Legal Responsibilities for a Data Breach

Melissa K. Ventrone, Thompson Coburn

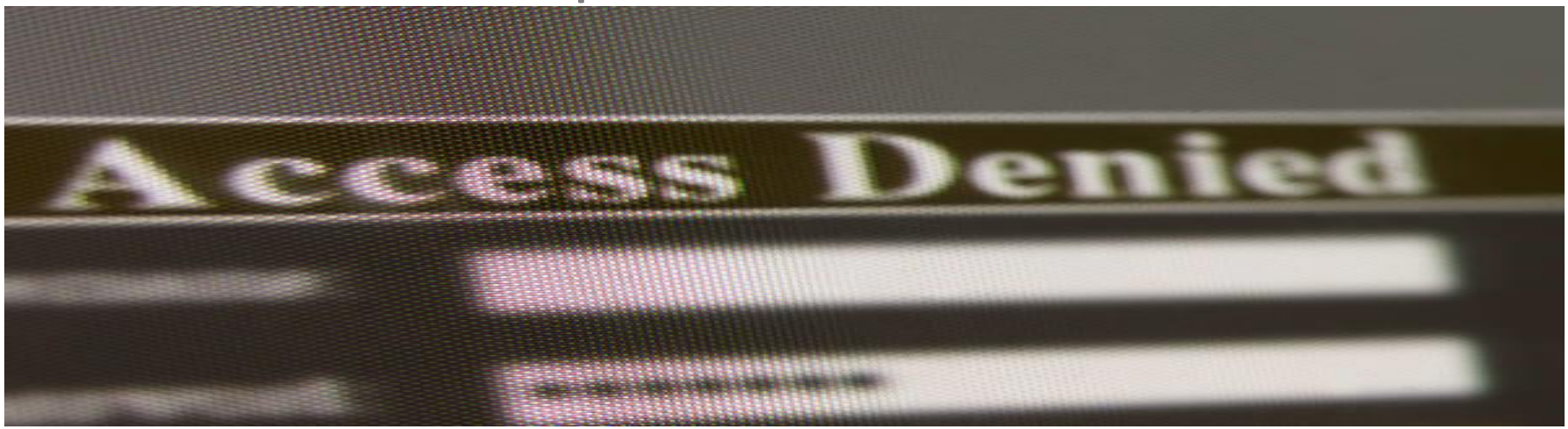
August 18, 2016

THOMPSON COBURN LLP

Welcome and Introduction

Overview

- What is a Data Breach?
- What Triggers Reporting Requirements?
- Federal Data Breach Laws
- Contractual Requirements



Key Definitions

- PII – personally identifiable information
- PHI – protected health information
- ePHI – electronic protected health information
- HPHI– highly protected health information

What is a Data Breach?

- Generally defined as:
  - Unauthorized access or acquisition of certain protected information
  - How do you know whether there is unauthorized access or acquisition of protected information?
- Some agencies:
  - Require notice to the agency if there is a breach of the system

What is Protected Information

- Attorney's favorite answer:
  - It depends….so call me!
- Definitions by law – incredibly complex when not involving "traditional" data elements
- Contracts may define protected information
  - Privacy policies and privacy notices
  - Business-to-business

Deeper Dive into PII/PHI

THOMPSON COBURN LLP

- It depends:
  - Many statutes require name in combination with:
    - SSN, driver's license or state identification number, financial account information, information that provides access to online account, credit card information with the security code
  - But the statutes vary:
    - Notification required if username and password

What Triggers Notification?

- First, determine to whom notification is required:
  - By statute: the individual and/or regulatory agency
  - By industry regulation: a specific industry agency
  - By contract: to business partners, or vendors, or the credit card brands
- Second, determine when notification is required
  - Most statutes require notification when there is a breach (unauthorized access or acquisition) of PII or PHI

What Triggers Notification?

- Legal requirements
- Industry requirements:
  - Defense Federal Acquisition Regulations
  - North American Electric Reliability Corporation
  - Federal Energy Regulatory Commission
- Contractual requirements

What Else?

- Credit monitoring/identity restoration
  - Which states require it?
  - Identity mitigation services – what is this?
- What steps have you taken to prevent a similar incident in the future?

Regulatory Scrutiny and Litigation – The "Do Nots"

- Do not ignore cybersecurity preparedness
- Do not ignore signs or warnings of a data breach
- Do not ignore questions from regulators
- Do not over-notify

Important Statistics

THOMPSON COBURN LLP

- Cost of a data breach is approximately $4 million per incident, a 29% increase since 2013 and 5% increase since 2015.
- Average length of time before a data breach is discovered is 201 days, with organizations requiring another 70 days to contain breaches once they'd been identified.
- Average cost per record: $158
- Being prepared can reduce this figure by $16 per record
  - For 100,000 records, savings equals $1,600,000

THOMPSON COBURN LLP

QUESTIONS?

Contact Information

Melissa K. Ventrone
Partner, chair Data Privacy and Security
Thompson Coburn
55 E Monroe Suite 3700
Chicago, IL 60603
mventrone@thompsoncoburn.com
O: 312.558.2219
M: 312.485.0540