PIERCE ATWOOD LLP

Privacy & Data Security

2014 Year in Review

Agenda

- The Year of the Data Breach
- Federal Regulatory Developments
- Litigation Developments
- State Developments
- Big Data
- Key Takeaways

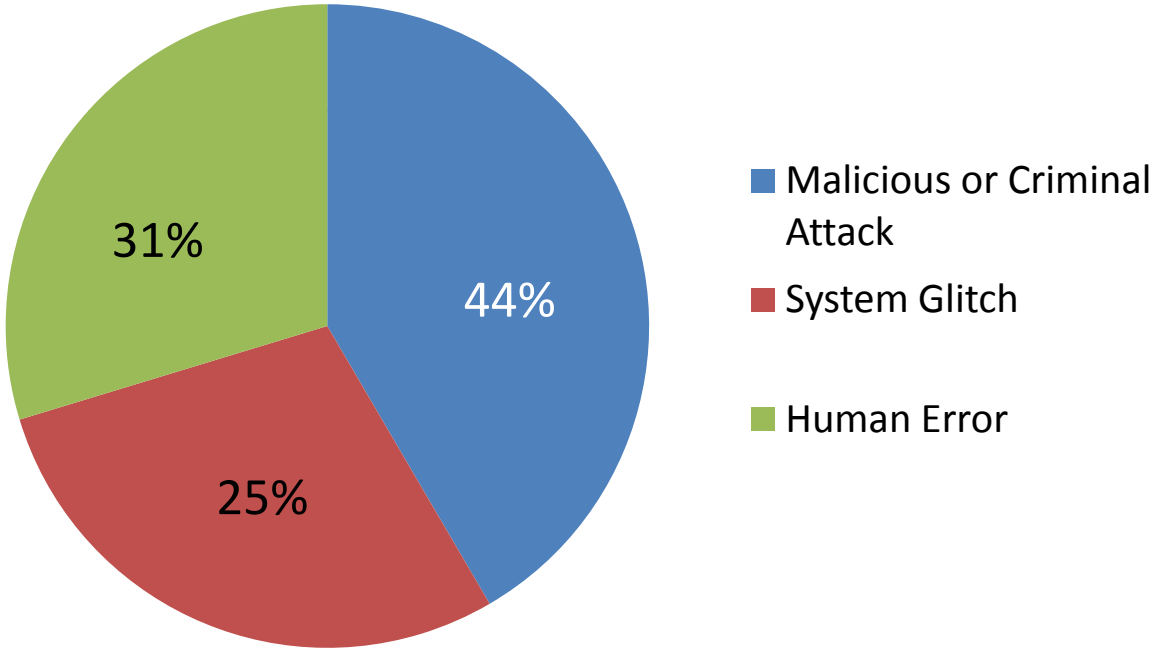
The Year of the Data Breach

"If you buy a card for 20 bucks and you can make 400 dollars off each card, that's a pretty good return on your investment." Brian Krebs

Data Breach Facts

Ponemon Institute "2014 Cost of Data Breach Study: Global Analysis"

U.S. Causes of a Data Breach



Per Capita Costs

(total cost of a data breach / number of lost or stolen records)

- **Average per capita costs**

  2013: $188 2014: $201

- **Per capita costs for three root causes**
  - Malicious/criminal attack: $246
  - System glitch: $171
  - Human error: $160

- **Average organizational cost in the U.S.**
  - 2013: $5.40 million
  - 2014: $5.85 million

Sony Data Breach

- "I'm not destroying my career over a minimally talented spoiled brat…"
- "You've behaved abominably and it will be a very, very long time before I forget what you did to this movie and what you've put all of us through."
- A "bipolar 28 year old lunatic"

Sony Data Breach

- Broadens our understanding of the risks
  - Shut down company network
  - Threats in the event of movie release
  - Broadcast company e-mails
- Costs go far beyond regulatory compliance and litigation
  - Bad PR
  - Lost movie profits
  - Exposed trade secrets

Federal Regulatory Developments

- Federal Trade Commission
- HHS Office of Civil Rights

FTC Authority

- Section 5 of the FTC Act prohibits two kinds of conduct in trade
  - conduct that is **"unfair"**
  - conduct that is **"deceptive"**
- Failure to take reasonable measures to safeguard personal information constitutes an unfair practice
- Representations made to consumers about a company's protection of personal information are deceptive

Challenges to FTC Authority

- FTC v. Wyndham Worldwide Corp.
  - Hackers gained unauthorized access to Wyndham's network and customer's personal information (i.e., payment card info) on 3 separate occasions. Wyndham failed to take reasonable measures after discovering the first 2 breaches.

- In the Matter of LabMD, Inc.
  - LabMD billing information for over 9,000 consumers found on a peer-to-peer file-sharing network. LabMD documents containing personal information of at least 500 consumer later found in the hands of identity thieves.

FTC v. Wyndham Worldwide Corp.

- Wyndham raises the following issues:
  - Challenges FTC's authority to bring unfairness claims for failure to provide reasonable data security;
  - Alleges FTC must formally promulgate regulations prior to bringing claims; and
  - Alleges FTC did not meet its burden to demonstrate unfairness or deception

Status of the Case

- April 2014 - U.S. District Court ruled in favor of the FTC and denied Wyndham's motion to dismiss
- July 2014 - Third Circuit Court of Appeals granted Wyndham's petition to appeal.
- Third Circuit expected to rule in 2015

In the Matter of LabMD, Inc.

- FTC denied LabMD's motion to dismiss
- After 11th Circuit denied its petition to appeal, LabMD filed suit in Georgia District Court
- Georgia District Court granted the FTC's motion to dismiss
- LabMD, again, appealed to the 11th Circuit
- In August, the 11th Circuit agreed to hear oral argument

Lessons Learned from FTC Enforcement Actions

- **Accurately describe your privacy and data security practices**
- **Implement the practices you've represented to customers**
- **Mobile applications must comply with privacy and data security obligations too**

Say What You Do & Do What You Say

- **TRUSTe** misrepresentation of recertification process and failure to update corporate for-profit status
- **Snapchat** misrepresentation of disappearing nature of snapchats and the amount of personal data collected
- **EU-US Safe Harbor** 14 companies falsely claimed compliance

Mobile Apps

- **Don't misrepresent mobile app security**
  - **Fandango & Credit Karma**. Misrepresentation of the security of their mobile apps based on disabling of SSL validation.

- **Comply with COPPA**
  - **Yelp Inc.** Failure to screen-out users under the age of 13 on its mobile app resulted in COPPA violations.

Lessons Learned from OCR Enforcement Actions

- **Encrypt laptops**
- **Implement sufficient privacy and data security policies and procedures**
- **Make changes based on gaps identified in risk analysis**

Encrypt Laptops with ePHI

- **QCA Health Plan, Inc.** Unencrypted laptop stolen from employee car disclosing ePHI of ~ 150 individuals.
  - Settled for $250,000

- **Concentra Health Services**. Unencrypted laptop stolen from its facility.
  - Settled for $1,725,220

Implement Sufficient Policies & Procedures

- **Policies and procedures must be sufficient**
  - **QCA Health Plan, Inc.** Failure to implement sufficient security policies and procedures or physical safeguards.
  - **Skagit County, Washington**. Failure to implement sufficient security policies, procedures and training.
- **Once established, implement policies and procedures**
  - **Anchorage Community Mental Health Services.** ACMHS adopted sample Security Rule policies in 2005 but failed to follow such policies.

Risk Assessments

- **Conduct risk assessment**

- **Implement changes based on gaps identified in risk assessment**

  - **Concentra Health Services**. Conducted a risk analysis recognizing the risk unencrypted laptops posed but then failed to encrypt all necessary laptops.

Litigation Developments

Class Actions & Article III Standing

Private Right of Action for HIPAA Violations

Class Action Developments

- Article III standing – plaintiff must have suffered an "injury in fact"
- Courts inconsistent in defining "harm" to demonstrate "injury in fact"

No Article III Standing

- Many courts have found the increased risk of identity fraud or theft is not enough
  - Rely on Clapper v. Amnesty Int'l USA, 133 S. Ct. 1338 (2013)
  - Examples:
    - In re SAIC Backup Tape Data Theft Litig., 2014 WL 1858458 (D.D.C. May 9, 2014)
    - Strautins v. Trustwave Holdings, Inc., 2014 WL 960816 (N.D. Ill. March 12, 2014)

Article III Standing

- A number of recent cases, however, have found standing.
  - **In re Target Corporation Customer Data Security Breach Litigation**, No. 14-2522 (D. Minn. Dec. 18, 2014). Unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees were found sufficient to defeat defendant's motion to dismiss based on standing.
  - **In re Sony Gaming Networks and Customer Data Security Breach Litigation**, 996 F. Supp. 2d 942 (S.D. Cal. 2014). Future payment card fraud or identity theft found sufficient to establish injury-in-fact.

Class Action Takeaways

- Courts are inconsistent as to whether data breach causes injury-in-fact

- Even if a claim survives the initial stages (i.e., standing and motion to dismiss based on lack of harm), there are significant hurdles to class certification (i.e., individual issues re harm and causation)

- Continuously evolving

HIPAA Private Right of Action

- In Emily Byrne v. Avery Center for Obstetrics and Gynecology the Supreme Court of CT found:
  - **HIPAA does not preempt** Connecticut common law negligence claims arising from health care provider breach
  - HIPAA and its regulations may be utilized to **inform the standard of care**

State Developments

State regulatory enforcement

New state laws

State AGO's Increasingly Active

- **Multi-state investigations increasingly common**
  - E.g., MA participating in multi-state investigation into Target breach led by IL and CT AGOs
- **Overlapping jurisdiction with federal regulators**
  - E.g., Snapchat settled with Maryland AGO in addition to FTC

New State Laws

- **Kentucky** became the 47th state to enact a data breach notification law

- **Florida** passed a new data breach law which broadens the definition of "personal information" to include: 1) username or email address and 2) password or security question and answer

- **California** passed a number of new laws including AB 1710 which explicitly requires businesses that maintain personal information to comply with security and notification obligations

Big Data

Complicates principles of transparency and consent

Big Data – A Complicating Factor

- Privacy principles value transparency and consumer choice
- Lack of transparency with big data
- Data collection will continue to increase with the ubiquity of wearables and the internet of things

White House 90-Day Review

- In January President Obama called for a 90-day review of big data and privacy.

- Following this review, the administration released a report recommending Congress take the following actions:

  - Pass national data breach legislation
  - Advance the Consumer Privacy Bill of Rights
  - Expand technical expertise to stop discrimination

FTC Data Broker Report

- FTC released "Data Brokers: A Call for Transparency and Accountability"
- Provides legislative recommendations and best practices for data brokers
- Highlights importance of transparency, consumer access and choice, and limited data collection and retention for any company dealing with a data broker

Key Takeaways

Key Takeaways

- Privacy “norms” continue to evolve
- Can’t just check a box to satisfy data protection responsibilities
- Big data complicates things
- Regulatory enforcement is increasing (FTC, OCR, State AGO’s)
- Legislative action and litigation continue to press the boundaries

PIERCE ATWOOD LLP

Presenters

Peter Guffin
pguffin@pierceatwood.com

Merrill's Wharf
254 Commercial Street
Portland, ME 04101

PH / 207.791.1199

Sara Benjamin
sbenjamin@pierceatwood.com

100 Summer Street
Suite 2250
Boston, MA 02110

PH / 617.488.8162