Data Breaches 2024 -- What Should I Do Now?

Background: Another massive data breach was announced a few days ago, impacting over 3 BILLION records. Hacked data includes current and past names, addresses, phone numbers, dates of birth, social security numbers, and the like. With this information, cybercriminals can easily pose as someone else and open financial accounts, effectively stealing identities and assets (monies and otherwise).

Note: There have been a LOT of data breaches in 2024, this one just being the most recent.

What can you do?

Experts recommend a variety of actions. I'll list them here, and then provide instructions how to do each one.

1. Check to see if your personal information was included in the most recent data breach.
2. Check your credit reports to see if there has been any unusual activity.
3. Put fraud alerts on your credit reports so you'll be alerted if anyone accesses them.
4. Freeze your credit reports so no one else can access them.
5. Add other security measures to your financial records, if you haven't already done that.
6. If identity theft has already occurred, contact your financial institution, creditors, and the police.
7. Explore other resources.

Here's how to do each of these tasks. They're not difficult, but they can be time-consuming, since there are three separate credit reporting bureaus (Equifax, Experian, and TransUnion), and they all have to be contacted for each of these steps. Just contacting one of them is not sufficient.

Check to see if your personal information was included in the most recent data breach.

To determine if your personal information was included in the most recent data breach, do the following:

1. Access https://npd.pentester.com/.
2. In the fields at the top of the page, type your last name, first name, and year of your birth. You may also choose your state from the drop-down menu; however, the state is not absolutely necessary.
3. When finished, click **Search**. The screen will be refreshed, showing any data records that match your search criteria.
4. Scroll as needed, looking for your own records. Note that you may have more than one record, particularly if you have had different phone numbers or addresses.

5. Repeat the process for all of your family members -- both living AND deceased!

Note that this search is only for the most recent data breach. If your name doesn't appear here, that doesn't mean that your data is not at risk! Therefore, it's highly recommended that you still continue to do the other steps below.

Also note that if you want to protect the identify of a deceased person, the process is a little different. See https://lifelock.norton.com/learn/identity-theft-resources/identity-theft-ghost-stories for a good explanation of what to do in that case.

Check your credit reports to see if there has been any unusual activity.

Each year, you're entitled to receive a free credit report from each of the three reporting bureaus.

For an easy way to request these free annual reports, do the following:

1. Access http://www.annualcreditreport.com/.

2. Click the **Request your free credit reports** button.

3. Follow the instructions on the screen.

Remember to request reports from all three credit bureaus: Equifax, Experian, and TransUnion.

4. After receiving the reports, review them to see if there are any unusual or unfamiliar entries. If so, that could be an indicator that your accounts have already been compromised.

Note that, while this is a really good check, you can only request these reports for free once a year. That's not enough to keep up with the cybercriminals.

Put fraud alerts on your credit reports so you'll be alerted if anyone accesses them.

I'm not going to spend a lot of time on this section. Even though the alerts are good (and free) -- and until this last breach might have been all you'd need to do -- with the massive breach last week, actually freezing the reports is the currently recommended action.

However, if you still want to place the alerts, the steps are similar to placing a freeze. (Details about freezes will be in the next section.) In short, you'd contact each credit bureau and request a fraud alert.

Here's contact information for placing fraud alerts on your credit reports:

- Equifax -- https://www.equifax.com/, 800-525-6285
- Experian -- https://www.experian.com/, 888-397-3742
- TransUnion -- https://www.transunion.com/, 800-680-7289

Note that each of the credit bureaus have a lot of paid services too, and they'll likely be a lot of advertisements about them -- but you can skip those ads if all you want are alerts or freezes.

Freeze your credit reports so no one else can access them.

This is the recommended action now. While it can cause additional steps if you are opening a new credit card or bank account, or setting up a new mortgage or car loan, or doing other financial transactions, that inconvenience is extremely minor in comparison to what you could have to do if someone steals your credit and ruins everything you might have already worked hard to obtain.

Basically, when you freeze your credit, that means that no one can run a credit check on you; the credit bureaus will deny the request -- and, therefore, your request for new credit will be denied. However, you can plan ahead and temporarily unfreeze your credit -- just for enough time for the credit check to be processed -- and then reinstate the freeze. The freeze/unfreeze/re-freeze process is simple; however, it does cause additional steps and inconvenience on your part. However, as stated earlier, it's a much smaller inconvenience than if someone starts posing as you and opening credit in your name -- and running up sky-high bills!

Here are the basic steps for freezing your credit. Note that your screens may vary slightly depending on how you access them.

Note that, as in a lot of the previous sections, you have to repeat the process for each of the three credit bureaus.

1. Access the credit bureaus' websites, or contact them by phone. Here's the contact information:

- Equifax -- https://www.equifax.com/personal/credit-report-services/credit-freeze/, 888-298-0045
- Experian -- https://www.experian.com/freeze/center.html, 888-397-3742
- TransUnion -- https://www.transunion.com/credit-freeze, 800-916-8800

2. Follow the instructions on the screen or on the phone.

In my experience, I had to set up accounts (with user names and passwords) for each credit bureau. Some required additional validation (like two-factor authentication, where they sent confirmation codes to my cell phone), and some required that I answer a series of multiple-choice credit-related questions to prove my identity. Credit-related questions can include such things as:

- Which of these cars have you ever owned?
- Which of these addresses have you lived at?
- In 1999, where did you have a car loan?
- Which mortgage company did you use for your first home?
- Have you ever had a credit card with any of these companies?

And the like.

After freezing your credit, you'll receive a confirmation notice, along with instructions for unfreezing your credit, either permanently (not recommended) or temporarily (useful when you're applying for some new credit).

Remember to freeze not only your credit reports, but also those for your other family members.

Add other security measures to your financial records, if you haven't already done that.

This section describes several other security actions that you should take, if you haven't already done so. Again, some of them will cause a bit of inconvenience, but that inconvenience is minor compared with the potential consequences of not doing them.

1. Add two-factor authentication to all your financial and medical accounts. This means that when you log onto an account (such as your banking website, your MyChart records, your credit card providers, and the like), you will have to do more than just type your name and password. Typically, after typing your name and password, there will be a screen about further confirming your identity by sending a code to the cell phone number or email address in their records. When you receive this code, then you can type it on the logon screen, and then continue with your transactions. This process adds another layer of security to your accounts.

Note that you can do this with lots of types of accounts. The most crucial ones are financial and medical, but typically, if an account offers this feature, it's recommended to go ahead and set it up.

2. Periodically change your passwords and PINs for all your financial and medical accounts. Remember to use hard-to-guess, unique passwords, not using common words or passwords that are shared with other accounts.

3. If available at your financial institution (bank or credit union), you can set up alerts that notify you when specified types of transactions occur. By setting up these alerts, you can more easily monitor the activity, to ensure that nothing unusual or unauthorized is occurring.

4. Periodically review your contact information at your financial institutions, medical providers, and credit providers to ensure that everything is correct.

5. Beware of scams, phishing, and other attempts to gain personal information that may arrive via email, text, or phone.

If identity theft has already occurred, contact your financial institution, creditors, and the police.

The previous sections have talked about how to prevent identity theft, focusing on freezing your credit reports. However, if you've already experienced identity theft, be sure to immediately do the following:

- Notify your financial institution(s).
- Notify all your creditors.
- Notify the police.

For a good checklist, see https://www.wellsfargo.com/assets/pdf/personal/privacy-security/fraud/identity-theft-kit.pdf. Even though it's primarily directed toward Wells Fargo customers, there's still a lot of good general information in their advice.

Other resources

- Information about some other large data breaches in 2024: https://www.komando.com/news/security/biggest-data-breaches-of-2024-so-far/
- Additional information about the NPD data breach: https://ktla.com/news/data-breach-may-have-exposed-private-info-of-billions-of-people-lawsuit-says/
- Federal Trade Commission resources related to identity theft: https://www.ftc.gov/news-events/topics/identity-theft
- Wells Fargo guide to spotting common scams: https://www.wellsfargo.com/privacy-security/fraud/bank-scams/

Conclusion

Hopefully these guidelines and resources are useful as you protect your hard-earned credit and identity and that of your family members. Remember the old saying, attributed to Benjamin Franklin, "an ounce of prevention is worth a pound of cure".

written by Diana Nelson Haase, 19 August 2024