Publications
June 01, 2014
SECURITY BREACH NOTIFICATION CHART - Massachusetts

Mass. Gen. Laws 93H § 1 ***et seq.***

201 C.M.R. 17.00

H.B. 4144 (signed into law August 3, 2007)

Effective October 31, 2007

H.B. 4806 (signed into law on January 10, 2019)

Effective April 11, 2019

Application. A natural person, legal entity, or any MA government agency (collectively, Entity) that owns, licenses, maintains, or stores data that includes PI about a resident of MA.

Security Breach Definition. An unauthorized acquisition or unauthorized use of unencrypted data or encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of PI, maintained by an Entity that creates a substantial risk of identity theft or fraud against a MA resident.

- A good-faith but unauthorized acquisition of PI by an Entity, or employee or agent thereof, for the lawful purpose of such Entity, is not a breach of security unless the PI is used in an unauthorized manner or subject to further unauthorized disclosure.
- **Note:** Notification obligations apply to a Breach of Security ***OR*** acquisition or use without authorization.

Notification Obligation. An Entity that owns or licenses the data shall provide notice to the affected residents, when the Entity knows or has reason to know of (i) a breach of security, **OR** (ii) that the PI of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose.

Attorney General/State Agency Notification. When notice is provided to a MA resident, notice must be provided to both the state Attorney General and the director of Consumer Affairs and Business Regulation.

The notice shall include, but not be limited to:

- the nature of the breach of security or unauthorized acquisition or use;
- the number of residents of MA affected by such incident at the time of notification;
- the name and address of the person or agency that experienced the breach of security;
- the 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.

A person who experienced a breach of security shall file a report with the attorney general and the director of consumer affairs and business regulation certifying their credit monitoring services comply with the law's requirements for providing credit monitoring to individuals if social security numbers are affected.

Note that both agencies currently promulgate online forms containing the required information.

- Upon receipt of notice, the director of consumer affairs and business regulation shall report the incident publicly on its website and make available electronic copies of the sample notice sent to consumers on its website.
- Upon receipt of notice, the director of consumer affairs and business regulation shall identify any relevant consumer reporting agency or state agency and forward the names of the identified consumer reporting agencies and state agencies to the notifying Entity. The Entity shall, as soon as practicable and without unreasonable delay, also provide notice to consumer reporting agencies and state agencies identified by the director of consumer affairs and business regulation.

Third-Party Data Notification. An Entity that maintains or stores, but does not own or license data that includes PI about a resident of MA, shall provide notice, as soon as practicable and without unreasonable delay, when such Entity (i) knows or has reason to know of a breach of security or (ii) when the Entity knows or has reason to know that the PI of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the owner or licensor.

Such Entity shall cooperate with the owner or licensor of such PI. Cooperation shall include, but not be limited to (i) informing the owner or licensor of the breach of security or unauthorized acquisition or use, (ii) the date or approximate date of such incident and the nature thereof, and (iii) any steps the Entity has taken or plans to take relating to the incident, except that such cooperation shall not be deemed to require the disclosure of confidential business information or trade secrets, or to provide notice to a resident that may not have been affected by the breach of security or unauthorized acquisition or use.

Timing of Notification. The notification shall be given as soon as practicable and without unreasonable delay following discovery of the breach. Entities cannot delay notification "on the grounds that the total number of residents affected is not yet ascertained."

Personal Information Definition. A resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relates to such resident:

- Social Security number;
- Driver's license or state-issued identification card number; or
- Financial account number or credit card number, with or without any required security code, access code, personal ID number, or password, that would permit access to a resident's financial account.

PI does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Notice Required. Notice provided to the resident shall not include the nature of the breach or unauthorized acquisition or use of the number of residents of MA affected by said breach or unauthorized access or use. It must, however, 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 pursuant to this chapter.

If the person or agency that experienced a breach of security is owned by another person or corporation, the notice to the consumer shall include the name of the parent or affiliated corporation.

Notice may be provided by one of the following methods:

- Written notice; or
- Electronic notice, if notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 (E-Sign Act).

Credit Monitoring. An Entity that experiences an incident requiring notice and involving social security numbers shall provide credit monitoring services at no cost to such affected residents for a period of not less than 18 months. The Entity shall provide all information necessary for enrollment and shall include information on how the resident may place a security freeze.

Substitute Notice Available. If the Entity required to provide notice demonstrates that the cost of providing written notice will exceed $250,000, or that the affected class of MA residents to be notified exceeds 500,000 residents, or the Entity does not have sufficient contact information to provide notice. Substitute notice shall consist of all of the following:

- Email notice, if the Entity has email addresses for the members of the affected class of MA residents;
- Clear and conspicuous posting of the notice on the home page of the Entity's website, if the Entity maintains one; and
- Publication in or broadcast through media that provide notice throughout MA.

Exception: Compliance with Other Laws.

- **Primary Regulator.** Notification pursuant to laws, rules, regulations, guidance, or guidelines established by an Entity's primary or functional state or federal regulator is sufficient for compliance if (a) notice is provided to affected Massachusetts residents in accordance with the maintained or required procedures when a breach occurs; and (b) the Entity also notifies the attorney general and the director of the office of consumer affairs and business regulation.

Other Key Provisions:

- **Delay for Law Enforcement.** Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and has notified the Attorney General, in writing, thereof and informs the Entity of such determination. Notice required by the statute must be made without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation. The Entity shall cooperate with law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided, however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.
- **Attorney General Enforcement.** Penalties include civil penalties, damages, and injunctive relief.