



MAURA HEALEY
GOVERNOR

KIMBERLEY DRISCOLL
LIEUTENANT GOVERNOR

COMMONWEALTH OF MASSACHUSETTS

Office of Consumer Affairs and Business Regulation

501 Boylston Street, Suite 5100, Boston, MA 02116

(617) 973-8700 FAX (617) 973-8799

www.mass.gov/consumer

YVONNE HAO
SECRETARY OF ECONOMIC
DEVELOPMENT

LAYLA D'EMILIA
UNDERSECRETARY

Frequently Asked Questions Regarding Data Breach Notifications and Changes to the Data Breach Notification Law, M.G.L. Chapter 93H, through Chapter 444 of the Acts of 2018.

1. Q: What is the effective date of this law?

A: It was signed by the Governor on January 10, 2019 and takes effect 90 days later on April 10, 2019.

2. Q: Where can I find the new law?

A: Here is the link: <https://malegislature.gov/Laws/SessionLaws/Acts/2018/Chapter444>

3. Q: What is the current law?

A: Chapter 93H required that *a person or agency that owns or licenses data that includes personal information about a resident of the commonwealth, shall provide notice, as soon as practicable and without unreasonable delay, when such person or agency (1) knows or has reason to know of a breach of security or (2) when the person or agency knows or has reason to know that the personal information of such resident was acquired or used by an unauthorized person or used for an unauthorized purpose, to the Attorney General, to the Office of Consumer Affairs and Business Regulation (OCABR) and to the affected resident(s).*

The notice to be provided to the Attorney General and the OCABR must include, but not be limited to, 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**, and **any steps the person or agency has taken or plans to take relating to the incident.**

4. Q: What changes were made by Chapter 444 of the Acts of 2018 which amends Chapter 93H?

A: Beginning April 10, 2019, the notice provided to the Attorney General and the OCABR must include, in addition to the **nature of the breach and number of MA residents**, the following information:

- 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;
- 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 WISP (written information security program); and
- any steps the person or agency has taken or plans to take relating to the incident, **including whether they have updated the written information security program.**

5. Q: If the Social Security number of a MA resident has been compromised by the data breach that is being reported, what additional steps does the person or agency that experienced the breach have to take?

A: Under the new section 3A that was added to Chapter 93H, if a Social Security number of a MA resident has been compromised, the person or agency that experienced the breach must offer free credit monitoring services to the MA residents for 18 months through a third party vendor. If the person or agency that has experienced a breach of security is a consumer reporting agency, then the consumer reporting agency must offer free credit monitoring services to the MA residents for at least 42 months through a third party vendor.

6. Q: If a MA resident's Social Security number was not compromised in the data breach being reported, is the person or agency that experienced the breach required to offer or provide any type of free credit monitoring services?

A: No. There is no requirement that the person or agency provide credit monitoring services to MA residents.

- 7. Q:** How does a MA resident whose Social Security number has been compromised sign up for the free credit monitoring services being offered by the person or agency that experienced the breach?

A: The person or agency must provide all the information necessary for the MA resident to enroll in credit monitoring services as well as information on how the resident may place a security freeze on their consumer credit report at no cost in the notice provided to the consumer.

- 8. Q:** What other steps must the person or agency take when a resident's Social Security number has been compromised and they have fulfilled all of the above?

A: A person or agency who experienced a breach of security must also file a report with the Attorney General and the OCABR certifying that their credit monitoring services comply with the requirements of section 3A of Chapter 93H.

- 9. Q:** Does this report have to be filed separately from the data breach notification?

A: No. The person or agency that experienced the breach may include that acknowledgment with the notification filed with the OCABR. Reporting entities may provide the OCABR with notification by mail, email or by filing online using the Office's reporting portal found here: <https://www.mass.gov/forms/data-breach-notification-submission>

- 10. Q:** In exchange for offering credit monitoring services to the resident, can the person or agency that experienced the data breach require the resident to sign a waiver prohibiting that consumer resident from taking legal action against the person or agency relating to the data breach?

A: No. A resident cannot be required by the person or agency that experienced the data breach to waive their private right of action as a condition of being offered the free credit monitoring services. This is true whether or not the person or agency is offering the free credit monitoring services because they are required to under section 3A of Chapter 93H or they are opting to do so as a gesture of good will to offset the harm of the data breach.

- 11. Q:** Were any other changes made to the notice to be provided to the MA resident by the person or agency that experienced the data breach?

A: Yes. The law has always required that the notice to be provided to the resident must 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. The notice to the resident shall not, however, include the nature of the breach of security or unauthorized acquisition or use, or the number of residents affected by said breach of security or unauthorized access or use.

Pursuant to both federal and state law, the **notice must now** also include that **there shall be no charge for a security freeze** and, after April 10, 2019, **what, if any, mitigation services will be provided to the resident.**

12. Q: What if the person or agency that experienced the data breach is owned by another person or corporation?

A: The notice to the consumer must include the name of the parent corporation or the affiliated corporation.

13. Q: Who else must receive a copy of the notice sent to the MA resident?

A: The person or agency that experienced the breach of security must provide a sample copy of the notice it sent to the MA residents to the Attorney General and the OCABR. Even if the number of residents affected by the breach is not known, the filing of the sample notice must be provided with the breach notification.

14. Q: Does the person or agency that experienced a breach need to submit a data breach notification or provide the notice to consumers if information about the breach is unknown?

A: Yes. The breach notification should be reported to the OCABR as soon as practicable and without any unreasonable delay. As additional information about the breach is discovered, the person or agency that experienced the breach shall provide updates in both the notification to the OCABR and to the consumer.

15. Q: What is the Office of Consumer Affairs and Business Regulation required to do with these sample notices that are sent to the MA residents?

A: The Office must post on its website a copy of each of these notices within 1 business day of receipt from the person that experienced the data breach.

The OCABR reminds reporting persons or agencies to ensure that the sample copy of the notice sent to the consumers and provided to OCABR does not include any personal information of the consumer resident.

