Fourth Annual Connecticut Privacy Forum
Hartford, Connecticut

Office of Consumer Affairs & Business Regulation

Massachusetts Office of Consumer Affairs and Business Regulation And Data Security Law

Barbara Anthony
Undersecretary of Consumer Affairs and Business Regulation
Commonwealth of Massachusetts

Better businesses. Smarter consumers.

October 3, 2012

Office of Consumer Affairs & Business Regulation

This Presentation Covers:

- The Notification Requirement
- Defining “Personal Information”
- The Regulation: An Overview
- Required Safeguards
- How to Safeguard
- Recent Actions
- Top 10 Issues in Data Security Law

Office of Consumer Affairs & Business Regulation

Massachusetts Data Security Law

Data Breach Notifications Law

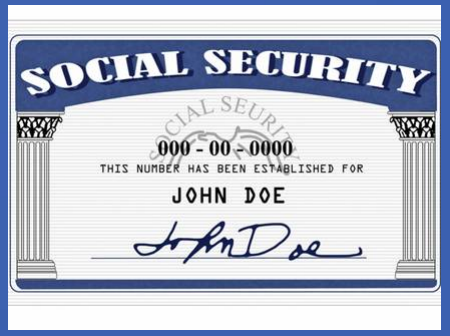
Data Security Regulations

Better businesses. Smarter consumers.

Office of Consumer Affairs & Business Regulation

The Massachusetts Notification Law

- M.G.L. c. 93H § 3
- A person who owns or licenses a resident's personal information (PI) must notify:
  - The resident affected
  - The Attorney General
  - OCABR



- When the person knows or has reason to know of
  - A security breach or
  - An unauthorized use

Office of Consumer Affairs & Business Regulation

The Massachusetts Notification Law

- The notice to the MA state offices must include
  - nature of the breach
  - number of residents affected
  - steps taken or to be taken in response
- The notice to the MA resident must include
  - information about the right to obtain a police report
  - how to request a security freeze
  - fees to be paid to a consumer reporting agency
  - *NO* information about the nature of the breach
  - *NO* information about the number of residents impacted.

Defining "Personal Information"

Last Name, First Name or Initial

PLUS

1.		2.		3.
Social Security Number	**OR**	Driver's license (or state-issued ID)	**OR**	Financial account or credit/debit card number (with or without pin)

Note: PI Includes Employee Information

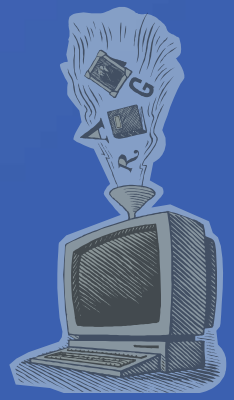
Office of Consumer Affairs & Business Regulation

The Regulation: An Overview

- The regulation applies to
  - Entities that own or license PI
- What is covered
  - A MA resident's PI
- It requires encryption of PI that is
  - Transmitted over public networks
  - Transmitted wirelessly
  - On laptops & portable devices

Required Safeguards

All organizations must have a Written Information Security Program (WISP)



The WISP must contain

- Evaluation of reasonably foreseeable risks to PI
- Evaluation of current safeguards
- Employee training and compliance
- Policies/procedures for storage, access, and transportation
- Documentation of responses to a security breach

Third-Party Service Providers

- Due Diligence
  - Select a service provider capable of protecting PI
- Contract Requirements
  - Require, by contract, that the service provider implement and maintain data security protections
  - Grace period for contracts signed before March 1, 2010 expired March 1, 2012

How to Safeguard PI

System Security Methods

- Control Access
- Encrypt
- Monitor

Office of Consumer Affairs & Business Regulation

Data Security Enforcement in Mass.

The Attorney General

- Applicable Authority
  - M.G.L. c. 93H § 6
  - M.G.L. c. 93A § 4
- MGL Ch. 93A § 4 allows for
  - Injunctive relief
  - Restitution
  - Civil penalties up to $5,000 for each violation
  - Investigation costs and attorneys' fees