to settlement
- Eighth Circuit Court of Appeals: Trial court should have considered whether people who did not actually lose anything may proceed against Target for potential future losses.
- Settlement on hold

ECKERT SEAMANS
ATTORNEYS AT LAW

Home Depot

In re: The Home Depot, Inc., Customer Data Security Breach Litigation, Case No. 1:14-md-02583-TWT (U.S. Dist. Court, Northern Dist. of Georgia)

"If You Used a Credit or Debit Card at a Self-Checkout Lane at a U.S. Home Depot Store Between April 10, 2014 and September 13, 2014 or Received Notice From Home Depot That Your Information Was Compromised, You May Be Eligible for Benefits from a Data Breach Class Action Settlement"

- $13 Million Settlement Fund
- Up to $10K per claim

ECKERT SEAMANS
ATTORNEYS AT LAW

VIZIO

FTC v. VIZIO, Inc., 2:17-cv-00758 (U.S. Dist. Court, Dist. of NJ)

February 6, 2017:

“The FTC announced that it has agreed to settle charges that VIZIO, Inc. (“VIZIO”), installed software on about 11 million consumer televisions to collect viewing data without consumers’ knowledge or consent. The stipulated federal court order requires VIZIO to pay $2.2 million to the FTC and New Jersey Division of Consumer Affairs.”

ECKERT SEAMANS
ATTORNEYS AT LAW

Other Notable Settlements:

- Ashley Madison ($1.6 million)
- New York and Presbyterian Hospital with OCR under HIPAA ($3,300,000)
- Adobe ($1 million to 15 different states)
- Advocate Health Care Network (12 hospitals and more than 200 other treatment locations in Illinois; $5.55 million to the U.S. Health and Human Services Department)

ECKERT SEAMANS
ATTORNEYS AT LAW

RELATIONSHIPS WITH THIRD PARTIES:

HOW TO PROTECT YOUR INTERESTS CONTRACTUALLY

ECKERT SEAMANS
ATTORNEYS AT LAW

Contractual Protection

DATA SECURITY

- Compliance with minimum security standards (Examples: PCI-DSS, ISO/IEC, your own internal standards)
- Breach response protocol (prompt notification, communications, notification)
- Indemnification for: investigation, mitigation, regulatory investigations & claims, fines/penalties, third party claims
- Cyber insurance in place, covers your company

ECKERT SEAMANS
ATTORNEYS AT LAW

Contractual Protection (Cont'd)

- Define: Who is authorized, what information is protected (e.g., PII vs. "Confidential" or trade secret), what constitutes a breach
- Collection, access, use, storage, disposal and disclosure – all compliant with law

ECKERT SEAMANS
ATTORNEYS AT LAW

Contractual Protection (Cont'd)

DATA PRIVACY

- Collection/sharing/utilization of data will be compliant with applicable law (domestic and foreign)
- Data sharing or selling is prohibited or may not be done without consent
- Compliant privacy policies and disclosures are in place
- Indemnification for: investigation, mitigation, regulatory investigations & claims, fines/penalties, third party claims

ECKERT SEAMANS
ATTORNEYS AT LAW

WHAT DOES THE FUTURE HOLD?

ECKERT SEAMANS
ATTORNEYS AT LAW

TRENDS and PREDICTIONS

- Aftershock password breaches will expedite the death of the password
- Nation-State cyber-attacks will move from espionage to war
- Healthcare organizations will be the most targeted sector with new, sophisticated attacks emerging
- Criminals will focus on payment-based attacks despite the EMV shift taking place over a year ago
- International data breaches will cause big headaches for multinational companies

Source: Experian 2017 Data Breach Industry Forecast

ECKERT SEAMANS
ATTORNEYS AT LAW

Questions?

Sandy B. Garfinkel, Esq.
412.566.6868 | sgarfinkel@eckertseamans.com

ECKERT SEAMANS
ATTORNEYS AT LAW