



# Hot Topics in Privacy & Security Law

Presented by Robert J. Scott  
Managing Partner Scott & Scott, LLP

[www.ScottandScottllp.com](http://www.ScottandScottllp.com)

## Overview

### Federal and State Statutory and Regulatory Issues

- HIPAA Privacy and Security Rules – 2009 Recovery Act extends HIPAA reach to business associates
- GLBA Safeguards Rules
- Data breach notification laws
- Data protection and destruction laws

### Civil Liability

- Unfair Trade Practice Claims
- Negligence
- Breach of Contract
- Unlawful Trade Practices

### Claim Scenarios

- TJX
- Radio Shack
- BJ's Wholesale Club
- Choice Point
- DSW
- Heartland
- Hannaford Bros

# State Data Breach Notification Laws

## State Data Breach Notification Laws

State	Time To Notify Consumers of a Breach of Personal Information	Civil or Criminal Penalties for Failure to Promptly Notify Customers of Breach	Private Right of Action	Exemption for Encrypted Personal Info	Exemption for Criminal Investigations or Information Publicly Available from Government Entities	Exemption for Immaterial Breaches
Arizona	Most expedient time possible, without unreasonable delay	•		•	•	
Arkansas	Most expedient time possible, without unreasonable delay	•		•	•	•
California	Most expedient time possible, without unreasonable delay		•	•	•	
Colorado	Most expedient time possible, without unreasonable delay	•		•	•	•
Connecticut	Immediately			•	•	•
Delaware	Immediately, in the most expedient time possible, without unreasonable delay	•	•	•	•	
District of Columbia	Most expedient time possible, without unreasonable delay	•	•		•	
Florida	Without unreasonable delay	•		•	•	
Georgia	Most expedient time possible, without unreasonable delay			•	•	
Hawaii	Without unreasonable delay	•	•	•	•	
Idaho	Most expedient time possible, without unreasonable delay	•		•	•	•



## Network Security and Privacy Injury Claims

- FTC Investigations
- State Investigations
- Privacy Causes of Action
- Mitigation Strategies

## State Investigations

- State Consumer Protection Laws
- Breach Notification Violations
- Violations for Failure to Protect and Properly Destroy Customer Data

## Private Causes of Action

- Breach of Contract Claims
- Third-Party Beneficiary Claims
- Contractual and Non-Contractual Indemnity Claims
- Tort / Negligence Claims
- Failure to Maintain Adequate Security
- Negligent Retention of Data
- Negligent Misrepresentation Regarding Breaches in Security

## Contact Information

**Robert J. Scott, Esq.**

Managing Partner

Scott & Scott, LLP.

1256 Main Street, Suite 200

Southlake, TX 76092

**Phone:** (800) 596-6176

**Fax:** (800) 529-3292

**E-Mail:** [rjscott@scottandscottllp.com](mailto:rjscott@scottandscottllp.com)

# HOT TOPICS IN PRIVACY AND SECURITY LAW



Rachel Simon  
Regional Underwriting Manager  
Dallas & Houston Regions

*April 7, 2010*

**CHARTIS** 



# Key Areas of Exposure

## Financial Account Information

- Credit card data
- Bank account and PIN information

## Protected Healthcare Information

- Benefit Information
- Employee Health Information

## Personally Identifiable Information (PII) of *Customers, Constituents, Clients, Employees*

- Social Security Numbers
- Drivers License Information
- Addresses
- Medical Records

## Confidential Corporate Information

## Public Infrastructure

# Network and Privacy Threats

- Unauthorized Access/Unauthorized Use
- Virus/Malicious Code
- Theft or Destruction of Confidential Corporate Information
- Theft or Exposure of Personal Identifying Information
- Theft or Exposure of Protected Health Information
- Cyber Extortion

# Data Breach and ID Theft Impacts

- Bad press/Reputational damage
- Unbudgeted expenses
- Dissatisfied customers and employees
- Loss of customers/employees
- Regulatory investigations
- Lawsuits
- Lost Business/Revenue
- Damage to Balance Sheet

# Exposure Trends...

- **285 Million** records were breached in 2008, which is more than the previous four years combined
- **87%** of breaches were considered avoidable through simple or intermediate controls
- **67%** of breaches were aided by significant error
- **91%** of all compromised records were linked to organized crime

***"It's impossible to create an environment where you cannot have a data breach."***

- Larry Ponemon of the Ponemon Institute

- 2009 institute findings:
  - The average cost of a breach: \$6.75M dollars, up from 2008 and 2007
  - The average per record cost of a data breach is \$204, up from 2008 and 2007
  - Errors of Third Parties (information holders) make up 42% of all breaches

# Risk Management Questions

- Do **You** have physical and system access controls in place?
- Do **You** have documented procedures for firewall, intrusion prevention, anti-virus, patch management?
- Do **You** have encryption tools to ensure integrity and confidentiality of sensitive data including data on removable media?
- Do **You** have a program in place to periodically test security controls?
- Does **Your** hiring process include the following: criminal, credit, references, drug screening?

# Risk Management Questions

- Do **You** implement policies and procedures to ensure compliance with legislative, regulatory and/or contractual privacy requirements that govern your industry?
- Have **You** assigned the responsibility for Information Security & Privacy to a senior manager?
- Do **You** have an entity-wide Information Security & Privacy Policy and an Information Security Incident Response Plan in place?

# Risk Management Questions

- Do **Your** contracts require defense and indemnification?
- Do **Your** contracts require vendors to maintain adequate security of information?
- Do **You** require vendors to maintain security and privacy insurance?



# What Coverage is Available?

**Traditional insurance products do not respond:**

(GL, property, crime, D&O, E&O)

**Security and privacy coverage (sometimes called cyber liability) responds to:**

- Failures of Network Security
- Privacy Events
- 3<sup>rd</sup> and 1st Party losses should be covered

# Security & Privacy Liability Coverage

## Policy responds to security failures and privacy events

- Computer attack against an **insured**
- Wrongful disclosure or breach of private or confidential data, including corporate data
  - Security and Privacy Liability (3<sup>rd</sup> party)
  - Event Management (1<sup>st</sup> party)
  - Information Asset (1<sup>st</sup> party)
  - Network Interruption (1<sup>st</sup> party)
  - Cyber Extortion (1<sup>st</sup> party)

# Insurance Considerations

- Limits and retentions
  - Entity size
  - Industry
  - Risk appetite
- Comparing policy language
- Comparing carrier advantages
  - Professional experience: underwriters, claims staff, defense counsel
- Securing choice of counsel

# Questions



# CHARTIS

## Your world, insured

Chartis is the marketing name for the worldwide property-casualty and general insurance operations of Chartis Inc. For additional information, please visit our website at [www.chartisinsurance.com](http://www.chartisinsurance.com). All products are written by insurance company subsidiaries or affiliates of Chartis Inc. Coverage may not be available in all jurisdictions and is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain coverage may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.

The data contained in this presentation are for general informational purposes only. The advice of a professional insurance broker and counsel should always be obtained before purchasing any insurance product or service. The information contained herein has been compiled from sources believed to be reliable. No warranty, guarantee, or representation, either expressed or implied, is made as to the correctness or sufficiency of any representation contained herein.

The claim scenarios summarized herein are offered only as examples. Coverage depends on the actual facts of each case and the terms, conditions and exclusions of each individual policy. Anyone interested in the above product(s) should request a copy of the policy itself for a description of the scope and limitations of coverage. Chartis is the marketing name for the worldwide property-casualty and general insurance operations of Chartis Inc. All products are written by insurance company subsidiaries or affiliates of Chartis Inc. Coverage may not be available in all jurisdictions and is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain coverage may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds and insureds are therefore not protected by such funds.