

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

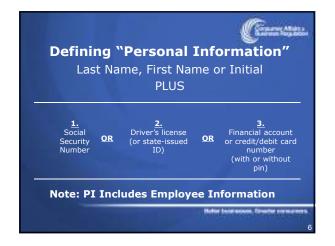


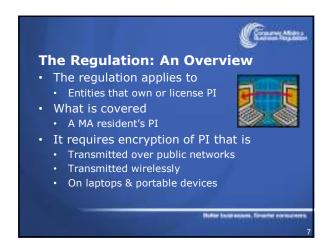
The Massachusetts Notification Law M.G.L. c. 93H § 3 A person who owns or licenses a resident's personal information (PI) must notify: The resident affected The Attorney General OCABR When the person knows or has reason to know of: A security breach or An unauthorized use

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

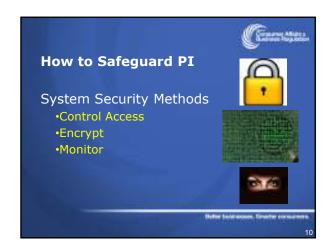
The notice to the MA resident must include
information about the right to obtain a police report
how to request a security freeze
fees to be paid to a consumer reporting agency
NO information about the nature of the breach
NO information about the number of residents impacted.

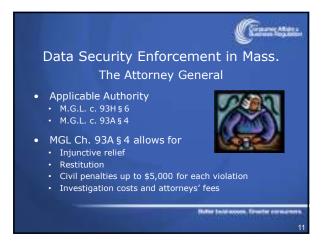


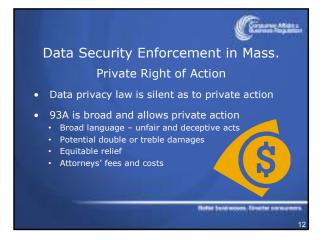












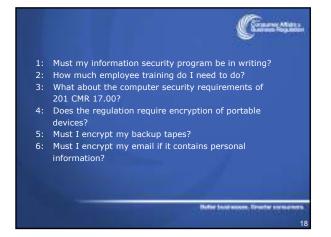
MA Actions Under Data Security Law • Briar Group LLC - 125,000 credit card #s • \$110K penalty • Belmont Savings Bank - 13,000 bank account #s • \$7,500 penalty • Maloney Properties - 600 customer SS #s • \$15,000 penalty • South Shore Hospital - 800,000 patients' data • \$750,000 penalty

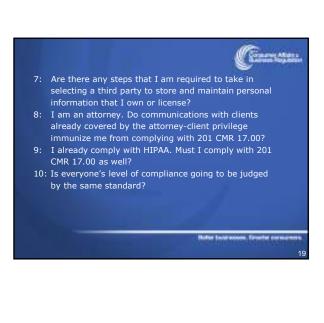




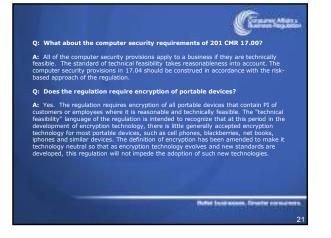
Industry Response from Letters • Encryption • Encrypting data not previously encrypted • Even data "at rest" (not required) – South Shore Hospital • Training • Instituting or strengthening existing training programs • Many are instituting "reminder" trainings • Videos, newletters, continuing education courses • Limit accessibility • Many companies are changing passwords and restricting access to personal information to employees that need it











Companie.	
Q: Must I encrypt my backup tapes?	
A: You must encrypt backup tapes on a prospective basis. However, if you are going	
to transport a backup tape from current storage, and it is technically feasible to encrypt (i.e. the tape allows it) then you must do so prior to the transfer. If it is not technically	
feasible, then you should consider the sensitivity of the information, the amount of personal information and the distance to be traveled and take appropriate steps to secure and safeguard the personal information. For example, if you are transporting a	
large volume of sensitive personal information, you may want to consider using an armored vehicle with an appropriate number of guards.	
Q: Must I encrypt my email if it contains personal information?	
A: If it is not technically feasible to do so, then no. However, you should implement	
best practices by not sending unencrypted personal information in an email. There are alternative methods to communicate personal information other through email, such as establishing a secure website that requires safeguards such as a username and	
password to conduct transactions involving personal information.	
Puter have soon. Erecter communes.	
22	
(Figures Abbas)	
	-
Q: Are there any steps that I am required to take in selecting a third party to store and maintain personal information that I own or license?	
A: You are responsible for the selection and retention of a third-party service provider who is capable of properly safeguarding personal information. The third party	
service provider provision in 201 CMR 17.00 is modeled after the third party vendor provision in the TC's Safeguards Rule.	
Q: I am an attorney. Do communications with clients already covered by the	
attorney-client privilege immunize me from complying with 201 CMR 17.00?	
A: If you own or license personal information, you must comply with 201 CMR 17.00 regardless of privileged or confidential communications. You must take steps outlined	
in 201 CMR 17:00 to protect the personal information taking into account your size, scope, resources, and need for security.	
Before land more a familie and married	
23	
(County Atlant)	
Section 1	
Q: I already comply with HIPAA. Must I comply with 201 CMR 17.00 as well?	
A: Yes. If you own or license personal information about a resident of the	
Commonwealth, you must comply with 201 CMR 17.00, even if you already comply with HIPAA.	
Q: Is everyone's level of compliance going to be judged by the same standard?	
A: Both the statute and the regulations specify that security programs	
A: Both the statute and the regulations specify that security programs should take into account the size and scope of your business, the resources that you have available to you, the amount of data you store, and the need	
for confidentiality. This will be judged on a case by case basis.	
Hefre Involvement Terretor on marriers	
24	

Constitu
QUESTIONS?
Natur Instruction, Structur consumers.
25