CYBERSCOUT®

Frequently Asked Questions – Eversource Data Exposure March 2021

Questions & Responses:

1. What Happened?

As part of a security review, Eversource identified that one of its cloud data storage folders had been misconfigured and set to open access rather than restricted access. This occurred on March 16, 2021 and the Company immediately restricted access to the folder that same day. The Company's Security team then undertook a full investigation to understand what information was contained in the folder and the nature and scope of the incident.

In the folder were several files that contained the personal information of some Eversource eastern Massachusetts customers, including your information. However, based on our Security team's investigation, the Company has no indication that the personal information has been accessed, acquired or misused by any external party.

2. When did Eversource find out about this?

The files were created in August 2019 and the issue was discovered in March 2021.

3. What kind of data was exposed?

The personal information involved included name, address, phone number, social security number and Eversource account number and Massachusetts service address. No banking or financial information was involved.

4. Do criminals have access to the exposed data?

This exposure was unintentional and not the result of an attack or breach of Eversource systems. The same day that the misconfiguration was discovered, the files were locked and subsequently deleted. While it's possible they were accessed while unintentionally exposed, Eversource IT Security experts say it is highly unlikely due to the complex and unique file names, which were not published anywhere and would have been required for access.

5. Why am I receiving this notification?

Some State and Federal laws require that we notify you in writing. In any case, we want you to be aware of this incident because some of your personal information may have been exposed and we want to provide you with the information contained in the notification and offer you credit monitoring services as a precaution. We're committed to protecting the privacy and personal information of every one of our customers.

6. Why did you wait so long to notify me?

We moved as quickly as we reasonably could once the issue was identified. It took us a little time to determine what information was included and who was affected.

7. **Why didn't you just call me?**

   State and Federal laws require written notification. Also, we wanted to be sure you knew this was a legitimate notice and that the affected people received the notice.

8. **How many people were affected?**

   We have notified approximately 11,000 customers.

9. **Was the data encrypted?**

   No. The information was stored in an unencrypted format.

10. **Is my spouse affected? He/she is/was a customer as well.**

    Each impacted person will receive a letter from Eversource. Unless he/she has received a letter, he/she is not affected by this incident.

11. **Has the missing data been misused?**

    There is no evidence that any of the data has been misused.

12. **What is Eversource doing to make sure this does not ever happen again?**

    Our Security team conducted a thorough investigation and has taken appropriate actions. We have implemented additional security measures and updated our current security protocols to prevent this from happening again.

Identity Theft Concerns

13. **I am concerned about identify theft - what can I do?**

    There are a variety of steps you can take, many of which were detailed in the letter. These include placing a fraud alert with the credit bureaus, reviewing your financial statements, and signing up for credit monitoring.

14. **I am not satisfied that you are doing enough to protect me - I will be contacting my attorney or filing a lawsuit.**

    I understand your concerns entirely. Please allow me to take your name and number and I'll have Eversource management give you a call back soon to discuss this with you further.

    Note to CSR: Escalate call in database. Be sure you capture a telephone number so a return call can be made.

15. Since my address is included with the missing information, am I in any danger of being robbed?

Your address is likely available through many other sources of public records and is not generally considered sensitive personal information by itself.

16. What will happen if I find out my identity has been stolen?

In the unlikely event that your information is misused, a personal advocate will work with you from the first call you make to report the problem until the crisis is resolved. Cyberscout will notify the appropriate agencies, businesses, institutions, and create a comprehensive case file resolution assistance.