



The Massachusetts Data Security Law

- ◆ Effective March 1, 2010
- ◆ Requires notification and reporting of security breaches of personal info
- ◆ Definition of personal info: Last name and first name (or last name and first initial) **AND** one of the following:
 - SS number
 - Driver's license number or state-issued ID number
 - Financial account info (debit/credit card number)
- ◆ Notification required to the individual(s) and the Attorney General's office and the Office of Consumer Affairs and Business Regulation (notice may be written or electronic)
- ◆ Companies must dispose of such records properly and permanently
- ◆ Requires a "Comprehensive Information Security Program" (CISP)
 - Mandatory and must be written
 - Addresses safeguards
 - Designed to ensure safekeeping and confidentiality of records
 - Must discuss minimum requirements
 - Must be appropriate for your business
 - Must assess paper, electronic and other records
 - Must develop security procedures and identify person in charge
 - Must have a monitoring/maintenance program
 - Must have process for responding to breaches
 - Must have a training component
 - Must discuss access, amount of personal info collected and disciplinary action for employees that violate policy
 - Must take steps to retain third parties who meet regs
 - Must reference 3/1/12 as the date that third parties must comply (as part of contracts)
 - Must have a "Computer System Security Requirements" (CSSR) – which includes user authentication protocols, limiting access, use of passwords, encryption, monitoring and employee education as well as physical safeguards

Penalties – enforced by AG who can enforce civil penalties of up to \$5K for each violation (under Chapter 93H) and \$100 per data subject, up to a max of \$50K (under Chapter 93I)