Bloomberg Law

Domestic Privacy Profiles

# Massachusetts

*Seth P. Berman and Charles F. Pierre*
*Nutter McClennen & Fish LLP*

# Massachusetts

***Seth P. Berman*** *and* ***Charles F. Pierre****, of Nutter McClennen & Fish LLP, Boston, provided expert review of the Massachusetts Profile and wrote the Risk Environment section, with the assistance of summer associate Maya Ginga.*

## I. APPLICABLE LAWS AND REGULATIONS

### A. Constitutional Provisions –

There are no constitutional provisions in Massachusetts conferring a general right of privacy on Massachusetts residents.

### B. Personal Data Protection Provisions –

Under Massachusetts law, persons have the general right against unreasonable, substantial, or serious interference with their privacy. The superior court has equity jurisdiction to enforce this right and to award damages accordingly (**Mass. Gen. Laws ch. 214, § 1B**). In addition, Massachusetts has a wide variety of laws governing privacy and data security, primary among them the Commonwealth's data breach notification law (**Mass. Gen. Laws ch. 93H, § 1** through **Mass. Gen. Laws ch. 93H, § 6**). The data breach law is outlined below and discussed in detail at **Section I.C.8.**

There are additional privacy laws and regulations in Massachusetts, including regulations governing data security (see **Section I.C.6.**), laws on data disposal (see **Section I.C.7.**), laws governing eavesdropping and electronic surveillance (see **Section I.F.**), do-not-call laws (see **Section I.E.1.**), and security freeze provisions (see **Section I.D.4.**). Finally, laws related to privacy and data security applicable to specific sectors, such as health care and insurance, are set forth in the portions of this profile dedicated to those sectors.

#### 1. Who is covered? –

The data breach notification requirements apply to any Massachusetts resident whose information was acquired or used by an unauthorized person or used for an unauthorized person (**Mass. Gen. Laws ch. 93H, § 3(b)**).

#### 2. What is covered? –

The data breach notification law requires any person or agency that owns or licenses data that includes personal information about a Massachusetts resident to notify the Office of the Attorney General, the Director of the Office of Consumer Affairs and Business Regulation, and the resident of any breach in accordance with the provisions of the law (**Mass. Gen. Laws ch. 93H, § 3(b)**). In addition, a person or agency who maintains, but does not own or license, data that includes personal information must notify the owner or licensor of the data of any breach in accordance with the law (**Mass. Gen. Laws ch. 93H, § 3(a)**). For details on the general data breach notification requirements, see **Section I.C.8.**

#### 3. Who must comply? –

The data breach notification law applies to any person or agency that owns or licenses personal information or that maintains or stores, but does not own, personal information (**Mass. Gen. Laws ch. 93H, § 3(a)** and (b)). "Person" means a natural person, corporation, association, partnership, or other legal entity, while "agency" is any agency, executive office, department, board, commission, bureau, division, or authority of the Commonwealth, any of its branches, or any political subdivision (**Mass. Gen. Laws ch. 93H, § 1(a)**).

### C. Data Management Provisions

#### 1. Notice & Consent –

***Electronic surveillance:*** In general, electronic surveillance requires the consent of all parties to a wire or oral communication (see **Section I.F.**).

***Right of publicity:*** A person whose name, portrait, or picture is used for advertising or trade purposes without the person's written consent may bring an action for injunctive relief and damages (see **Section I.E.1.**).

 

***Data breach notification:*** For information on notice requirements under the Commonwealth's data breach notification law, see **Section I.C.8.**

***Insurance and health provisions:*** Provisions of Massachusetts law governing insurance information and privacy protection applicable to personal information maintained by insurers in Massachusetts contain specific notice and consent provisions (see **Section I.E.7.**). In addition, provisions of Massachusetts law governing specific types of health care facilities and providers and health data contain requirements regarding notice and consent relative to such data (see **Section I.D.9.**).

**2. Collection & Use** –

***Right of publicity:*** A person whose name, portrait, or picture is used for advertising or trade purposes without the person's written consent may bring an action for injunctive relief and damages (see **Section I.E.1.**).

***Insurance and health provisions:*** Provisions of Massachusetts law governing insurance information and privacy protection applicable to personal information maintained by insurers in Massachusetts contain specific collection and use requirements (see **Section I.E.7.**). In addition, provisions of Massachusetts law governing specific types of health care facilities and providers and health data contain requirements regarding collection and use of such data (see **Section I.D.9.**).

***Student records:*** Massachusetts regulations govern the collection of data contained in a student record (see **Section I.E.2.**).

**3. Disclosure to Third Parties** –

***Data breach notification:*** For information on requirements under the data breach notification law regarding the unauthorized access to or use of personal information by a third party, see **Section I.C.8.**

***Insurance and health provisions:*** Provisions of Massachusetts law governing insurance information and privacy protection applicable to personal information maintained by insurers in Massachusetts contain specific requirements regarding disclosures to third parties (see **Section I.E.7.**). In addition, provisions of Massachusetts law governing specific types of health care facilities and providers and health data contain requirements regarding third-party disclosures (see **Section I.D.9.**).

**4. Data Storage** –

Under Massachusetts regulations governing the duty to protect and the standards for protecting personal information, any person that owns or licenses personal information about a Massachusetts resident must develop a comprehensive information security program that contains a number of elements, including a specific requirement to develop security policies for employees relating to the storage, access, and transportation of records containing personal information outside of business premises (**201 CMR 17.03(2)(c)**), as well as including reasonable restrictions on physical access to records containing personal information and storage of such records in locked facilities, storage areas, or containers (**201 CMR 17.03(2)(g)**). For a comprehensive discussion of the data security regulations, see **Section I.C.6.**

**5. Access & Correction** –

***Insurance and health provisions:*** Provisions of Massachusetts law governing insurance information and privacy protection applicable to personal information maintained by insurers in Massachusetts contain specific requirements regarding access to and correction of such data (see **Section I.E.7.**). In addition, provisions of Massachusetts law governing specific types of health care facilities and providers and health data contain requirements regarding access and correction (see **Section I.D.9.**).

***Student records:*** Massachusetts regulations govern access to and correction of data contained in a student record (see **Section I.E.2.**).

***Credit reports:*** Specific laws govern the correction of inaccurate or incomplete information in a credit report (see **Section I.D.4.**).

**6. Data Security** –

***Regulations on security standards for personal information:*** The Massachusetts data breach notification law contains a provision requiring the Office of Consumer Affairs and Business Regulation (OCABR) to adopt regulations relative to any person that owns or licenses personal information about Massachusetts residents that are designed to safeguard such information and are consistent with any federal regulation applicable to such persons (**Mass. Gen. Laws ch. 93H, § 2(a)**). The OCABR has promulgated these regulations (**201 CMR 17.01** to **201 CMR 17.05**; hereinafter the "Data Security Regulations"), which are outlined in detail below.

*Purpose and scope:* The Data Security Regulations establish minimum standards applicable to safeguarding personal information in both paper and electronic records and are designed to ensure the security and confidentiality of customer information consistent with industry standards. The regulations apply to all persons that own or license personal information about Massachusetts residents (**201 CMR 17.01**). "Person" is defined to include a natural person, corporation, association, partnership, or other legal entity other than an agency, executive office, department, board, commission, bureau, division, or authority of the Commonwealth or any of its political subdivisions (**201 CMR 17.02**, fifth paragraph).

*Duty to protect and protection standards:* Every person owning or licensing personal information about a Massachusetts resident must develop, implement, and maintain a comprehensive information security program that is written in one or more accessible parts and contains administrative, technical, and physical safeguards appropriate to the following:

- the size, scope, and type of business of the person;
- the amount of resources available to the person;
- the amount of stored data; and
- the need for security and confidentiality of both consumer and employee information (**201 CMR 17.03(1)**).

The program must include, at a minimum, the following elements:

- designating one or more employees to maintain the program;
- identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of any paper or electronic records, and improving the effectiveness of current safeguards, including ongoing training, employee compliance, and detection and prevention of security system failures;
- developing security policies for storage, access, and transportation of records outside business premises;
- imposing disciplinary measures for violations of the program;
- preventing terminated employees from accessing records containing personal information;
- overseeing any service providers by ensuring their ability to maintain appropriate security measures and requiring them to implement such measures;
- placing reasonable restrictions on physical access to records, and storing them in locked facilities, storage areas, or containers;
- regular monitoring of the security program to ensure that it is operating in the proper manner;
- annual review of security measures, or after a material change in business practices; and
- documenting responses to any incident involving a security breach, and post-incident review (**201 CMR 17.03(2)**).

*Computer system security requirements:* Every person who owns or licenses personal information about a Massachusetts resident and electronically stores or transmits the information must include in its comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that must, at a minimum and where technically feasible, include the following:

- secure user authentication protocols, including control of user IDs, secure methods of assigning and selecting passwords, or use of unique identifiers (i.e., biometrics or tokens);

• secure access control measures that restrict access to necessary personnel and assign unique IDs and passwords reasonably designed to maintain the integrity of security;

• encryption of all transmitted records and files travelling across public networks, and encryption of all data transmitted wirelessly;

• reasonable system monitoring;

• encryption of all personal data stored on laptops or other portable devices;

• up-to-date firewall protection and operating system patches for files stored on an Internet-based system;

• up-to-date versions of system security agent software, including malware protection; and

• education and training of employees on the proper use of the computer security system (**201 CMR 17.04**).

***Additional regulations applicable to state agencies:*** Specific regulations govern the collection, maintenance, and disclosure of personal data contained in manual or computerized personal data systems that are applicable to the State Secretary's Office and all agencies therein in the context of the Commonwealth's Fair Information Practices Act (**Mass. Gen. Laws ch. 66A, § 3**). These regulations cover topics such as physical security, permitted and prohibited disclosures under the Public Records Act, and rights of access, among other topics (**950 CMR 33.00**to **950 CMR 33.32**).

Regulations of the Executive Office of Administration and Finance set forth additional privacy and security requirements applicable to the Commonwealth's executive offices and their agencies, including requiring each agency to designate an information officer and establishing collection, disclosure, and access rules (**801 CMR 3.00** to **801 CMR 3.06**).

The Attorney General has promulgated regulations setting requirements that the office must meet with respect to the safeguarding of personal information, including a written information security program and computer system security requirements (**940 CMR 27.00** to **940 CMR 27.04**).

School principals or their designees are responsible for the privacy and security of student records maintained at their school (**603 CMR 23.05**). For more information on these requirements, see **Section I.E.2.**

**7. Data Disposal** –

Agencies and persons are subject to specific requirements regarding the disposition and destruction of records containing personal information of Massachusetts residents. For purposes of these requirements, an "agency" is any county, city, town, or constitutional office or any agency thereof, including departments, divisions, bureaus, boards, commissions, or committees (**Mass. Gen. Laws ch. 93I, § 1**, first paragraph), while a "person" includes natural persons, corporations, associations, partnerships, or other legal entities (**Mass. Gen. Laws ch. 93I, § 1**, third paragraph). Covered personal information includes a resident's first name and last name or first initial and last name in combination with one or more of the following:

• social security number;

• driver's license or state ID number;

• financial account number or credit or debit card number, with or without any required security code, access code, personal ID number, or password permitting access to a resident's financial account; or

• biometric identifier (**Mass. Gen. Laws ch. 93I, § 1**, fourth paragraph).

When disposing of records, any agency or person must meet minimum standards for proper disposal of records containing personal information, including redacting, burning, pulverizing, or shredding paper documents so that personal data cannot be practicably read or reconstructed, and destruction or erasure of electronic and other non-paper media so that personal data cannot be practicably read or reconstructed. Agencies or persons may contract with third parties to dispose of personal information, but such third parties must dispose of the information in accordance with the law's requirements and must implement and monitor compliance with policies and procedures that prohibit unauthorized access to or acquisition of personal information during the collection, transportation, or disposal of such information (**Mass. Gen. Laws ch. 93I, § 2**, first and second paragraphs).

Civil fines may be imposed for violations, along with other remedies (see **Section II.C.**).

Specific provisions apply to the destruction of school records (see **Section I.E.2.**).

**8. Data Breach** –

Massachusetts has a data breach notification law applicable to required notifications by natural persons, businesses, and government agencies (**Mass. Gen. Laws ch. 93H, § 1** through **Mass. Gen. Laws ch. 93H, § 6**). The provisions are outlined in detail below.

***Primary definitions:*** A "breach of security" is the unauthorized acquisition or unauthorized use of unencrypted data, or encrypted data if the data is accompanied by the confidential process or key capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a Massachusetts resident. Good faith but unauthorized acquisition of such data by an employee or agent of the individual or entity for the purposes of the individual or entity does not constitute a breach of system security unless the information is used in an unauthorized manner or subject to further unauthorized disclosure (**Mass. Gen. Laws ch. 93H, § 1(a)**, second paragraph).

A "person" means a natural person, corporation, association, partnership, or other legal entity (**Mass. Gen. Laws ch. 93H, § 1(a)**, seventh paragraph), while "agency" is any agency, executive office, department, board, commission, bureau, division, or authority of the Commonwealth, any of its branches, or any political subdivision (**Mass. Gen. Laws ch. 93H, § 1(a)**, first paragraph).

"Personal information" is the first name and last name or first initial and last name in combination with any of the following data elements that relate to a Massachusetts resident:

• social security number;

• driver's license number or state ID card number; or

• financial account number or credit or debit card number, with or without any required security code, access code, or password allowing access to a resident's financial accounts.

The term does not include information obtained from publicly available information or from publicly available federal, state, or local government records (**Mass. Gen. Laws ch. 93H, § 1(a)**, eighth paragraph).

***Notification requirement:*** A person or agency that owns or licenses data that includes personal information about a Massachusetts resident must provide notice as soon as practicable and without unreasonable delay when the person or agency knows or has reason to know of a breach of security or when the person or agency knows or has reason to know that the personal information was acquired or used by an unauthorized person or used for an unauthorized purpose. The notice must be provided to the Attorney General, the Director of the Office of Consumer Affairs and Business Regulation (OCABR), and the resident (**Mass. Gen. Laws ch. 93H, § 3(b)**). A person or agency that maintains or stores, but does not own or license, data that includes personal information must notify the owner or licensor of the data of any breach in the security of the system as soon as practicable and without unreasonable delay upon discovery and must cooperate with the owner or licensor, including informing the owner or licensor of specified information concerning the breach (**Mass. Gen. Laws ch. 93H, § 3(a)**).

Notice may be delayed if a law enforcement agency determines that such notice will impede a criminal investigation and has notified the Attorney General in writing and informs the person or agency obligated to provide notice. Notice must be made as soon as practicable and without unreasonable delay, however, after the law enforcement agency determines and informs the person or agency that notification will no longer impede an investigation. The person or agency is obligated to cooperate with law enforcement in its investigation through the provision of specified information (**Mass. Gen. Laws ch. 94, § 4**).

***Form and content of notice:*** The notice required to be provided to the Attorney General and the OCABR must include the nature of the breach of security or unauthorized acquisition and use; the number of Massachusetts residents affected; the name and address of the person or agency that experienced the breach of security; name and title of the person or agency reporting the breach of security, and their relationship to the person or agency that experienced the breach; the type of person or agency reporting the breach of security; the person responsible for the breach of security, if known; the type of personal information compromised, including, but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data; whether the person or agency maintains a written information security program; and any steps the person or agency has taken or plans to take relating to the incident, including updating the written information security program. The person who experienced a breach of security must also file a report with the attorney general and the OCABR certifying their credit monitoring services comply with section 3A (**Mass Gen. Laws ch. 93H, § 3(b)**). On receipt of the notice, the Director of the OCABR must identify any relevant consumer reporting agency or state agency, as appropriate, and must forward the name of any agency so identified to the notifying person or agency. That person or agency then must also provide notice to the consumer reporting agencies or state agencies identified by the Director. The notice to the resident must include the consumer's right to request a police report, the steps consumers may take to request a security freeze (which will be free of charge) (see **Section I.D.4.**), as well as mitigation services to be provided. However, the notification shall not include the nature of the breach or unauthorized acquisition or use or the number of residents affected (**Mass. Gen. Laws ch. 93H, § 3(b)**). Specific requirements apply to internal notifications required of agencies within the executive department (**Mass. Gen. Laws ch. 93H, § 3(e)**).

***Required credit monitoring services:*** Where a data breach involves the loss of a Massachusetts residents' Social Security number, **Chapter 93H** now requires breached entities to offer credit monitoring services to affected individuals. This new requirement makes Massachusetts the fourth state behind California, Connecticut and Delaware to have enacted such requirement. The statute has several requirements for this service, the most important of which is that it must be for a period of at least 18 months for most entities and 42 months if the breached entity is a consumer reporting agency. A report certifying compliance with the credit monitoring services must also be filed with the Attorney General and the Director of Consumer Affairs and Business Regulation.

Notice may include written notice, electronic notice if it is consistent with federal requirements regarding electronic records and signatures, or substitute notice, where the person or agency demonstrates that the cost of providing notice will exceed $250,000, the class of residents required to be notified exceeds 500,000, or the person or agency does not have sufficient contact information to provide regular notice (**Mass. Gen. Laws ch. 93H, § 1(a)**, sixth paragraph). Substitute notice must consist of e-mail notice if the person or agency has e-mail addresses for members of the affected class, clear and conspicuous posting of the notice on the home page of the person or agency if it maintains a website, and publication in or broadcast through media or medium that provides notice throughout the Commonwealth (**Mass. Gen. Laws ch. 93H, § 1(a)**, ninth paragraph).

***Compliance with other laws:*** The data breach notification law does not relieve a person or agency from any requirements of an applicable general, special, or federal law regarding the privacy and protection of personal information. However, a person who maintains procedures for responding to a security breach pursuant to federal law or regulations is deemed to be in compliance with the data breach notification law if the person provides notification in compliance with those requirements and notifies the Attorney General and the Director of the OCABR as soon as practicable and without unreasonable delay. The notice to the AG and the OCABR must include any steps the person or agency takes or plans to take with respect to the breach pursuant to the applicable federal law or regulation, and if the person or agency does not comply with the applicable requirements, the person or agency is in violation of the data breach notification law (**Mass. Gen. Laws ch. 93H, § 5**).

***Remedies:*** The Attorney General may bring a cause of action under **Mass. Gen. Laws ch. 93A, § 4** to restrain violations of the data breach notification law and to impose penalties. For more information, see **Section II.C.**

***Proposed legislation:*** A number of bills pending in the 2017 legislative session would amend the provisions of the data breach notification law (see **Section IV.B.**).

**9. Data Transfer & Cloud Computing** –

***Regulations on security standards for personal information:*** Massachusetts regulations governing data security requirements applicable to all persons owning or licensing personal information of Massachusetts residents include

provisions regarding the storage and transmission of data via public networks and wirelessly. For more information on these requirements, see **Section I.C.6.**

***Attorney use of cloud-based systems:*** In **Ethics Opinion 12-03**, the Massachusetts Bar Association states that a lawyer may store and synchronize electronic work files containing confidential client information across different platforms using an Internet-based storage method provided that the lawyer undertakes reasonable efforts to ensure that the provider's terms of use and privacy policies, practices, and procedures are compatible with the lawyer's professional obligations, including the duty to protect confidential client information. However, lawyers must follow a client's express instruction that confidential information not be stored in this manner and should refrain from storing or transmitting particularly sensitive information via the Internet without first obtaining the client's express consent.

**10. Other Provisions** –

Our research has revealed no other generally applicable data management provisions in Massachusetts.

**D. Specific Types of Data**

**1. Biometric Data** –

***Data security regulations:*** Under the Massachusetts data security regulations, every person who owns or licenses data containing the personal information of a Massachusetts resident must, among other requirements, include as part of a comprehensive information security program secure user authentication protocols, including a reasonably secure method of the use of biometrics and a unique identifier technology (**201 CMR 17.04(1)(b)**). For more information on these regulations, see **Section I.C.6.**

***Data disposal requirements:*** Biometric information is a data element that, in combination with a person's name, is considered "personal information" subject to requirements regarding the proper disposal of data containing such information (see **Section I.C.7.**).

***Proposed legislation:*** Bills introduced in the 2017 session of the Massachusetts General Court would, if enacted, add biometrics to the definition of "personal information" that would be subject to the Commonwealth's data breach security requirements (see **Section I.C.8.**). For additional information on the proposal, see **Section IV.B.**

**2. Consumer Data** –

***Prohibition on requiring written personal information to complete check transaction:*** No person, firm, partnership, or corporation that accepts a check as payment for a business transaction may require, as a condition of accepting the check, that the person provide a credit card number or any personal information other than a name, address, motor vehicle license number or state ID card number, and telephone number, unless certain conditions apply. For more information on this prohibition, see **Section I.D.3.**

***Data breach notification law:*** Consumer data generally includes information, such as an individual's name coupled with defined data elements like social security numbers or account numbers, that is considered "personal information" subject to the provisions of the data breach notification law (see **Section I.C.8.**).

***Data security and data disposal standards:*** Consumer data generally includes information, such as an individual's name coupled with defined data elements like social security numbers or account numbers, that is considered "personal information" subject to provisions of Massachusetts law and regulations imposing data security requirements on persons who own or license such information (see **Section I.C.6.**) and requirements regarding the proper disposal of data containing such information (see **Section I.C.7.**).

**3. Credit Card Data** –

***Prohibition on requiring written personal information to complete credit card transaction or for acceptance of a check:*** No person, firm, partnership, or corporation that accepts a credit card for a business transaction may require that a credit card holder write personal information not required by the credit card issuer on the credit card transaction form. Such identification includes a holder's address or telephone number. The prohibition does not apply when a person, firm, partnership, or corporation requests such information as necessary for shipping, delivery, or installation of purchased merchandise or services or for a warranty when the information is voluntarily provided (**Mass. Gen. Laws ch. 93, § 105(a)**).

In addition, no person, firm, partnership, or corporation that accepts a check as payment for a business transaction may require, as a condition of accepting the check, that the person provide a credit card number or any personal information other than a name, address, motor vehicle license number or state ID card number, and telephone number. The entity accepting the check also may verify the signature, name, and expiration date on a credit card number, and if a telephone number is requested, the person presenting the check may provide either a home number or a daytime number (**Mass. Gen. Laws ch. 93, § 105(b)(1)**). The entity accepting the check also may not require the person paying by check to permit a credit card to be charged to cover the amount of the check, contact the credit card issuer to determine if the amount of credit available to the customer is sufficient to cover the amount of the check, require that the credit card number be recorded as a condition for acceptance at any point in the transaction, or record any information regarding a person's race on the check (**Mass. Gen. Laws ch. 93, § 105(b)(2)**-(5)).

The prohibitions outlined above do not apply to a person who requests or records a credit card number in lieu of requiring a cash deposit to secure payment or who records a credit card number and expiration date as a condition for cashing or accepting a check where the person has agreed with the card issuer to cash or accept checks from the issuer's cardholders and the issuer acts as a guarantor of the transaction (**Mass. Gen. Laws ch. 93, § 105(c)**). A violation is considered to be an unfair and deceptive trade practice, and individuals aggrieved by a violation may inform the Office of Consumer Affairs and Business Regulation or the Attorney General (**Mass. Gen. Laws ch. 93, § 105(d)**; see **Section II.C.**).

***Data breach notification law:*** When used in combination with a person's name, credit or debit card numbers, with or without any required security code, access code, or password allowing access to a resident's financial accounts, are included in the definition of "personal information" subject to the provisions of the general data breach notification law (see **Section I.C.8.**).

***Data security and data disposal standards:*** When used in combination with a person's name, credit or debit card numbers, with or without any required security code, access code, or password allowing access to a resident's financial account, are included in the definition of "personal information" subject to provisions of Massachusetts law and regulations imposing data security requirements on persons who own or license such information (see **Section I.C.6.**) and requirements regarding the proper disposal of data containing such information (see **Section I.C.7.**).

**4. Credit Reports** –

***Permitted credit report disclosures:*** In general, under the Massachusetts consumer protection law, a credit reporting agency (CRA) may only provide a credit report under specified circumstances, primarily to a person who it reasonably believes will use the report for a particular purpose such as in connection with a credit transaction, for employment purposes, for insurance underwriting, or other purposes (**Mass. Gen. Laws ch. 93, § 51**). For any use not specified in section 51, users can only obtain a consumer report if the user (i) obtains prior written, verbal or electronic consent of the consumer; and (ii) discloses, prior to obtaining consent, the user's reason for accessing the consumer report to the consumer (**Mass Gen. Laws ch. 93 § 51B**). In addition, a CRA may furnish the following identifying information to a governmental agency with respect to any consumer: name, address, former addresses, places of employment, or former places of employment (**Mass. Gen. Laws ch. 93, § 55**).

***Correction of credit report information:*** If the completeness or accuracy of any item of information in a credit report is disputed by a consumer, the consumer may report the inaccuracy to the CRA, which must reinvestigate and record the current status of the information within 30 business days of receipt of notice. If a dispute is deemed frivolous or irrelevant by the CRA, it must notify the consumer of this finding within five business days of receipt of the dispute. If the reinvestigation finds that the information is inaccurate or can no longer be verified, the CRA must delete the information within three business days. In the event the reinvestigation does not resolve a dispute, the consumer may file a statement setting forth the nature of the dispute. Finally, within ten business days of the completion of a reinvestigation, the CRA must furnish the consumer with a statement that the reinvestigation is complete and a general description of any steps taken as a result (**Mass. Gen. Laws ch. 93, § 58**).

***Consumer report for employment purposes:*** A CRA that furnishes a consumer report for employment purposes that includes information that is a matter of public record but that nonetheless could adversely affect the consumer's ability to obtain employment must notify the consumer of the fact that the public record information is being reported and the name and address of the requesting party or must maintain procedures to ensure that such information is complete and up-to-date. Items of public record relating to arrests, indictments, convictions, suits, tax liens, and outstanding judgments are considered up-to-date if the current public record status of the item is reported. In addition, CRAs furnishing reports for employment purposes must enter into an agreement with the user providing that no consumer report may be requested until the user has provided notice to the employee or prospective employee of the request (**Mass. Gen. Laws ch. 93, § 60**).

***Necessary disclosures to consumers:*** Upon request of a consumer, a CRA must clearly and accurately disclosure the nature, contents, and substance of all information in its file on the consumer at the time of the request; the sources of all of its credit information, except for sources of information acquired solely for use in preparing an investigative consumer report; and the recipients of the consumer's report which it has furnished for employment purposes within the previous 2 years, and for any other purpose within the previous 6 months (**Mass. Gen. Laws ch. 93, § 56(a)**). In addition, **Mass. Gen. Laws ch. 93 § 56(b)** provides for specific rights CRAs must disclose to consumers upon contact (by phone, mail, electronic communication, or in person) regarding information on the consumer the CRA may contain in its files. The written disclosure must also be made upon a consumer's request to be advised on his or her rights.

***Security freezes:*** A consumer may request a security freeze by sending a request to a CRA by certified, overnight, or regular mail to an address designated by the agency or by another method specified by regulation (**Mass. Gen. Laws ch. 93, § 62A**, second paragraph). Under regulations promulgated by the Office of Consumer Affairs and Business Regulation ("OCABR Regulations"), notice also may be provided by a form of approved, encrypted electronic communication at an electronic address designated by the agency (**201 CMR 16.03(b)**).

***Note:*** *Federal legislation effective Sept. 21, 2018—the Economic Growth, Regulatory Relief, and Consumer Protection Act (**Pub. L. No. 115-174**)—established a national security freeze law applicable to consumers in general as well as to protected consumers (i.e., those under age 16 or those who are incapacitated or for whom a guardian or conservator has been appointed). The law amends provisions of the **Fair Credit Reporting Act** by establishing federal parameters for placing, temporarily lifting, or removing such freezes; it also prohibits the imposition of fees by a consumer reporting agency (CRA) for such services (**15 U.S.C. § 1681c-1(i)** and (j)). The federal law preempts state law provisions governing security freezes (**Mass. Gen. Laws ch. 93, § 62A**). In the case of state fee provisions, the federal law is more favorable to consumers, but some states have stronger protections in their security freeze laws than those under the federal provision, including states that prohibit access to a security freeze for employer background checks. The federal law specifically permits access to a report subject to a freeze for such purposes.*

*Information required to be provided to consumers:* Both the security freeze law and the OCABR Regulations require CRAs to provide specified information to consumers regarding security freezes—including the processes for placing, removing, and lifting a freeze, as well as notice that separate freezes are required for each CRA—and information on required fees and procedures to replace lost personal ID numbers and passwords (**Mass. Gen. Laws ch. 93, § 62A**, first paragraph; **201 CMR 16.03**).

*Placement of freeze:* A CRA must place a security freeze on a consumer's account as soon as practicable but no later than three business days after receipt of the request. The CRA must send written confirmation of the freeze to the consumer within five business days after receipt of the request that includes a unique personal ID number or password, or both, to be used to remove or lift the freeze (**Mass. Gen. Laws ch. 93, § 62A**, third paragraph; **201 CMR 16.04**). In addition, the OCABR Regulations require that specific notice set forth in **Mass. Gen. Laws ch. 93, § 56(b)** with respect to security freezes must be provided (**201 CMR 16.04(e)**). Third parties that request access to a credit report on which a freeze has been placed pursuant to an application for credit and for which access is not permitted by the consumer may treat the application as incomplete (**Mass. Gen. Laws ch. 93, § 62A**, eighth paragraph).

*Lifting security freeze:* A consumer wishing to lift a security freeze must contact the CRA with a request containing the proper identification and personal ID number or password, together with the third party designated to receive the report and the specific period of time for which the report will be available. The CRA must comply with the

request to lift the freeze as soon as practicable but no later than three business days after receipt of the request (**Mass. Gen. Laws ch. 93, § 62A**, fourth and fifth paragraphs; **201 CMR 16.05**).

*Removal of security freeze:* A security freeze must remain in place until a consumer requests that it be lifted or removed (**Mass. Gen. Laws ch. 93, § 62A**, sixth paragraph; **201 CMR 16.06**). A CRA must remove a security freeze within three business days of receipt of a request for removal containing the proper identification and personal ID number or password (**Mass. Gen. Laws ch. 93, § 62A**, ninth paragraph). A CRA also may remove a freeze that was placed as a result of a material misrepresentation by the consumer on five business days' notice to the consumer (**Mass. Gen. Laws ch. 93, § 62A**, sixth paragraph). The OCABR Regulations specify the elements of the notice, including the basis on which the CRA determined the existence of a material misrepresentation, the effective date of any action taken, and contact information with respect to disputing the findings (**201 CMR 16.07**).

*Changes to information:* A CRA may not make any changes in the official information in a report that is subject to a security freeze without sending written confirmation to the consumer within 30 days of the change of any of the following: name, date of birth, social security number, and address. Any notice of an address change must be sent to both the former and new address of the consumer. Technical modifications, such as name and street abbreviations, complete spellings, or number transpositions, do not require the notice (**Mass. Gen. Laws ch. 93, § 62A**, seventh paragraph; **201 CMR 16.08**).

*Lost personal ID number or password:* The OCABR Regulations set forth the procedure for CRAs with respect to receipt of notice of a lost personal ID number or password. The CRA must cancel the lost number and, as soon as practicable and without unreasonable delay but no more than three business days after receipt of notice, mail the consumer a new personal ID number or password. The new number may not contain the consumer's social security number or any sequence of three or more numbers thereof (**201 CMR 16.09**).

*Exceptions:* The security freeze requirements do not apply to the use of credit reports by a variety of persons and entities, including persons with whom the consumer has a financial obligation for purposes of reviewing an account or collecting an obligation; persons to whom access has been granted for facilitating the extension of credit; persons acting pursuant to warrant or court order, specified federal, state, or local agencies; or any person or entity for purposes of providing the consumer's credit score at the consumer's request, among others (**Mass. Gen. Laws ch. 93, § 62A**, tenth paragraph, subsecs. (a)-(i)).

In addition, specified entities are not required to place a security freeze in a credit report, including check services and fraud prevention companies, deposit account information service companies, or consumer reporting agencies that act only to resell credit information by assembling information held and maintained in the databases of one or more credit reporting agencies and that do not maintain a permanent database of information from which new credit reports are produced (**Mass. Gen. Laws ch. 93, § 62A**, twelfth paragraph, subsecs. (a)-(c)).

*Fees:* In accordance with **15 U.S.C § 1681c-1** and to the extent permitted by federal law, a consumer reporting agency shall not charge a fee to any consumer who elects to place, lift or remove a security freeze from a consumer report. (**Mass Gen. Laws ch. 93, § 62A**) (See the note on the Economic Growth, Regulatory Relief, and Consumer Protection Act, above).

***Data breach notification law:*** Persons or agencies required to provide notice of a security breach may be required to provide the notice to identified consumer reporting agencies under specified circumstances (see **Section I.C.8.**).

**5. Criminal Records** –

***Inquiries about criminal records:*** In general, an employer may not request information, keep a record of such information, use a form requesting information, or discriminate against any person for the failure to comply with an oral or written request for information concerning an arrest, detention, or disposition regarding any law violation for which no conviction resulted; first convictions for specified minor violations such as drunkenness, simple assault, or traffic violations; or any misdemeanor conviction more than five years old from the date of the employment application, unless the applicant was convicted of a separate offense within that period. No person may be found guilty of perjury or of otherwise giving a false statement if he falls within these provisions (**Mass. Gen. Laws ch. 151B, § 4(9)**).

In addition to the above restrictions, an employer may not request criminal record offender information (referred to as "CORI") on an initial application form, making Massachusetts a "ban-the-box" state. Such inquiries may be made, however, if the applicant is applying for a position for which any federal or state law or regulation creates mandatory or presumptive disqualification based on a conviction for one or more types of criminal offenses, or the employer is subject to an obligation under state or federal regulation not to employ any person who has been convicted of one or more types of offenses (**Mass. Gen. Laws ch. 151B, § 4**(9½)). Regulations promulgated by the Department of Criminal Justice Information Services provide guidance with respect to accessing CORI for the purposes of employment, volunteer opportunities, or professional licensing, including permissible and restricted access to CORI and storage, retention, and destruction requirements (**803 CMR 2.00** to **803 CMR 2.27**). Specifically, no individual or entity may require a person to provide a copy of the person's CORI (**803 CMR 2.08**), and non-law enforcement requestors are not permitted to request an individual's CORI without the individual's authorization (**803 CMR 2.22**).

***Inquiries about criminal convictions by state agency employers:*** In an executive order issued in January 2008, Massachusetts Governor Deval Patrick announced that it is the policy of the Commonwealth's Executive Department to conduct criminal background checks and consider the results for employment purposes to the extent that an applicant has been deemed otherwise qualified for a position and the content of the criminal record is relevant to the position in question. Specific examples of relevance include instances in which a criminal conviction triggers a statutory disqualification or where a position requires interaction with vulnerable populations and a check is required to ensure that an applicant does not pose a safety risk. The order provides for training of Executive Department agencies and their employees and requires the launch of a public education program to inform the public and employers about their rights (**Executive Order No. 495**, Jan. 11, 2008).

***Required background checks:*** Certain entities involved in health care or working with vulnerable individuals are required to conduct background checks for all job applicants. For information on these requirements, consult the regulations promulgated by the Executive Office of Health and Human Services at **101 CMR 15.00** to **101 CMR 15.15**, and the regulations promulgated by the Department of Children and Families at **110 CMR 18.00** to **110 CMR 18.16**.

**6. Drivers' Licenses/Motor Vehicle Records** –

***Data breach notification law:*** When used in combination with a person's name, driver's license numbers and state ID numbers are included in the definition of "personal information" subject to the provisions of the data breach notification law (see **Section I.C.8.**).

***Data security and data disposal standards:*** When used in combination with a person's name, driver's license and state ID numbers are included in the definition of "personal information" subject to provisions of Massachusetts law and regulations imposing data security requirements on persons who own or license such information (see **Section I.C.6.**) and requirements regarding the proper disposal of data containing such information (see **Section I.C.7.**).

**7. Electronic Communications/Social Media Accounts** –

Our research has revealed no Massachusetts laws specific to the privacy and data security of electronic communications or social media accounts. Under Massachusetts criminal law, a warrant may be issued on probable cause to a foreign corporation providing electronic communications services to provide records that would reveal the identity of the customer, any data stored on the customer's behalf, records of customer use, and source and content information. The law further requires a Massachusetts corporation providing electronic communications services to produce records pursuant to a warrant or subpoena issued by another state (**Mass. Gen. Laws ch. 276, § 1B**).

For information on electronic surveillance of oral or wire communications, see **Section I.F.**

**8. Financial Information** –

***Data breach notification law:*** When used in combination with a person's name, financial account information, together with any required security code, access code, or password allowing access to a resident's financial account information, is included in the definition of "personal information" subject to the provisions of the data breach notification law (see **Section I.C.8.**).

***Data security and data disposal standards:*** When used in combination with a person's name, financial account information, together with any required security code, access code, or password allowing access to a resident's financial account information, is included in the definition of "personal information" subject to Massachusetts law and regulations imposing data security requirements on persons who own or license such information (see **Section I.C.6.**) and requirements regarding the proper disposal of data containing such information (see **Section I.C.7.**).

***Insurance information and privacy protection provisions:*** Individually identifiable information gathered in connection with an insurance transaction from which judgments may be made about an individual's finances is included in the definition of "personal information" subject to Massachusetts law governing insurance information and privacy protection. For a discussion of these requirements, see **Section I.E.7.**

**9. Health Data** –

***Health care providers:*** On request, a health care provider must provide a patient or the patient's representative access to and a copy of his medical records. A fee may be charged unless the record is being requested pursuant to support a claim or appeal under the federal **Social Security Act** or any federal or state financial need-based program. The term "health care provider" includes physicians, surgeons, therapists, dentists, nurses, optometrists, chiropractors, psychologists, and podiatrists (**Mass. Gen. Laws ch. 112, § 12CC**).

Certain disclosures by physicians, health care facilities, nursing homes, or other medical providers are permitted without patient consent to a government agency concerning the diagnosis, treatment, or condition of a patient in connection with specified government benefits or mandatory health department reporting (**Mass. Gen. Laws ch. 112, § 12G**).

***Hospitals and other health care facilities:*** Records maintained by a hospital or clinic other than one under the control of the Department of Mental Health may be inspected by the patient to whom they relate or the patient's attorney on delivery of a written authorization by the patient, and copies must be provided after payment of a reasonable fee. The fee does not apply to a record requested pursuant to support a claim or appeal under the federal **Social Security Act** or any federal or state financial need-based program. With respect to hospitals or clinics controlled by the Department of Mental Health, a disclosure may only be made if the Department determines that the disclosure is in the best interest of the patient (**Mass. Gen. Laws ch. 111, § 70**; see also **Mass. Gen. Laws ch. 111, § 70E**, fifth paragraph, subsec. (g)).

The records and communications of hospitals and other licensed facilities are generally confidential to the extent provided by law (**Mass. Gen. Laws ch. 111, § 70E**, fifth paragraph, subsec. (b)). However, third party reimbursers may inspect and copy records relative to a coverage, benefit, or reimbursement claim, and disclosures for peer review or utilization review (**Mass. Gen. Laws ch. 111, § 70E**, twelfth paragraph).

A person whose rights are violated as described above may bring a civil action pursuant to the Commonwealth's malpractice law (see **Section I.G.1.**).

***Fair Information Practices Act:*** Provisions in the Fair Information Practices Act govern the obligations of state agencies with respect to medical and health information. Specifically, a state agency may disclose medical or psychiatric data to a treating physician on the physician's request if a medical or psychiatric emergency arises precluding a data subject from giving approval for the release. The data subject must be given notice of the release on termination of the emergency (**Mass. Gen. Laws ch. 66A, § 2(c)**). Other provisions of the Fair Information Practices Act, including general collection, access, and amendment requirements, are applicable to any medical information held by a state agency; for information on the regulations governing these requirements, see **Section I.C.6.**

***Genetic testing:*** Records of hospitals, dispensaries, laboratories, hospital-affiliated registries, specified insurance entities, and commercial genetic testing companies pertaining to any genetic information are not public records, and their contents may not be divulged without the informed written consent of the data subject unless by court order or other statutory exception (**Mass. Gen. Laws ch. 111, § 70G(b)**). No facility, physician, or health care provider may conduct a genetic test without first obtaining prior written consent or disclose the results of a test to a third party without the informed written consent of the data subject (**Mass. Gen. Laws ch. 111, § 70G(c)**). Violations are deemed to be an unfair business trade or practice, and an aggrieved person may bring an action in his own name, or the Attorney General may institute an action for injunctive and other equitable relief (**Mass. Gen. Laws ch. 111, § 70G(d)**).

Specific provisions apply to the collection, use, and disclosure of genetic information by employers (see **Section I.E.6.**) and insurers (see **Section I.E.7.**).

***Psychologists and mental health facilities:*** A psychologist generally must have written consent to disclose any confidential communications about a patient. Exceptions are permitted when authorized in specified court proceedings; when needed for the protection of others if the patient presents a clear and present danger to himself, has made an explicit threat to kill or inflect serious bodily injury on another, or has a history of physical violence that a psychologist has reason to believe poses a clear and present danger; or when needed to collect amounts owed by the patient under certain conditions (**Mass. Gen. Laws ch. 112, § 129A**).

The Department of Mental Health must keep records related to the admission, treatment, and periodic review of patients admitted to a mental health facility under state supervision. The records are confidential and may not be disclosed except to the patient or the patient's attorney on request, pursuant to judicial order, when disclosure is in the best interest of the patient, or pursuant to specified provisions regarding sex offenses (**Mass. Gen. Laws ch. 123, § 36**).

Additional restrictions on the disclosure of mental health information are applicable to health maintenance organizations (**Mass. Gen. Laws ch. 176G, § 4B**), medical service corporations (**Mass. Gen. Laws ch. 176B, § 20**), and insurance companies (**Mass. Gen. Laws ch. 175, § 108E**).

***Drug rehabilitation information:*** Records of treatment provided to patients of drug rehabilitation facilities are confidential and may be disclosed only on judicial order, where the disclosure is authorized by provisions of federal law, or with the informed consent of the patient. The consent must be in writing and signed and must state the name of the person or organization to which the disclosure is to be made, along with the specific type of information to be disclosed and the purpose of the disclosure (**Mass. Gen. Laws ch. 111E, § 18(a)**).

***Cancer and other registries:*** Massachusetts maintains a number of registries and monitoring systems for the purpose of disease prevention and early intervention. In each instance, the law provides that information provided to a registry or monitoring system is confidential and may not be disclosed or printed except under specified circumstances. See, for example, **Mass. Gen. Laws ch. 111, § 111B** (cancer registry) and **Mass. Gen. Laws ch. 111D, § 6** (infectious disease reports).

***HIV/AIDS:*** Facilities, physicians, and health care providers are generally prohibited from testing a person for HIV, disclosing the results of such a test, or identifying the subject of a test to a third party without the subject's written oral consent. In addition, employers may not require an HIV test as a condition of employment. Exceptions are provided for specified reporting to public health authorities and for pre- and post-mortem testing for donation purposes (**Mass. Gen. Laws ch. 111, § 70F**).

***Health data held by insurance companies:*** Under the Protect Access to Confidential Healthcare (PATCH) Act, **Chapter 63 of the Acts of 2018**, patients may now require health insurance carriers to send their medical information exclusively to them, as opposed to the policyholder (**Mass. Gen. Laws ch. 176O, § 27(b)**, (f)). Because an insurance carrier's explanation of benefits (EOB) summaries often disclose sensitive information regarding a patient's health condition, adult dependents may now keep their medical information from being shared with their policyholder. In addition, health insurance carriers in Massachusetts must also use a common summary of payments form developed by the Massachusetts Division of Insurance (**Mass. Gen. Laws ch. 176O, § 27(a)**). Insurance carriers must disclose their right to request their medical information be sent directly to them instead of the policyholder in evidence of coverage documents, member privacy communications, and on common summary of payments forms, and must be conspicuously displayed on the carrier's member website and online portals for individual members (**Mass. Gen. Laws ch. 176O, § 27(g)**).

For more information specific to the obligations of entities covered by Massachusetts insurance law with respect to the collection, use, and disclosure of information, see **Section I.E.7.**

**10. Social Security Numbers** –

***Data breach notification law:*** When used in combination with a person's name, social security numbers are included in the definition of "personal information" subject to the provisions of the data breach notification law (see **Section I.C.8.**).

***Data security and data disposal standards:*** When used in combination with a person's name, social security numbers are included in the definition of "personal information" subject to provisions of Massachusetts law and regulations imposing data security requirements on persons who own or license such information (see **Section I.C.6.**) and requirements regarding the proper disposal of data containing such information (see **Section I.C.7.**).

**11. Usernames & Passwords** –

Our research has revealed no specific laws in Massachusetts related to the privacy and security of usernames and passwords. Legislation introduced in the current session of the Massachusetts legislature would, if enacted, prohibit employers and certain educational institutions from requiring an employee or student to disclose a username or password to a personal social media account or taking adverse action against an employee or student for refusing to provide such access. For more information on this legislation, see **Section IV.B.**

***Data breach notification law:*** When used in combination with a person's name, financial account information or credit or debit card numbers, with or without any required security code, access code, or password allowing access to a resident's financial accounts, are included in the definition of "personal information" subject to the provisions of the general data breach notification law (see **Section I.C.8.**).

***Data security regulations:*** Under the Massachusetts data security regulations, every person who owns or licenses data containing the personal information of a Massachusetts resident must, among other requirements, include as part of a comprehensive information security program secure user authentication protocols, including a reasonably secure method of assigning and selecting passwords (**201 CMR 17.04(1)(b)**). For more information on these regulations, see **Section I.C.6.**

***Data disposal requirements:*** Financial account or credit or debit card numbers, with or without any required security code, access code, personal ID number, or password, when used in combination with a person's name, are considered "personal information" subject to requirements regarding the proper disposal of data containing such information (see **Section I.C.7.**).

**12. Information about Minors** –

***Medical and dental treatment information:*** A minor may consent to his own medical or dental treatment in accordance with provisions governing emergency situations where a delay in treatment will endanger the life or mental well-being of the minor or in other circumstances such as where the minor is married, a member of the armed forces, or otherwise emancipated. Any information or record kept in connection with such treatment is confidential between the minor and the physician or dentist and may not be released without the written consent of the minor or pursuant to court order. However, if the physician or dentist believes that the condition of the minor is sufficiently serious to be life-threatening, the physician or dentist must notify a parent or legal guardian of the condition and inform the minor of the notification (**Mass. Gen. Laws ch. 112, § 12F**).

***Educational records:*** Parents and students generally have the right to access student records (see **Section I.E.2.**).

**13. Location Data** –

Our research has uncovered no Massachusetts laws specifically governing the privacy and security of location data. However, on April 4, 2017, the Attorney General's Office entered into an **Assurance of Discontinuance** with an advertising company that agreed not to use its "geofencing" technology to target particular individuals. Geofencing allows companies to direct advertisement to users through browsers and applications on the users' mobile devices when they are in a particular area or territory. In the case at issue, the advertiser was serving advertisements that offered alternatives to abortion as mobile users entered a location in the vicinity of abortion providers. Even though the advertiser had not geofenced clinics in Massachusetts, the Attorney General concluded that such conduct, were it to occur in Massachusetts, would constitute an unfair and deceptive trade practice. The advertiser agreed to enter into the Assurance of Discontinuance "in order to avoid the time, expense, and uncertainty of litigation."

**14. Other Personal Data** –

Our research has uncovered no other Massachusetts law provisions regarding personal data beyond those specified above.

**E. Sector-Specific Provisions**

**1. Advertising & Marketing** –

***Right of publicity:*** Any person whose name, portrait, or picture is used within Massachusetts for advertising purposes or for purposes of trade without the person's consent may bring a civil action to prevent and restrain such use and may recover damages for any injuries sustained as a result of the use. Damages may be trebled for knowing violations. An exception applies to professional photographers exhibiting their work, unless the exhibition continues after receipt of written notice from the subject objecting to the exhibition. In addition, the names of authors, composers, or artists may be used in connection with their work for advertising or trade purposes, and a person's identity can be used to sell goods if the person used his identity in connection with the manufacture or distribution of the goods (**Mass. Gen. Laws ch. 214, § 3A**).

***Do-not-call:*** The Office of Consumer Affairs and Business Regulation (OCABR) must maintain a no sales solicitation calls listing of persons who do not wish to receive unsolicited telephonic sales calls. The list must be updated not less than quarterly (**Mass. Gen. Laws ch. 159C, § 2**). The OCABR must include the part of any national consumer database relating to Massachusetts residents in its no sales solicitation list (**Mass. Gen Laws ch. 159C, § 7**).

Any person who obtains a person's name, address, or telephone number from a public directory or source with the intent to republish the information or sell it to a third party for marketing and sales solicitation purposes must exclude the name, address, or phone number of any consumer who appears on the no sales solicitation list outlined above. This provision does not apply to a telephone company whose sole purpose is to publish a telephone directory or to a person compiling such a directory on the telephone company's behalf (**Mass. Gen. Laws ch. 159C, § 5**).

Violations are subject to sanctions by the Attorney General (see **Section II.C.**) as well as a private cause of action (see **Section I.G.1.**).

***Anti-spam law:*** Massachusetts is one of a handful of states that has not enacted an anti-spam law, although attempts to do so have been made. A **page** on the state's website discusses relevant federal legislation and regulations as well as prior case law on spam.

***Data breach notification law:*** Businesses engaged in the advertising and marketing sector that own or license data that includes "personal information" as defined under the Commonwealth's data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to businesses in the advertising and marketing sector (see **Section I.C.6.** and **Section I.C.7.**).

**2. Education** –

***Access to and maintenance of student records:*** Any person operating or maintaining an educational institution in Massachusetts must, on request of any student or former student, furnish a written transcript of the student's record. There is no charge allowed for the original transcript provided, but duplicate or additional transcripts are subject to a fee of $1.00 per page, not to exceed $5.00 in total (**Mass. Gen. Laws ch. 71, § 34A**). If the person obligated to provide a transcript as described above fails to respond within 30 days of the request, the student or former student may file a petition in superior court for relief, and the court may issue an appropriate order, with a failure to obey considered contempt of court. In addition, the court may award costs and reasonable attorney fees to the petitioner (**Mass. Gen. Laws ch. 71, § 34B**).

Each school committee must, at the request of a parent or guardian of a student, allow the parent or guardian to inspect academic, scholastic, or other records of the student, regardless of the student's age. For students age 18 and over, a school committee must allow the student complete access to all student records on request (**Mass. Gen. Laws ch. 71, § 34E**). Specific provisions apply to a request for access to records by noncustodial parents (**Mass. Gen. Laws ch. 71, § 34H**).

In addition, regulations promulgated by the Massachusetts Department of Elementary and Secondary Education pursuant to **Mass. Gen. Laws ch. 71, § 34D**govern the maintenance, retention, duplication, storage, and periodic destruction of student records by public elementary and secondary schools (**603 CMR 23.00**to **603 CMR 23.12**). The provisions of these regulations are outlined below.

*Scope:* The regulations are designed to ensure parents' and students' rights of confidentiality, inspection, amendment, and destruction of student records. The rights described in the regulations are the rights of the student's parent for any student under age 14. For students age 14 through 17 or those who have entered ninth grade, the rights may be exercised by the student or the parent, acting alone or together. Students age 18 and older have these rights exclusively, although parents may continue to exercise the right until expressly limited by the student, who may choose which rights to limit, and all parents have the right to inspect academic, scholastic, or other records of the student regardless of the student's age (**603 CMR 23.01**).

*Collection of data and privacy and security:* Information and data contained in or added to a student record must be limited to information relevant to the educational needs of the student. Any such data should include the name, signature, and position of the source and the date of entry. Standardized test results need only include the name of the test and/or the publisher and the date of testing (**603 CMR 23.03**). Memory aids and other information contained in the personal file of a school employee and not accessible or revealed to authorized school personnel or any third party are not considered part of the student record. Such information may be shared with the student, parent, or a temporary substitute of the school employee, but if it is released to authorized school personnel, it becomes part of the student record (**603 CMR 23.04**).

School principals or their designees are responsible for the privacy and security of student records maintained at their school. The superintendent of schools or his designee is responsible for the privacy and security of school records not under the supervision of a school principal. Each must ensure that student records are kept physically secure, that any computerized systems are electronically secure, and that authorized personnel are properly trained in the importance of information privacy and security, as well as in provisions regarding access to student records by noncustodial parents (**603 CMR 23.05**).

*Destruction of records:* Student transcripts must be maintained by the school department and may only be destroyed 60 years after the student's graduation, transfer, or withdrawal from the school system (**603 CMR 23.06(1)**). During a student's enrollment, a principal or designee must periodically review and destroy misleading, outdated, or irrelevant information in a temporary record, provided that the student and/or parent is given written notice and the opportunity to receive a copy of the information prior to destruction (**603 CMR 23.06(2)**). Such temporary records must be destroyed no later than seven years after the student graduates, transfers, or withdraws from the school system. Written notice of the approximate date of destruction and the right to request a copy must be given to the student and the student's parent at the time of graduation, transfer, or withdrawal (**603 CMR 23.06(3)**).

*Access to student records:* Eligible students and their parents have access to student records. Access must be provided as soon as practicable and within 10 days of the initial request except for noncustodial parents (see below). The entire student record must be made available regardless of its physical location. The regulations outline the rights of students and parents, including the right to have a student record interpreted by school personnel or inspected by a third party (**603 CMR 23.07(2)**). Authorized school personnel may access student records when required to perform their official duties without the consent of a student or parent (**603 CMR 23.07(3)**).

In general, third parties may not access information in a student record without the specific, informed, written consent of the eligible student or parent. The regulations provide for a variety of exceptions to this requirement, including releases of specified directory information; releases pursuant to court order; releases to specified state agencies and federal, state, and local education officials; releases necessary in emergencies; and releases to health personnel, among others (**603 CMR 23.07(4)**).

*Noncustodial parents:* A noncustodial parent generally has access to student records, unless the parent has been denied legal custody or has been ordered to supervised visitation, has been denied visitation, has had access to the student restricted by a temporary or permanent protective order, or is subject to an order of a probate and family court judge restricting distribution of student records to the parent. The regulations specify requirements noncustodial parents must meet to gain access (**603 CMR 23.07(5)**).

*Amendment and correction of school records:* An eligible student or parent has the right to add information, comments, data, or other relevant written material to the student record (**603 CMR 23.08(1)**). In addition, the eligible student or parent may request in writing deletion or amendment of any material contained in a student record, except for information inserted in the record by a special education evaluation team, which are subject to specific requirements. If a student or parent believes that adding information is insufficient to explain, clarify, or correct

objectionable material, he must present the objection in writing or must have the right to have a conference with the principal. Within one week after receipt of such a request or conference, the principal must render a decision in writing to the student or parent that states the reasons for the decision. The principal must promptly take such steps as are necessary to effectuate a decision favorable to the student or parent (**603 CMR 23.08(2)**).

*Appeals and notification requirements:* A student or parent who believes that an action of a principal does not comport with the requirements outlined above may appeal to the superintendent of schools. The regulations set forth the procedures applicable to such appeals (**603 CMR 23.09**). Schools are required to send to a student and parent an annual routine information letter, in their primary language, informing them of any standardized testing programs and research studies to be conducted and other routine information to be collected from the student during the year and the general regulatory provisions regarding parent and student rights. Schools required by law to conduct a bilingual program must furnish all forms, regulations, and other documents required to be provided to parents in the language spoken in the student's home (**603 CMR 23.10**).

***Data breach notification law:*** Businesses engaged in the education sector that own or license data that includes "personal information" as defined under the Commonwealth's data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to businesses in the education sector (see **Section I.C.6.** and **Section I.C.7.**).

**3. Electronic Commerce** –

***Data breach notification law:*** Businesses engaged in the electronic commerce sector that own or license data that includes "personal information" as defined under the Commonwealth's data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to businesses in the electronic commerce sector (see **Section I.C.6.** and **Section I.C.7.**).

**4. Financial Services** –

***Insurance information and privacy protection provisions:*** For a discussion of requirements applicable to licensed insurers concerning the collection and disclosure of financial information, see **Section I.E.7.**

***Data breach notification law:*** Businesses engaged in the financial services sector that own or license data that includes "personal information" as defined under the Commonwealth's general data breach notification law are subject to the law's provisions regarding required notices in a breach of the security of a system. However, the law specifically provides that persons or agencies subject to privacy provisions contained in federal law or regulations that maintain procedures for breach notification in accordance with such law or regulations are deemed to be in compliance (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to businesses in the financial services sector (see **Section I.C.6.** and **Section I.C.7.**).

**5. Health Care** –

***Access and disclosure requirements:*** Collection, access, and disclosure requirements applicable to hospitals, physicians, and other health care providers and facilities are detailed at **Section I.D.9.**

***Data breach notification law:*** Businesses engaged in the health care sector that own or license data that includes "personal information" as defined under the Commonwealth's data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to businesses in the health care sector (see **Section I.C.6.** and **Section I.C.7.**).

**6. HR & Employment** –

***General prohibition against interference with privacy:*** Under Massachusetts law, persons have the general right against unreasonable, substantial, or serious interference with their privacy. The superior court has equity jurisdiction to enforce this right and to award damages accordingly (**Mass. Gen. Laws ch. 214, § 1B**). This statute forms the primary basis for employee challenges against employer activities in the courts of the Commonwealth. In determining whether an employer has violated the general privacy provision, courts have generally balanced the employer's legitimate business interests against the level of intrusion on an employee's privacy rights (see, for example, *Gauthier v. Police Comm'r of Boston*, **408 Mass. 335**, **557 N.E.2d 1374** (Mass. 1990) (regarding drug testing) and *Garrity v. John Hancock Mutual Life Ins. Co.*, **2002 BL 1704** (D. Mass. 2002) (regarding sexually explicit e-mail)).

***Criminal records requirements:*** For information on requirements applicable to employers with respect to criminal records of employees or applicants, see **Section I.D.5.**

***Employee access to and correction of personnel records:*** Employers must notify an employee within 10 days of placing information in the employee's personnel record that has been used or may be used to negatively impact the employee's qualification for promotion, transfer, or additional compensation, as well as information that may expose the subject to disciplinary action. In addition, an employer must provide an employee the opportunity to review the employee's personnel record within five business days of receiving a written request from the employee. The review must take place at the place of employment during regular business hours. Employers must provide a copy of the personnel record within five business days of receipt of a written request from an employee. Employers cannot be required to provide access more than twice in a calendar year, provided that any notification of the placement of negative information as described above does not count as a permitted annual review (**Mass. Gen. Laws ch. 149, § 52C**, fifth paragraph). The law defines the terms "employee," "employer," and "personnel record"; of note is the fact that persons who are employed or were formerly employed by a private institution of higher education in a tenured position are not considered to be employees (**Mass. Gen. Laws ch. 149, § 52C**, second through fourth paragraphs).

If there is disagreement with information contained in the personnel record, removal or correction of such information may be mutually agreed upon. If no agreement is reached, an employee may submit a written statement explaining the employee's position, which becomes part of the personnel record and must be included when information is transferred to a third party. If an employer places information in an employee's file that it knows to be false, the employee has a remedy through a collective bargaining agreement, other personnel procedures, or judicial process to have the information expunged (**Mass. Gen. Laws ch. 149, § 52C**, sixth paragraph).

Employers having more than 20 employees are required to maintain personnel records of employees and to retain them without deletions or expungement from the date of employment to the date three years after the termination of employment. In addition, records that are the subject of an administrative or judicial proceeding must be retained until the termination of the proceeding (**Mass. Gen. Laws ch. 149, § 52C**, seventh paragraph).

Violations are subject to a fine of not less than $500 nor more than $2,500, levied by the Attorney General (**Mass. Gen. Laws ch. 149, § 52C**, ninth paragraph).

***Lie detector tests:*** Employers are prohibited, with respect to an employee or applicant, including applicants for employment as a police officer, to subject the employee or applicant to submit to a lie detector test, to request that the employee or applicant take a lie detector test, or to discharge, not hire, demote, or otherwise discriminate against the employee or applicant for asserting his rights. The prohibition does not apply to lie detector tests conducted by law enforcement agencies as otherwise permitted in a criminal investigation. The fact that a lie detector test was conducted outside Massachusetts with respect to employment is not a defense against the prohibition, and all employment applications must contain a notice explaining the prohibition (**Mass. Gen. Laws ch. 149, § 19B(2)**).

Violations are subject to fines (see **Section II.D.**) and a potential civil cause of action (see **Section I.G.4.**).

***Genetic testing:*** It is unlawful for any employer, employment agency, or labor organization to collect, solicit, or require disclosure of genetic information as a condition of employment; to solicit submission to or require a genetic test; or to refuse to hire or employ a person on the basis of genetic information (**Mass. Gen. Laws ch. 151B, § 4(19)**).

***HIV/AIDS:*** Employers may not require an HIV test as a condition of employment (**Mass. Gen. Laws ch. 111, § 70F**).

***Data breach notification law:*** Employers that own or license data that includes "personal information" as defined under the Commonwealth's data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to employers (see **Section I.C.6.** and **Section I.C.7.**).

**7. Insurance** –

***Insurance information and privacy protection law:*** Massachusetts insurance code provisions regarding insurance information and privacy protection (**Mass. Gen. Laws ch. 175I, § 1** to 22, referred to hereinafter as "the IIPP law") establish standards with respect to the collection, use, and disclosure of information gathered in connection with an insurance transaction by insurance institutions, insurance representatives, and insurance support organizations. The provisions of the IIPP law are outlined in detail below.

*Scope:* The provisions of the IIPP law apply to insurance institutions, insurance representatives, and insurance support organizations, including life, health, or disability insurers that collect information or engage in insurance transactions with Massachusetts residents or engage in an insurance transaction with an applicant, individual, or policyholder who is a resident (**Mass. Gen. Laws ch. 175I, § 1**).

*Primary definitions:* The law defines "insurance institution," "insurance support organization," and "insurance representative" in the context of the IIPP law. In addition, "personal information" is defined as any individually identifiable information gathered in connection with an insurance transaction from which judgment can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristic, including an individual's name, address, and medical record information, but excluding privileged information. "Medical record information" is personal information relating to a person's physical or mental condition, medical history, or medical treatment that is obtained from a medical profession or medical care institution, from the individual, or from the individual's spouse, parent, or guardian (**Mass. Gen. Laws ch. 175I, § 2**).

*Pretext interviews:* Insurance institutions, representatives, and support organizations generally are prohibited from conducting pretext interviews to obtain information in connection with an insurance transaction. However, pretext interviews may be undertaken to obtain information from a person or institution that does not have a generally or statutorily recognized privileged relationship with the person to whom the information relates in connection with investigating a claim where criminal activity, fraud, or misrepresentation are reasonably suspected (**Mass. Gen. Laws ch. 175I, § 3**).

*Notice of information practices:* Insurance institutions and representatives must provide a notice of information practices to all applicants and policy holders. With respect to applications, the notice must be provided no later than the time the application for insurance is made. In the case of a renewal, notice must be provided no later than the policy renewal date, except that notice is not required if personal information is collected only from the policyholder or public records or if a notice meeting the requirements of the IIPP law has been given within the previous 24 months. With respect to policy reinstatements or changes in benefits, notice must be given no later than the time the request for reinstatement or change in benefits is received by the insurance institution, except that notice is not required if personal information is collected only from the policyholder or public records (**Mass. Gen. Laws ch. 175I, § 4(a)**).

The notice must be in writing and must contain specified items, including whether personal information may be collected from persons other than the individual, the types of personal information collected and the sources and techniques used, the types of disclosures that may be made (see below), a description of the individual's rights, and that information obtained from a report prepared by an insurance support organization may be retained by the organization and disclosed to others (**Mass. Gen. Laws ch. 175I, § 4(b)**). In lieu of the notice described above, an insurance institution or representative may provide an abbreviated notice informing the applicant or policyholder that personal information may be collected from persons other than the individual, such information may be disclosed to third parties without authorization, a right of access and correction exists with respect to all personal information collected, and the full notice is available on request (**Mass. Gen. Laws ch. 175I, § 4(c)**). The obligations

 

described above may be satisfied by another insurance institution or representative acting on behalf of the person subject to the obligations (**Mass. Gen. Laws ch. 175I, § 4(d)**).

*Marketing and research surveys and investigative consumer reports:* Insurance institutions and representatives must clearly specify questions designed to obtain information solely for marketing or research purposes from an individual in connection with an insurance transaction (**Mass. Gen. Laws ch. 175I, § 5**).

In general, insurance institutions, representatives, and support organizations are prohibited from preparing or requesting an investigative consumer report in connection with an insurance transaction unless they inform the individual that he may request to be interviewed in the preparation of the report and is entitled to a copy of the report on request (**Mass. Gen. Laws ch. 175I, § 7(a)**). Insurance institutions and representatives must institute reasonable procedures to conduct interviews when requested and must inform an insurance support organization preparing a report on their behalf of any request by an individual for a personal interview. The organization must have reasonable procedures to conduct such interviews (**Mass. Gen. Laws ch. 175I, § 7(b)**-(c)). Investigative consumer reports may not contain any information designed to determine an individual's sexual orientation or information related to counseling for AIDS or AIDS-related complex (ARC) (**Mass. Gen. Laws ch. 175I, § 7(d)**).

*Disclosure requirements:* An insurance institution, representative, or support organization may not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is with the written consent of the individual, provided that if the authorization is submitted by another insurance institution, representative, or support organization, it meets statutory requirements regarding the form and content of an authorization, or if the authorization is submitted by a person other than such an party, it meets these requirements and is signed, dated, and obtained one year or less before the date disclosure is sought (**Mass. Gen. Laws ch. 175I, § 13(1)**). The IIPP law outlines the elements required to be included in an authorization for disclosure, including the types of information to be disclosed, specified names and dates, the purposes for which information is collected, and the length of time for which the authorization is valid, among others (**Mass. Gen. Laws ch. 175I, § 6**).

Disclosures also are permitted to persons other than insurance institutions, representatives, and support organizations if reasonably necessary to enable the person to perform a business, professional, or insurance function for the disclosing party, and the person agrees not to disclose the information further without written authorization unless otherwise permitted by law or when reasonably necessary for the person to perform its business function, or to enable that person to provide information to the disclosing insurance institution, representative, or support organization for purposes of determining eligibility for a benefit or payment or to detect criminal activity, fraud, or material misrepresentation (**Mass. Gen. Laws ch. 175I, § 13(2)**). The law provides for additional permitted disclosures to an insurance institution, representative, or support organization when reasonably necessary for criminal activity or fraud detection or for the disclosing or receiving party to perform its function with respect to an insurance transaction, provided that the recipient is prohibited from redisclosing the information without written authorization (**Mass. Gen. Laws ch. 175I, § 13(3)**). Finally, disclosures are allowed to medical care institutions and medical professionals under specified circumstances, to insurance regulatory authorities, to law enforcement authorities under specified circumstances, as otherwise permitted or required by law, pursuant to judicial order, for specified research or statistical purposes, or to affiliates or consumer reporting agencies, among many others (**Mass. Gen. Laws ch. 175I, § 13(4)**-(18)). Specifically, insurance institutions, representatives, and support organizations may disclose information collected or received in connection with an insurance transaction without written authorization of the disclosure to a person whose only use of the information will be to perform services or functions in connection with marketing of a product or service, provided that no medical record information, privileged information, or personal information regarding health, character, personal habits, mode of living or general reputation of an individual is disclosed; the individual has been given the opportunity to indicate that he does not want personal information disclosed for marketing purposes and has not so indicated; and the person receiving the information agrees not to use it except in connection with the marketing of a product or service (**Mass. Gen. Laws ch. 175I, § 13(11)**).

*Access to insurance information:* Insurance institutions, representatives, and support organizations must make personal information collected or maintained in connection with an insurance transaction available to the individual to whom it refers or to the individual's representative (**Mass. Gen. Laws ch. 175I, § 8(a)**). If any individual, after providing proper identification, submits a written request to an insurance institution, representative, or support

organization for access to recorded personal information reasonably described by the individual that can be reasonably located by the insurer, the party to whom the request was made, within 30 business days of receipt of the request, must:

• provide the individual with a copy of the personal information or inform the individual of the nature and substance of the information in writing;

• permit the individual to see and copy, in person, the information or to obtain a copy of the information by mail, at the individual's election, unless the information is encoded, in which case the insurer must provide an accurate translation in plain language;

• disclose to the individual the identity of any person to whom the insurer has disclosed the information within the two years preceding the request, if recorded, and if not recorded, the names of those institutions or persons to whom the information is normally disclosed; and

• provide the individual with a summary of procedures by which the individual may request correction, amendment, or deletion of the information (**Mass. Gen. Laws ch. 175I, § 8(b)**).

Any personal information provided as outlined above must contain the name of or identify the source of information, except that a natural person acting in a personal capacity need not be revealed if confidentiality was specifically promised (**Mass. Gen. Laws ch. 175I, § 8(c)**).

Medical record information originally supplied by a medical care institution or a medical provider and requested as outlined above, together with the identity of the medical professional or medical care institution that provided the information, may be supplied directly to the individual requesting it or to a medical provider designated by the individual, at the election of the individual. Disclosure of mental health information directly to the individual may be made only with the approval of the qualified professional person with treatment responsibility for the condition to which the mental treatment relates or a similarly qualified professional. On the release of any medical or mental health record information to a medical professional designated by an individual, the insurance institution, representative, or support organization must notify the individual that it has provided the information at the time of the disclosure (**Mass. Gen. Laws ch. 175I, § 8(d)**). Insurance institutions, representatives, and support organizations providing access to personal information as outlined above may charge a reasonable fee for costs incurred in providing copies (**Mass. Gen. Laws ch. 175I, § 8(e)**). The access obligations described above may be met by another insurance institution, producer, or support organization acting on behalf of the insurance institution, agent, or support organization (**Mass. Gen. Laws ch. 175I, § 8(f)**).

*Correction, amendment, and deletion:* Any individual has the right to have factual errors in his personal information corrected and misrepresentations or misleading entries amended or deleted (**Mass. Gen. Laws ch. 175I, § 9(a)**). Within 30 business days of receipt of a written request to correct, amend, or delete recorded personal information in its possession, an insurance institution, representative, or support organization must either correct, amend, or delete the information or reinvestigate the disputed information and, on completion of the investigation, make necessary corrections, amendments, or deletions or notify the individual of its refuse to correct, amend, or delete, the reasons for its refusal, and the individual's right to file a statement or request review by the Commissioner of Insurance (see below) (**Mass. Gen. Laws ch. 175I, § 9(b)**).

If an insurance institution, representative, or support organization corrects, amends, or deletes personal information, it must notify the requesting individual and must provide the corrected information to any person specified by the individual who may have received the recorded information in the previous two years, any insurance support organization if it has systematically received recorded personal information from the insurer in the past seven years (unless the support organization no longer maintains personal information about the individual), and any insurance support organization that furnished the subject personal information (**Mass. Gen. Laws ch. 175I, § 9(c)**).

Any individual disagreeing with the refusal of an insurance institution, representative, or support organization to correct, amend, or delete disputed health information may file a statement setting forth what the individual thinks is the correct information and the reasons why the individual disagrees with the refusal to correct, amend, or delete. The insurance institution, agent, or support organization must file the statement with the individual's disputed information, provide the statement in any subsequent disclosure of the disputed personal information, and furnish

the statement in the same manner as required when the insurer provides corrected information as outlined above (**Mass. Gen. Laws ch. 175I, § 9(d)**-(e)).

*Adverse underwriting decisions:* The IIPP law contains a variety of provisions with respect to required notices concerning adverse underwriting decisions, including notice for the reason for such decisions (**Mass. Gen. Laws ch. 175I, § 10**), restrictions on the collection of information concerning previous adverse underwriting decisions (**Mass. Gen. Laws ch. 175I, § 11**), and prohibitions on considering previous adverse underwriting decisions in making a current decision (**Mass. Gen. Laws ch. 175I, § 12**).

*Remedies:* The Commissioner of Insurance has the power to enforce the provisions of the IIPP law (**Mass. Gen. Laws ch. 175I, § 14**). For more information, see **Section II.C.** In addition, an individual remedy for persons aggrieved by a violation is provided (see **Section I.G.1.**). Finally, criminal penalties apply for knowingly obtaining personal information under false pretenses (see **Section I.H.**).

***Genetic information:*** No insurance company or officer or agent thereof may require genetic tests or genetic information as a condition on the issuance of insurance or the renewal of a policy. A violation constitutes an unfair or deceptive trade practice under the Commonwealth's consumer protection (**Mass. Gen. Laws ch. 93A, § 1**) and insurance (**Mass. Gen. Laws ch. 176D, § 1** to 14) provisions (**Mass. Gen. Laws ch. 175, § 108(H)**).

***Data breach notification law:*** Insurers that own or license data that includes "personal information" as defined under the Commonwealth's data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to insurers (see **Section I.C.6.** and **Section I.C.7.**).

**8. Retail & Consumer Products** –

***Prohibition on requiring written personal information to complete credit card or check transaction:*** No person, firm, partnership, or corporation that accepts a credit card in payment for a transaction may require that a credit card holder write personal information not required by the credit card issuer on the credit card transaction form. In addition, no such entity that accepts a check as payment for a transaction may require, as a condition of accepting the check, that the person provide a credit card number or any personal information other than a name, address, motor vehicle license number or state ID card number, and telephone number, unless certain conditions apply. For more information on these prohibitions, see **Section I.D.3.**

***Data breach notification law:*** Businesses engaged in the retail and consumer products sector that own or license data that includes "personal information" as defined under the Commonwealth's data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to businesses in the retail and consumer products sector (see **Section I.C.6.** and **Section I.C.7.**).

**9. Social Media** –

***Data breach notification law:*** Businesses engaged in the social media sector that own or license data that includes "personal information" as defined under the Commonwealth's data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to businesses in the social media sector (see **Section I.C.6.** and **Section I.C.7.**).

**10. Tech & Telecom** –

***Pending legislation:*** **S. 2053**, introduced Apr. 10, 2017, would, if enacted, require telecommunications and Internet service providers to obtain written consent from customers prior to collecting, using, disclosing, or otherwise disseminating their personal information, among other potential restrictions. For additional information on this and other proposals, see **Section IV.B.**

***Data breach notification law:*** Businesses engaged in the tech and telecommunications sector that own or license data that includes "personal information" as defined under the Commonwealth's data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (see **Section I.C.8.**).

***Data security and data disposal standards:*** Massachusetts law and regulations imposing data security and data disposal requirements on persons who own or license personal information about Massachusetts residents are applicable to businesses in the tech and telecommunications sector (see **Section I.C.6.** and **Section I.C.7.**).

***Criminal warrants issued to electronic communication service providers:*** Under Massachusetts criminal law, a warrant may be issued on probable cause to a foreign corporation providing electronic communications services to provide records that would reveal the identity of the customer, any data stored on the customer's behalf, records of customer use, and source and content information. The law further requires a Massachusetts corporation providing electronic communications services to produce records pursuant to a warrant or subpoena issued by another state (**Mass. Gen. Laws ch. 276, § 1B**).

***Electronic surveillance:*** For provisions governing communication common carriers with respect to Massachusetts's electronic surveillance law, see **Section I.F.**

**11. Other Sectors** –

Our research has revealed no specific Massachusetts law provisions applicable to other business sectors.

**F. Electronic Surveillance** –

A person who willfully intercepts, attempts to intercept, or procures another person to intercept any wire or oral communication is subject to a fine of not more than $10,000, as well as imprisonment in a state prison for not more than five years or imprisonment in a jail or house of correction for not more than 2.5 years, or to the fine and one of the two prison terms. Proof of the installation of an intercepting device evincing an intent to commit an interception not otherwise authorized by law is prima facie evidence of a violation (**Mass. Gen. Laws ch. 272, § 99(C)(1)**). Any person who willfully discloses or attempts to disclose to any person the contents of a wire or oral communication known to have been intercepted or who willfully uses or attempts to use the contents of a wire or oral communication knowing that the information was obtained through an interception is guilty of a misdemeanor punishable by imprisonment in a jail or house of correction for not more than two years or a $5,000 fine, or both (**Mass. Gen. Laws ch. 272, § 99(C)(3)**). Any person who permits or commits on behalf of another person a violation of the above prohibited acts or who participates in a conspiracy or acts as an accessory in a violation is subject to the same punishments as provided for the respective offenses (**Mass. Gen. Laws ch. 272, § 99(C)(6)**).

For purposes of each of these provisions, the term "interception" means to secretly hear or record the contents of any wire or oral communication through the use of an intercepting device by any person other than a person given prior authority by all parties to the communication, unless a law enforcement investigation exception applies (**Mass. Gen. Laws ch. 272, § 99(B)(4)**). Accordingly, Massachusetts is an "all-party consent" state.

It is not unlawful for an operator of a switchboard or an officer or employee of a communication common carrier whose facilities are used in the transmission of wire communications to intercept or use a communication in the normal course of employment while engaged in activity necessary to the rendition of such services, provided that such activities are limited to mechanical or service quality control checks. In addition, persons may possess or use an office intercommunication system used in the ordinary course of business. Additional exceptions are provided for investigative and law enforcement officers, persons authorized by warrant issued under the law, interceptions necessary to protect the safety of undercover officers, and financial institutions recording telephone communications with corporate or institutional trading partners under specified circumstances (**Mass. Gen. Laws ch. 272, § 99(D)(1)**). Disclosures are also permitted for specified law enforcement officers and in criminal proceedings. Disclosures may only be made on a showing of good cause, and any privileged information intercepted in accordance with, or in violation of, the electronic surveillance law does not lose its privileged status (**Mass. Gen. Laws ch. 272, § 99(D)(2)**).

A civil action is available for persons whose wire, electronic, or oral communications have been unlawfully intercepted (see **Section I.G.4.**).

## G. Private Causes of Action

**1. Consumer Protection** –

***General right of privacy:*** Under the Commonwealth's general right of privacy law (see **Section I.B.**), the superior court has equity jurisdiction to enforce the right to privacy and to award damages (**Mass. Gen. Laws ch. 214, § 1B**).

***Confidentiality of hospital and health facility records:*** A person whose rights to confidentiality of hospital or other health facility records are violated (see **Section I.D.9.**) may bring a civil action under **Mass. Gen. Laws ch. 231, § 60B** through **Mass. Gen. Laws ch. 231, § 60E**, the Commonwealth's malpractice law (**Mass. Gen. Laws ch. 111, § 70E**, eleventh paragraph).

***Insurance information privacy protection law:*** Under the insurance information privacy protection law (IIPP law; see **Section I.E.7.**), a person whose rights have been violated with respect to access to and correction of personal information or notice concerning an adverse underwriting decision may apply for appropriate equitable relief (**Mass. Gen. Laws ch. 175I, § 20(a)**). In addition, an insurance institution, representative, or support organization who discloses information may be liable for special and compensatory damages sustained by the aggrieved individual (**Mass. Gen. Laws ch. 175I, § 20(a)**). In any action brought under this provision, the cost of the action and reasonable attorney fees may be awarded to the prevailing party (**Mass. Gen. Laws ch. 175I, § 20(c)**). An action must be brought within three years from the date the alleged violation is or should have been discovered (**Mass. Gen. Laws ch. 175I, § 20(d)**). The remedies described above are exclusive (**Mass. Gen. Laws ch. 175I, § 20(e)**).

The IIPP law further specifies that no cause of action for defamation, invasion of privacy, or negligence may arise against any person for disclosing personal or privileged information in accordance with the law, but this immunity is not available for any person who discloses false information with malice or willful intent to injure or for any person who misidentifies an individual as the subject of information and discloses the misidentified information to others (**Mass. Gen. Laws ch. 175I, § 21**).

***Right of publicity:*** Any person whose name, portrait, or picture is used within Massachusetts for advertising purposes of for purposes of trade without the person's consent may bring a civil action to prevent and restrain such use and may recover damages for any injuries sustained as a result of the use. For more information on the right of publicity, see **Section I.E.1.**

***Do-not-call:*** A person who received more than one unsolicited telephonic sales call within a 12-month period by or on behalf of a person in violation of provisions of the Massachusetts do-not-call law (see **Section I.E.1.**) may bring an action to enjoin the violation and to recover either actual monetary damages resulting from the violation or not more than $5,000, whichever is greater (**Mass. Gen. Laws ch. 159C, § 8(b)**). The prevailing party in such an action may recover reasonable attorney fees and costs (**Mass. Gen. Laws ch. 159C, § 8(c)**). A defense to an action exists if the defendant can show that it has established and implemented reasonable procedures to effectively prevent unsolicited telephonic sales calls in violation of the do-not-call law (**Mass. Gen. Laws ch. 159C, § 9**). Proceedings generally must be brought within three years after the person knew or should have known of the violation or three years after the termination of any proceeding arising out of the same violation by the Commonwealth (see **Section II.C.**), whichever is later (**Mass. Gen. Laws ch. 159C, § 10**).

**2. Identity Theft** –

Any person who, with intent to defraud, poses as another person without the express authorization of that person and uses such person's personal identifying information to obtain or attempt to obtain money, credit, goods, services, anything of value, or any ID card or other indicator of identity or for purposes of harassing another is guilty of identity fraud punishable by a fine of not more than $5,000 or imprisonment in a house of correction for not more than 2.5 years, or both (**Mass. Gen. Laws ch. 266, § 37E(b)**). A person who, with intent to defraud, obtains personal identify information of another person without the express authorization of that person and uses the information for the above-specified purposes is guilty of identity fraud punishable by a fine of not more than $5,000 or imprisonment in a house of correction for not more than 2.5 years, or both (**Mass. Gen. Laws ch. 266, § 37E(c)**).

A person found guilty of any offense described above also must make restitution for any financial loss sustained by the victim, including costs incurred for correcting credit histories or costs in connection with any civil or administrative proceeding to satisfy any debt or other obligation of the victim, including lost wages and reasonable attorney fees (**Mass. Gen. Laws ch. 266, § 37E(d)**).

**3. Invasion of Privacy** –

Under Massachusetts law, persons have the general right against unreasonable, substantial, or serious interference with their privacy. The superior court has equity jurisdiction to enforce this right and to award damages accordingly (**Mass. Gen. Laws ch. 214, § 1B**).

**4. Other Causes of Action** –

***Genetic testing:*** A person aggrieved by a violation of provisions regarding the disclosure of genetic testing results (see **Section I.D.9.**) may bring an action in his own name, or the Attorney General may institute an action for injunctive and other equitable relief (**Mass. Gen. Laws ch. 111, § 70G(d)**).

***Lie detector tests:*** A person aggrieved by a violation of provisions prohibiting employers from requiring or conducting lie detector tests with respect to employees or applicants (see **Section I.E.6.**) may institute a civil action for injunctive relief and any damages, including treble damages for loss of wages or other benefits. Total awarded damages must be at least $500 for each violation. A prevailing person also is entitled to costs and reasonable attorney fees (**Mass. Gen. Laws ch. 149, § 19B(4)**).

***Electronic surveillance:*** A person whose oral or wire communication has been intercepted in violation of the Commonwealth's electronic surveillance law (see **Section I.F.**) has a civil cause of action against the violator and may recover actual damages, but not less than liquidated damages of $100 per day of violation or $1,000, whichever is higher, punitive damages, and a reasonable attorney fee and other litigation disbursement reasonably incurred. Good faith reliance on a warrant issued under the law is a complete defense to any civil action (**Mass. Gen. Laws ch. 272, § 99(Q)**).

**H. Criminal Liability** –

***Lie detector tests:*** A person who commits a second or subsequent violation of provisions prohibiting employers from requiring or conducting lie detector tests with respect to employees or applicants (see **Section I.E.6.**) is subject to 90 days' imprisonment, as well as civil fines (see **Section II.C.**). In the case of a corporation, the responsible individual is the president, chief operating officer, or any managerial or supervisory employee who allows or condones the violation. A waiver of the prohibition by the employee or applicant is not a defense to criminal prosecution (**Mass. Gen. Laws ch. 149, § 19B(3)**).

***Insurance information privacy protection law:*** Under the insurance information privacy protection law (IIPP law; see **Section I.E.7.**), a person who knowingly and willfully obtains information about an individual from an insurance institution, representative, or support organization under false pretenses is subject to a fine of not more than $10,000 or imprisonment for not more than one year, or both (**Mass. Gen. Laws ch. 175I, § 2**).

***Identity fraud:*** See **Section I.G.2.**

## II. REGULATORY AUTHORITIES AND ENFORCEMENT

**A. Attorney General** –

The Massachusetts **Attorney General** has authority to enforce the primary provisions of Massachusetts law regarding privacy and data security, including the data breach notification law (see **Section I.C.8.**), laws governing data disposal requirements (see **Section I.C.7.**), and do-not-call provisions (see **Section I.E.1.**), among others. However, the primary responsibility for oversight with respect to these laws lies with the **Office of Consumer Affairs and Business Regulation**.

**B. Other Regulators** –

The Massachusetts **Division of Insurance** is responsible for enforcing the Commonwealth's insurance information privacy protection law (IIPP law; see **Section I.E.7.**).

**C. Sanctions & Fines** –

***Data breach notification law:*** The Attorney General is authorized to bring an action to remedy violations of the data breach notification law (see **Section I.C.8.**) and for other appropriate relief (**Mass. Gen. Laws ch. 93H, § 6**). The Attorney General may seek a temporary restraining order or temporary or permanent injunction. In addition to granting such relief, the court may make an order or judgment necessary to restore to any person who has suffered an ascertainable loss by reason of the violation any moneys or property that may have been acquired as a result of the violation. Finally, if the court finds that a person has knowingly violated the data breach notification law, it may impose a civil penalty of not more than $5,000 for each violation, together with reasonable costs of investigation and litigation, including reasonable attorney fees (**Mass. Gen. Laws ch. 93A, § 4**).

***Data disposal requirements:*** Any agency or person who violates requirements governing the proper disposal of records containing personal information (see **Section I.C.7.**) is subject to a civil fine of not more than $100 per data subject affected, to a maximum of $50,000 for each instance of improper disposal. The Attorney General may file a civil action to recover the penalty (**Mass. Gen. Laws ch. 93I, § 2**, third paragraph). The Attorney General also may bring an action under the provisions of **Mass. Gen. Laws ch. 93A, § 4**, which may include a temporary restraining order or temporary or permanent injunction, an order or judgment necessary to restore to any person who has suffered an ascertainable loss by reason of the violation any moneys or property that may have been acquired as a result of the violation, or, for a knowing violation, the imposition of a civil penalty of not more than $5,000 for each violation, together with reasonable costs of investigation and litigation, including reasonable attorney fees (**Mass. Gen. Laws ch. 93I, § 3**).

***Insurance information privacy protection law:*** Under the insurance information privacy protection law (IIPP law; see **Section I.E.7.**), the Commissioner of Insurance may issue a statement of charges to any insurance institution, agent, or support organization in the event he believes there has been a violation of the law's provisions. The date of a hearing must be not less than 21 days from the date of service of the statement. At the hearing, the insurance institution, representative, or support organization may present evidence. The law specifies the Commissioner's power to call witnesses, power to require production, and other procedural powers, as well as the requirements for service of process (**Mass. Gen. Laws ch. 175I, § 15**). Specific process service requirements apply to foreign insurance support organizations (**Mass. Gen. Laws ch. 175I, § 16**).

After a hearing, if the Commissioner finds that an insurance institution, representative, or support organization has violated the provisions of the IIPP law, it may put the findings in writing and deliver them to the violating party along with a cease-and-desist order. Similarly, if the Commissioner finds that no violation has occurred, it must prepare a written report and deliver it to the charged party. The Commissioner may modify or set aside a report or order as issued above until the expiration of the time period for filing a petition for review (see below) or until such a petition is actually filed. After the time period for filing a petition for review has expired, if no such petition has been filed, the Commissioner may alter, modify, or set aside its order whenever conditions warrant (**Mass. Gen. Laws ch. 175I, § 17**).

In addition to issuing a cease-and-desist order, the Commissioner may order payment of a monetary penalty of not more than $1,000 for each violation, provided that any penalty assessed against an insurance representative may not exceed $10,000 and any penalty assessed against an insurance institution or support organization may not exceed $50,000, in the aggregate for multiple violations. In addition, a person violating a cease-and-desist order is subject to a monetary fine of not more than $10,000 for each violation, a fine of not more than $50,000 if the Commissioner determines that the violation has occurred with a frequency sufficient to constitute a general business practice, or the suspension or revocation of the insurance institution's or representative's license (**Mass. Gen. Laws ch. 175I, § 18**).

The law provides for petitions for review of orders issued pursuant to the above-described provisions both for persons subject to the order and for persons whose rights were violated. In general, a petition must be filed in the Supreme Judicial Court within 20 days after the date of service of the order. The law provides for procedural requirements with respect to such petitions (**Mass. Gen. Laws ch. 175I, § 19**).

***Prohibition on requiring written personal information to complete credit card transaction or for acceptance of a check:*** A violation of prohibitions applicable to specified entities who accept credit cards or checks with respect to requiring the recording of personal information as a condition of the transaction (see **Section I.C.3.**) is deemed to be an unfair and deceptive trade practice, and individuals aggrieved by such violation may inform either the Office of Consumer Affairs and Business Regulation or the Attorney General. Under the Commonwealth's consumer protection law, the Attorney General may bring an action that may include a temporary restraining order or temporary or permanent injunction, an order or judgment necessary to restore to any person who has suffered an ascertainable loss by reason of the violation any moneys or property that may have been acquired as a result of the violation, or, for a knowing violation, the imposition of a civil penalty of not more than $5,000 for each violation, together with reasonable costs of investigation and litigation, including reasonable attorney fees (**Mass. Gen. Laws ch. 93A, § 4**).

***Genetic testing:*** A violation of provisions governing the disclosure of genetic testing information (see **Section I.D.9.**) is deemed to be an unfair business trade or practice, and the Attorney General may institute an action for injunctive and other equitable relief (**Mass. Gen. Laws ch. 111, § 70G(d)**).

***Do-not-call:*** The Attorney General may bring proceedings related to the knowing violation of provisions of the Massachusetts do-not-call law (see **Section I.E.1.**). Remedies may include an injunction, a civil penalty of not more than $5,000 per knowing violation (but not less than $1,500 per knowing violation with respect to a person age 65 or over), and additional relief (**Mass. Gen. Laws ch. 159C, § 8(a)**). A defense to an action exists if the defendant can show that it has established and implemented reasonable procedures to effectively prevent unsolicited telephonic sales calls in violation of the do-not-call law (**Mass. Gen. Laws ch. 159C, § 9**). Proceedings generally must be brought within three years after the Attorney General knew or should have known of the violation (**Mass. Gen. Laws ch. 159C, § 10**).

***Access to and correction of personnel records:*** Violations of labor law provisions regarding employee access to and correction of personnel records (see **Section I.E.6.**) are subject to a fine of not less than $500 nor more than $2,500, levied by the Attorney General (**Mass. Gen. Laws ch. 149, § 52C**, ninth paragraph).

***Lie detector tests:*** A person who violates provisions prohibiting employers from requiring or conducting lie detector tests with respect to employees or applicants (see **Section I.E.6.**) is subject to a fine of not more than $1,000 but not less than $300. A second or subsequent violation is subject to a fine of not more than $1,500 or 90 days' imprisonment, or both. In the case of a corporation, the responsible individual is the president, chief operating officer, or any managerial or supervisory employee who allows or condones the violation. A waiver of the prohibition by the employee or applicant is not a defense to civil liability or criminal prosecution (**Mass. Gen. Laws ch. 149, § 19B(3)**).

**D. Representative Enforcement Actions**

**1. Copley Advertising** –

Massachusetts Attorney General Maura Healey reached a settlement, filed Apr. 4, 2017, with a digital advertising company, Copley Advertising LLC, that allegedly used mobile "geofencing" technology to send targeted ads to mobile devices when they enter a particular geographic area. Copley's technology enabled it to "tag" mobile devices near abortion providers and to serve ads from organizations that offer alternatives to abortion. Although Copley had not geofenced clinics in Massachusetts, the Attorney General concluded that such conduct, were it to occur in Massachusetts, would constitute an unfair and deceptive trade practice "because it intrudes upon a consumer's private health or medical affairs or status and/or results in the gathering or dissemination of private health or medical facts about the consumer without his or her knowledge or consent." Copley agreed to enter into an **Assurance of Discontinuance** "in order to avoid the time, expense, and uncertainty of litigation."

**2. Boston Children's Hospital** –

In December of 2014, Boston Children's Hospital (BCH) agreed pay $40,000 and takes steps to prevent future security violations in order to settle state allegations related to the 2012 loss of a physician's hospital-issued laptop containing unencrypted patient information. Under the terms of a **consent judgment** filed in Suffolk County Superior Court, the hospital will pay a $30,000 civil penalty and contribute $10,000 to a state-run data protection education fund.

**3. TD Bank** –

In December of 2014, TD Bank NA **agreed** to pay $825,000 and take steps to strengthen its security practices after a set of backup tapes containing the personal information of more than 260,000 individuals nationwide went missing and the bank allegedly delayed notifying the state and those affected by the incident. The Massachusetts Attorney General's Office said in a statement that the bank has been credited $200,000 to reflect the security measures and upgrades it had already taken following the incident.

**4. Equifax** –

On Sept. 19, 2017, Massachusetts Attorney General Maura Healey filed the **first enforcement action** in the nation concerning the data breach by Equifax, Inc. that compromised the personal information of as many as 3 million Massachusetts residents. In a **press release** announcing the action, the Attorney General noted that the suit is designed to hold Equifax accountable, make Massachusetts residents whole, and require measures to prevent a breach from occurring again.

For additional information, see **Section IV.C.**

**5. Yapstone Holdings** –

On Dec. 19, 2018, Attorney General Maura Healey **announced** a settlement with Yapstone Holdings Inc., a California-based payment processing company alleged to have exposed the personal information of 6,800 Massachusetts residents online. Yapstone agreed to pay $155,000 to resolve the allegations. In an**assurance of discontinuance** filed in Suffolk Superior Court, the company also agreed to comply with state laws and implement policies to improve the security of its systems and protect sensitive consumer data online.

**E. State Resources** –

The Office of Consumer Affairs and Business Regulation (OCABR) recently posted its data breach notification archive **online**. Reports are available from 2007 through 2017. According to a **press release** announcing the posting, the OCABR noted that the archive is a public record that all parties should be able to view without going through a public records request. Additional information on data breach notifications, including submission forms, is available on the OCABR **website**. Finally, in a recent **press release**, the OCABR encouraged all business owners to have cybersecurity plans in place designed to adequately protect personal information, with links to webpages for business owners and consumers.

The OCABR has also posted a **consumer guide to stopping junk mail and spam**, as well as information on the Commonwealth's **do-not-call registry**, including a link allowing consumers to register.

The Massachusetts Attorney General has a selection of information available to consumers and businesses on its website, including pages on **financial crime and identity theft**.

The Massachusetts Department of Elementary and Secondary Education provides **information** on access to student records by parents and students, including frequently asked questions and a summary of the Commonwealth's student record regulations, which are discussed in detail at **Section I.E.2.**

**III. RISK ENVIRONMENT** –

Massachusetts' Attorney General has long been active in pursuing data breach actions. Indeed, the Massachusetts Attorney General led the **interstate action against TJX Companies**, a retailer based in Massachusetts who in 2006 suffered the first major consumer data breach when hackers stole data of 45 million transactions, including credit and debit card information. In 2007, in the wake of this massive data breach, the Massachusetts legislature enacted M.**G.L. c. 93H**: "Security Breaches" (**Mass. Gen. Laws ch. 93H, § 1** through **Mass. Gen. Laws ch. 93H, § 6**). Chapter 93H defines personal information, and requires the state and affected parties to be notified in the event of a security breach or unauthorized usage of personal information. At the time it was passed, the new law was widely considered among the toughest data security laws in the nation. Also in 2009, the Office of Consumer Affairs and Business Regulation implemented **201 CMR 17.00** as a complement to Chapter 93H to further protect the Commonwealth's residents' personal information (**201 CMR 17.01** to **201 CMR 17.05**). **201 CMR 17.00**requires organizations to establish written information security plans and to take other proactive steps to protect personal data.

**A. Attorney General's Enforcement Actions** –

Chapter 93H and other consumer protection statutes grant the Massachusetts Attorney General the power to enforce the Commonwealth's privacy laws. The Attorney General's office has staff dedicated to this task, and has brought several notable cases, including:

• **Equifax (2018):** In September of 2017, Equifax announced that the personal information of nearly 143 million people, including up to 3 million Massachusetts residents, may have been compromised. Following the announcement, the Massachusetts Attorney General filed the nation's **first enforcement action**against the company for its failure to maintain appropriate safeguards to protect consumer data in violation of Massachusetts consumer protection and data privacy laws. The matter is currently ongoing.

• **Multi-State Billing Services (2017):** Attorney General obtained a **judgment**against Medicaid billing company that provided processing services for Massachusetts public school districts after a data breach put more than 2,600 Massachusetts children at risk of identity theft and fraud. The company had to pay $100,000 and implement improved security practices.

• **TD Bank (2014):** After losing unencrypted back-up tapes containing personal information for almost 100,000 Massachusetts customers, and delaying providing notice of the incident to the Attorney General's office, TD Bank **agreed to pay**$625,000 and strengthen its security practices.

• **Boston Children's Hospital (2014):** BCH **agreed to pay** $40,000 and take steps to prevent future security violations following the theft of a physician's BCH-issued laptop that contained protected health information of over 2,000 BCH patients.

• **Beth Israel Deaconess Medical Center (2014):** Under a 2014 **consent agreement**, the Beth Israel Deaconess Medical Center (BIDMC) in Boston agreed to pay $100,000 after an unauthorized person allegedly gained access to a physician's unlocked office on campus and stole an unencrypted personal laptop sitting unattended on a desk. The laptop was not hospital-issued but was used by the physician with BIDMC's knowledge and authorization on a regular basis. The laptop contained the protected health information of 3,796 patients and employees as well as the personal information of 194 Massachusetts residents.

• **Women and Infants Hospital (2014):** Women & Infants Hospital of Rhode Island (WIH) **agreed to pay** $150,000 to resolve allegations that it failed to protect the personal and protected health information of more than 12,000 patients in Massachusetts following WIH's realization that it was missing 19 unencrypted back-up tapes from two diagnostic centers, one in Massachusetts. Due to an inadequate inventory and tracking system, WIH allegedly did not discover the tapes were missing until the next year.

• **South Shore Hospital (2012):** The hospital **agreed to pay** $750,000 to resolve allegations that it failed to protect confidential health information of more than 800,000 consumers. South Shore Hospital shipped three boxes containing 473 unencrypted back-up computer tapes with personal and protected health information off-site to be erased at a data center. It took the data center six months to realize that only one of the boxes arrived at its destination. The hospital agreed to take steps to ensure compliance with state and federal data security laws and regulations as well as the above-mentioned fine.

The Commonwealth has participated in other noteworthy initiatives including the Attorney General joining a multi-state **amicus brief** in support of the respondent filed in *Spokeo, Inc. v. Robbins*, 578 U.S. __, **136 S. Ct. 1540** (2016), a case before the Supreme Court regarding the harms of firms selling false personal data. Additionally, in 2015, the Attorney General testified about proposed federal legislation that would undermine Massachusetts data breach laws. The Attorney General has also been involved in multistate litigation including the following:

• **Nationwide Mutual Insurance Company (2017):** $100,000 of **$5.5 million judgment** awarded to Massachusetts.

• **Target (2017):** $625,000 awarded to Massachusetts of **$18 million nationwide settlement**.

• **Adobe (2016):** $100,000 of **$1 million award** awarded to Massachusetts.

• **RadioShack (2015):Agreement** with RadioShack that limited its new owner, General Wireless Operations, Inc., from gaining access to or transferring customer data such as credit or debit card information, social security numbers, telephone numbers or dates of birth.

**B. Private Party Litigation** –

Massachusetts is not a hotbed for private data security enforcement actions. Indeed, it is not clear whether Chapter 93H creates a private right of action. In *Katz v. Pershing, LLC*, **806 F. Supp. 2d 452**, 458 (D. Mass. 2011), the district court clearly stated that the statute empowers only the Attorney General to bring action against companies for failure to notify of a breach ("[T]he power to enforce Chapter 93H is limited to the State Attorney General–the statute does not incorporate or otherwise authorize a private right of action."). On appeal, however, the 1st Circuit left the issue unresolved, stating that "The district court held that a cause of action for a violation of Chapter 93H can be brought only by the Attorney General. We do not decide that question today." *Katz v. Pershing, LLC*, **672 F.3d 64**, 78 (1st Cir. 2012).

Even if 93H does not create a private right of action, there are other grounds to bring tort claims in the wake of a data breach. Under Massachusetts state tort law, a risk of unauthorized use or disclosure of protected patient health information may be treated as an injury sufficient to establish standing. *Walker v. Boston Med. Ctr. Corp.*, **33 Mass. L. Rptr. 179**, **2015 BL 450571** (Mass. Super. 2015). In *Walker*, Plaintiffs brought suit against Boston Medical Center after receiving a letter from the hospital that their medical records might have been inadvertently exposed to unauthorized viewers. The Massachusetts Superior Court allowed plaintiff's claims to proceed under a "risk of injury" theory of standing because a "real and immediate risk" of injury may be enough for standing. The court noted that "the Massachusetts standard for recognizing standing appears to be more liberal [than other jurisdictions, citing N.J.], allowing standing when there is a risk of harm. How 'real and immediate' the risk of harm is should be evaluated when the facts surrounding the data breach, including the quantity and nature of access to the records, are presented after discovery." The court concluded that the plaintiff's general allegations of injury from the data breach was sufficient at the pleadings stage.

**C. Pending Legislation on Biometric Information** –

As of May 2019, the Massachusetts Senate has been contemplating legislation that would be enforceable both through a private right of action, and by the Attorney General, if their personal information or biometric information[1] is improperly collected. Under the proposed Act Relative to Consumer Data Privacy (**S. 120**), businesses, however, can disclose personal information of their employees so long as the business is collecting or disclosing such information within the scope of its role as an employer. For a business's violation of the Act, a customer could recover a) damages in an amount not greater than $750 per consumer per incident or actual damages, whichever is greater; b) an injunctive or declaratory relief; and c) reasonable attorney fees and costs. Additionally, the Attorney General may seek a civil penalty of not more than $2,500 for each violation or $7,500 for each intentional violation.

[1] The Bill defines biometric information as an individual's physiological, biological or behavioral characteristics including an individual's DNA that can be used, singly or in combination with each other or with other identifying data, to establish individual identity.

**D. Other Relevant Information** –

Since 2007, the Commonwealth's **Office of Consumer Affairs and Business Regulation** issues an annual 'Data Breach Report' (available **here**). The report consists of information regarding data breaches from that year including whether the breach was electronic or via paper document, the number of Massachusetts residents affected, whether credit card or driver's license numbers were compromised, and other information. Each report contains information about hundreds or thousands of breaches affecting residents of the Commonwealth.

**IV. EMERGING ISSUES AND OUTLOOK**

**A. Recent Legislation**

**1. Security Breaches** –

**Chapter 444 of the Acts of 2018**, signed Jan. 10, 2019, effective Apr. 11, 2019, imposes new requirements on the content of a breach notification to be provided to the attorney general, the director of consumer affairs, and consumer reporting agencies, including the following:

- the nature of the breach of security or unauthorized acquisition or use;
- the number of residents of the commonwealth affected by such incident at the time of notification;

• the name and address of the person or agency that experienced the breach of security;

• name and title of the person or agency reporting the breach of security, and their relationship to the person or agency that experienced the breach of security;

• the type of person or agency reporting the breach of security;

• the person responsible for the breach of security, if known;

• the type of personal information compromised, including, but not limited to, social security number, driver's license number, financial account number, credit or debit card number or other data;

• whether the person or agency maintains a written information security program; and

• any steps the person or agency has taken or plans to take relating to the incident, including updating the written information security program.

Moreover, notice to a resident must also include:

• the resident's right to obtain a police report;

• how a resident may request a security freeze and the necessary information to be provided when requesting the security freeze;

• that there shall be no charge for a security freeze; and

• mitigation services to be provided.

The law also requires a person who experienced a breach to file a report with the attorney general and the director of consumer affairs and business regulation certifying that their credit monitoring services comply with other provisions.

**2. Confidential Information** –

**Chapter 337 of the Acts of 2018**, signed Dec. 28, 2018, which pertains to the regulation of short-term rentals, requires the executive office of housing and economic development to establish procedures and protocols to protect the confidentiality and security of an operator's personal information and tax information and prohibits the disclosure of such information.

**Chapter 205 of the Acts of 2018**, signed Aug. 9, 2018, which establishes programs for automatically registering eligible voters, requires the state secretary to adopt regulations governing the collection and transmission of personal information, in particular requiring automatic voter registration agencies to, among other things, (a) implement measures, such as encryption, to secure information in order to prevent security breaches and the unauthorized use of personal information, (b) implement measures for reporting security breaches or the unauthorized use of personal information; and (c) provide protections against disclosure of confidential information, including home addresses.

**3. Health care payment information** –

**Chapter 63 of the Acts of 2018**, signed Mar. 30, 2018, amends **Mass. Gen. Laws ch. 176O, § 27** to ensure the confidentiality of health care payment information. The law requires the Division of Insurance to develop summary of payments forms to be used by all carriers that may be exchanged securely through electronic means. Carriers may allow an individual to receive summary of payments forms by non-electronic means, provided the individual clearly states in writing that the disclosure of all or part of the information could endanger the individual or the insured member. The law also prohibits carriers from specifying or describing sensitive health care services in a common summary of payments form. Effective Jun. 28, 2018.

**B. Proposed Legislation (191st General Court, 2019-2020)**

**1. Security Breaches** –

**SD 427**, introduced Jan. 14, 2019, would add biometric indicators to the definition of "personal information" under **Mass. Gen. Laws Ch. 93H, § 1**.

**SD 715**, introduced Jan. 16, 2019, would add "date of birth" to the definition of "personal information."

**SD 942**, introduced Jan. 17, 2019, would amend the breach notification law to include a requirement that the breach "creates a substantial risk of identity theft or fraud." It would also amend the statute by adding additional requirements to the content of the notice, such as the resident's right to obtain a police report and how a resident may request a security freeze.

**2. Financial Information** –

**SD 606**, introduced Jan. 16, 2019, would prohibit an entity that accepts an access device in connection with a transaction from retaining the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, more than 48 hours after authorization of the transaction. Furthermore, whenever there is a breach of the security of the system, the entity would be required to reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders. The measure would also authorize the attorney general to bring an action for violations.

**3. Net Neutrality and Consumer Protection** –

**SD 603**, introduced Jan. 16, 2019, in pertinent part calls for the establishment of standards for a Massachusetts Net Neutrality and Consumer Privacy Seal that shall allow an internet service provider to demonstrate, among other things, that it provides customers with a mechanism to easily opt-out of third-party access to customer proprietary information for purposes other than the provision of broadband internet access service from which that customer proprietary information was derived.

**4. Cybersecurity of IoT Devices and Autonomous Vehicles** –

**SD 612**, introduced Jan. 16, 2019, would authorize the department of consumer affairs to adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth, any person that manufactures any IOT device that collects personal information or IOT personal data about a resident of the commonwealth, and any person that manufactures any autonomous vehicle that uses or incorporates an IOT device in the vehicle that collects personal information or IOT personal data about a resident of the commonwealth. Such regulations shall be designed to safeguard the personal information and IOT personal data of residents of the commonwealth and shall be consistent with the safeguards for protection set forth in the federal regulations by which the person is regulated.

**5. Consumer Data Privacy** –

**SD 341**, introduced Jan. 12, 2019, would require a business that collects a consumer's personal information to provide at or before the point of collection a notice that contains various elements and would grant consumers the right to request certain information from the business. The measure would grant the consumer a private right of action against a business that violates the provisions, and would empower the attorney general to adopt regulations and pursue enforcement.

**6. Biometric Surveillance Systems** –

**SD 671**, introduced Jan. 16, 2019, would establish a moratorium on face recognition and other remote biometric surveillance systems.

**7. Medical Records** –

**SD 122**, introduced Jan. 10, 2019, would clarify and enhance privacy protections for electronic health records.

**C. Past Proposals**

**1. 190th General Court, 2017-2018** –

***Security Breaches:*** **H. 2814**, introduced Jan. 23, 2017, would have amended certain provisions pertaining to data security breaches and would have created a special commission on cybersecurity to assess the various threats across the Commonwealth. Consumer Protection and Professional Licensure.

**S. 95** and **H. 1985**, both introduced Jan. 23, 2017, would have added biometric indicators to the definition of "personal information."

***Broadband Privacy:*** **S. 2610**, introduced Jul. 17, 2018, would have promoted net neutrality and consumer protection. The bill would also have established standards for a Massachusetts Net Neutrality and Consumer Privacy Seal that would allow an Internet service provider to demonstrate that it, among other things, provides customers with a mechanism to easily opt-out of third-party access to customer proprietary information for purposes other than the provision of broadband Internet access service from which that customer proprietary information was derived.

**S. 2376**, filed Mar. 23, 2018, included a **report** of the Special Senate Committee on Net Neutrality, which responded to the federal government's decision to repeal rules on net neutrality. The report also addressed issues related the broadband privacy and proposes legislation on that topic.

**S. 2062**, introduced Apr. 18, 2017, would have prohibited an internet service provider from collecting, using, disclosing, or permitting third-party access to a customer's proprietary information without customer approval, with a few exceptions.

**S. 2053**, introduced Apr. 10, 2017, would have prohibited a telecommunications or internet service provider from collecting, using, disclosing, or otherwise disseminating personal information from a customer resulting from the customer's use of the telecommunications or internet service provider without express written approval from the customer.

**H. 3698**, introduced Apr. 27, 2017, would have prohibited an internet service provider from collecting, using, disclosing, or permitting access to sensitive customer proprietary information, with a few exceptions.

**H. 3766**, introduced Apr. 13, 2017, would have prohibited certain telecommunications or internet service providers from collecting personal information from customers without express written approval.

***Financial Information Privacy:*** **S. 149**, introduced Jan. 23, 2017, would have prohibited persons and entities conducting business in Massachusetts that accept a financial access device such as a credit or debit card in a transaction from maintaining information on security codes or magnetic strip information subsequent to the completion of the transaction or, in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. The legislation would have further provided for reimbursement to financial institutions when a person or entity suffers a breach of security for the reasonable costs incurred by the financial institution in response to the breach, including costs of cancellation or reissuance of access devices and closures of accounts.

**S. 116**, introduced Jan. 23, 2017, would have established the Massachusetts Financial Information Privacy Act. This law would have added a new chapter to the Commonwealth's Trade Regulation title that would prohibit financial institutions from selling, sharing, transferring, or otherwise disclosing nonpublic personal information to nonaffiliated third parties without customer consent, unless an exception applies. The proposed legislation also provided for civil penalties for violations.

***Social Media:*** **S. 991** and **H. 158**, both introduced Jan. 23, 2017, would prohibit employers and certain educational institutions from requiring an employee or student to disclose a username or password to a personal social media account or taking adverse action against an employee or student for refusing to provide such access. The Senate Ways and Means Committee recommended a new draft of the bill (**S. 2320**) on Mar. 1, 2018, which was subsequently amended as **S. 2346** on Mar. 21, 2018.

**S. 991** and **H. 158**, both introduced Jan. 23, 2017, would prohibit employers and certain educational institutions from requiring an employee or student to disclose a username or password to a personal social media account or taking adverse action against an employee or student for refusing to provide such access. The Senate Ways and Means Committee recommended a new draft of the bill (**S. 2320**) on Mar. 1, 2018, which was subsequently amended as **S. 2346** on Mar. 21, 2018.

**H. 253**, introduced Jan. 23, 2017, would prohibit school districts from requiring, requesting, or causing student to disclose usernames and passwords to a personal social media account.

Medical Records: **S. 2573**, introduced Jun. 21, 2018, would establish the Honorable Peter V. Kocot Act to enhance access to high quality, affordable, and transparent healthcare in the commonwealth, an act which includes provisions detailing the security of medical records.

**H. 4593**, introduced Jun. 11, 2018, would improve medical decision making by, among other things, establishing that a surrogate decision maker for an incapacitated person shall have the same right as the person to receive medical information and medical records and consent to disclosure.

***Confidential Information:***

**S. 2598**, introduced Jul. 12, 2018, would strengthen laws combating human trafficking and protecting survivors of modern-day slavery, including a provision to establish regulations regarding the collection of human trafficking crime data and ensuring the protection of confidential information, such as victims' identifying information.

**D. Other Issues**

**1. Equifax Breach** –

On Sept. 19, 2017, Massachusetts Attorney General Maura Healey filed the **first enforcement action** in the nation concerning the data breach by Equifax, Inc. that compromised the personal information of as many as 3 million Massachusetts residents. In a **press release** announcing the action, the Attorney General noted that the suit is designed to hold Equifax accountable, make Massachusetts residents whole, and require measures to prevent a breach from occurring again.

The complaint alleges that Equifax violated state privacy laws because it didn't employ reasonable security measures to protect consumer data. The complaint also asserts that Equifax failed to disclose the breach in a timely manner. The attorney's general office is seeking civil penalties, restitution, administrative costs, and attorney's fees.

**2. Proposed Federal Legislation** –

In March 2018, Massachusetts Attorney General Maura Healey joined other attorneys general in a **letter** sent to U.S. House of Representatives committee leaders regarding the **proposed Data Acquisition and Technology Accountability and Security Act**, stating that Congress should not preempt state data security and breach notification laws.

**3. Facebook/Cambridge Analytica** –

In March 2018, Massachusetts Attorney General Maura Healey joined other attorneys general in a **letter** sent to Facebook CEO Mark Zuckerberg, asking questions about data-sharing procedures that led to the alleged use of 50 million users' data without their consent by Cambridge Analytica. The National Association of Attorneys General seeks information about how the company will make privacy policies and terms of service clearer and more understandable; what controls the company has over data given to developers; what safeguards are in place to police these activities; and what kinds of user data the social media giant knew Cambridge Analytica was accessing and using, and when.

Facebook sent a detailed **response** to the National Association of Attorneys General on May 7, 2018, that outlines the company's policies and practices regarding user data, the facts related to the misuse of data, and the steps Facebook is taking to address the incident and prevent any recurrence.