DICKINSON WRIGHT PLLC presents

The Impact of Compliance

Online Tech – Fall Into IT
September 14, 2012

Tatiana Melnik
Attorney with Dickinson Wright PLLC
tmelnik@dickinsonwright.com | 734.623.1713

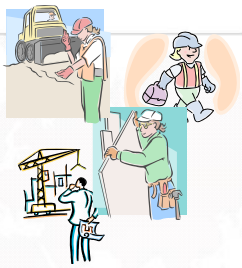
Outline

- **Part 1: Introduction**
  - Two Questions
  - A Story
- **Part 2: Compliance**
  - Regulatory Framework
  - Results of Non-Compliance
- **Part 3: What's a Company to do?**

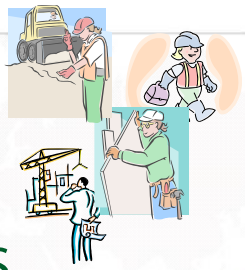
Two Questions . . .

- What do you think of when you hear the word "**compliance**"?
- What do you think of when you hear the phrase "**commercially reasonable security measures**"?

A Story . . .



A Story . . .



A Story . . .

A Story . . .

- One day . . .
  - Odd transfers –
    - 6 transfers over a 7 day period
    - New IP
    - New device
    - New people getting paid
    - New amounts ($56,000 and $116,000 vs. $37,000)
  - BUT –
    - **Answer the same security question correctly!**

A Story . . .

A Story . . .

A Story . . .

A Story . . .

- **Security Features Offered by the Bank**
  1. User ID and Password
  2. Device Identification
  3. Risk Profiling
  4. Security Questions
  5. Dollar Amount Rule
  6. eFraud Network

A Story . . .

- **Security Features NOT Offered by the Bank**
  1. Out-of-Band Authentication
  2. User-Selected Picture Functions
  3. Tokens
  4. Monitoring

A Story . . .

- Was it "commercially reasonable" for the bank to permit the transfers to go through?
  - **Bank – YES!**
    - Answered security question(s) correctly
    - Signed agreement that said user of services ultimately responsible for all transfers . . .

A Story . . .

- Was it "commercially reasonable" for the bank to permit the transfers to go through?
  - **Court – NO!**
    - Two layers of authentication – password and security question → Threshold to trigger security question lowered to $1
      - increased the no. of times answer would be typed
      - increased the risk that would be logged by malware
      - deprived the risk scoring system of its core functionality

A Story . . .

- Was it "commercially reasonable" for the bank to permit the transfers to go through?
  - **Court – NO!**
    - Also unreasonable:
      - transaction-monitoring practices
      - lack of standardization for notifying customers when high-risk transactions detected
      - one-size-fits all approach to customers

A Story . . .

- ***Patco Construction Co., Inc. v. People's United Bank***
  - Maine case
  - May 2009 - Fraud happened (~ $350K in losses)
  - 2010 - Patco sued People's United (which bought Ocean Bank)
  - May 2011 – District Court rules for People's
  - July 3, 2012 – First Circuit overturned decision and remanded the case back to district ct. (UCC Article 4A issues) (http://op.bna.com/bar.nsf/id/cbre-8vuq5j/$File/patco.pdf)

A Story . . .

- **Why do we care about Patco?**
  - Few courts have looked at this type of issue
  - In Examining **UCC Article 4A** issue, Court looked to the **Federal Financial Institutions Examination Council** guidance to assess the reasonableness of the bank's security procedures
    - FFIEC – issued guidance in 2005 on "Authentication in an Internet Banking Environment"
  - "**Collective failures taken as a whole**, rather than any single failure, which rendered Ocean Bank's security system commercially unreasonable."

Outline

- Part 1: Introduction
  - Two Questions
  - A Story
- **Part 2: Compliance**
  - Regulatory Framework
  - Results of Non-Compliance
- Part 3: What's a Company to do?

Compliance: Regulatory Framework

- **Federal Laws**
  - U.S. Constitution
  - Federal Legislation
  - State Laws
  - Common Law
  - Industry Practice

  * International Law

Compliance: Regulatory Framework

- **Federal Legislation: Context Still Matters**
  - Targeted Information
    - o Financial (GLBA)
    - o Medical (HIPAA)
  - Targeted Constituency
    - o Consumers (FTC Section 5)
    - o Children (COPPA)
  - Specific identification of information deemed to be "private"
  - Specific identification of obligations regarding the use of particular information

Compliance: Regulatory Framework

- **State Laws**
  - Various state statutes addressing
    - Social Security Numbers
    - Drivers licenses
    - Protection of health care information
    - Recordkeeping and data destruction
    - **Breach disclosure**
- **Industry Standards**
  - PCI DSS

Compliance: Regulatory Framework

- **International Laws**
  - E.U. Privacy Directive 95/46/EC
    - Addresses the collection, use, processing, and movement of personal data
  - EU Internet Privacy Law of 2002 (Directive 2002/58/EC)
    - Protects data in electronic transactions
  - Individual countries have their own laws

Compliance: Regulatory Framework

- **Laws Govern**
  - What information can be collected
  - How it must be stored and secured
  - Under what circumstances it can be shared
  - Under what circumstances it can be disclosed
  - Requirements for responding to data breaches and data losses
  - Penalties for data breaches and data losses

Compliance: Regulatory Framework

- **Increasingly, organizations must comply with multiple requirements**
  - Software vendors moving into healthcare
  - Banks that have direct access to PHI are business associates under HIPAA *(EFT interim final rules as into effect on Jan. 1, 2014)*
  - Healthcare organizations that process payments subject to PCI, HIPAA, § 5 of the FTC Act, State Laws (SSN nos, drivers licenses, etc.)

Results of Non-Compliance

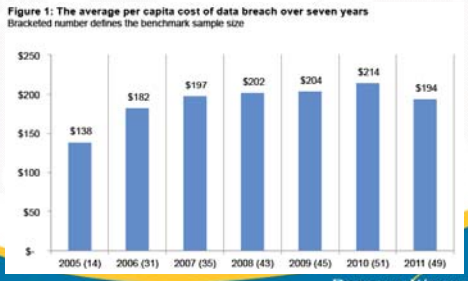
- **Class Actions**
  - **Sony** (April/May 2011)
    - Gaming network infiltrated
      - Problems began after it sued George Hotz
      - Appears that "Anonymous" was not pleased and began a DoS
      - Hacker(s) took advantage; entered system and stole data (Anonymous has denied responsibility for breach)
    - More than 100 million users affected
      - Stolen names, passwords, birth dates, and maybe credit cards
    - Cost of repair? As of May, up to $171 million *(ZDNet)*

Results of Non-Compliance

- **Data Breaches**
  - Costly to address:
    - employee overtime and productivity loss
    - investigation costs (internal and external – OCR, FTC, State AGs)
    - data breach notices
    - credit monitoring services
    - State and Federal reporting requirements
    - State and Federal fines and investigation settlement costs
    - lawsuits

Results of Non-Compliance

- **Ponemon Institute: 2011 Cost of Data Breach Study**



Results of Non-Compliance

- **Class Actions**
  - Healthcare industry hit with a string of data breach class actions
    - California
      - Sutter Health (13 as of Feb. 2012)
      - UCLA Health System
      - Health Net / IBM (as BAA)
    - Michigan – Henry Ford Health System

Results of Non-Compliance

- **Class Actions**
  - Many class actions dismissed on the basis of lack of standing and/or for failure to state a claim (e.g., Starbucks, LinkedIn, etc.)
  - BUT – **Costly to defend**!

Results of Non-Compliance

- **Federal Trade Commission**
  - Section 5
  - Actions against – Google, Facebook, Microsoft, Eli Lilly, etc.
  - In June, FTC sued Wyndham Hotels and 3 of its subs.
    - **Attackers breached network 3 times in 2 yrs using similar methods** → exposure of 600,000+ credit card accounts and $10.6 million in fraudulent credit card charges
    - *Failure to institute a robust information security program*
    - *"Unfair and deceptive"* practices – based on claims made in the privacy policy

Results of Non-Compliance

- **State Attorneys' General**
  - State Laws
  - Actions against - HP, Lifetime Fitness, Facebook, etc.
  - Under HITECH, AGs can pursue healthcare related data breaches
    - Actions against covered entities - Connecticut, Massachusetts, Indiana, and Vermont
    - Minnesota AG first to take action against business associate - Accretive Health (debt collection company)

Results of Non-Compliance

- **Office of the Civil Rights (HHS)**
  - HIPAA/HITECH
  - OCR has taken action against:
    - a large insurance company (Blue Cross Blue Shield of Tennessee settled for $1.5M)
    - a clinic provider (Cignet Health Fined $4.3M)
    - a state agency (Alaska Department of Health and Human Services settled for $1.7M)
    - a large hospital system (UCLA Health System settled for $865K)
    - a physician's practice (Phoenix Cardiac Surgery settled for $100K)

Results of Non-Compliance

- **Impact on Business**
  - Your customers don't trust you anymore…

Outline

- Part 1: Introduction
  - Two Questions
  - A Story
- Part 2: Compliance
  - Regulatory Framework
  - Results of Non-Compliance
- **Part 3: What's a Company to do?**

What's a Company to do?

- Get insurance
  - Breaches happen - this is part of living with IT
  - Insurance can defray many costs
- Take on only the liability that is necessary
  - Review contracts carefully and make sure risk apportioned appropriately
- Live up to advertised promises
  - Privacy policies are a contract with consumers and enforced by the FTC

What's a Company to do?

- Look to standards organizations for best practices
  - NIST guidance materials
- Plan ahead
  - Costs can be defrayed by planning ahead
  - Risk assessment
  - Thoughtful policies and procedures

What's a Company to do?

- Training and Awareness
  - Training staff will minimize risks of internal breaches
  - Rogue employee defense
- Enforce Policies and Procedures
- Audit for Compliance and Review Policies and Procedures

This slide presentation is informational only and was prepared to summarize relevant legal consideration when formulating a social media policy. It does not constitute legal or professional advice.

You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation, and Dickinson Wright would be pleased to assist you on these matters.