I'm Part of a Data Breach... What Does That Mean?

We live in a digital age where our personal information is stored on many many different digital platforms and is subject to attack and theft by identity thieves and fraudsters.

In 2023 there was an estimated 72% increase in US Data Breaches compared to 2021.

In the first half of 2024 there have already been over 700 Data Breach compromises with over 1 billion victim records exposed!

I Received A Data Breach Notification Letter... What Does it Mean? What Should I do?

There is NO Federal Data Breach Notification Law BUT all 50 States have laws covering responsibilities in the event of a breach. These include the time frame and ways victims should be notified and any remedial steps the affected entity must take to assist victims.

Many of us will have received Breach Notification Letters detailing the incident and the nature of the information compromised. Often times it's accompanied by free credit monitoring services for a period of time.

If you receive a letter, the first thing to do is to check that it is a **LEGITIMATE NOTIFICATION** and not a Phishing attempt! Check the Company's website for information and call them if necessary to check.

Being a victim of a data breach means that your personal information was exposed, **but it doesn't necessarily mean that your information has been fraudulently used.** A data breach occurs when unauthorized individuals access or steal data, which can include sensitive information like your name, address, Social Security number, credit card details, or other personal data.

After a data breach, there is a risk that your information could be used for fraudulent activities, such as identity theft, financial fraud, or phishing scams. However, it's important to note that just because your data was exposed doesn't mean it has been or will be misused.

Here are some steps you should consider taking to protect yourself:

1. **Monitor Your Accounts:** Regularly check your bank and credit card statements for any suspicious activity. Report any unauthorized transactions immediately.
2. **Change Passwords:** If the breach involved online accounts, change your passwords, especially if you reuse passwords across multiple sites.
3. **Enable Two-Factor Authentication (2FA):** Add an extra layer of security to your accounts by enabling 2FA wherever possible.
4. **Check Your Credit Reports:** Obtain free copies of your credit reports from the major credit bureaus (Experian, TransUnion, Equifax) and look for any unusual activity.
5. **Consider a Credit Freeze:** A credit freeze prevents new credit accounts from being opened in your name.
6. **Be Wary of Phishing Attempts:** Scammers might use your information to send convincing phishing emails or messages. Be cautious about clicking on links or providing further personal information.

Taking these precautions can help minimize the risk of your information being fraudulently used after a data breach.

More Information? Call Us... 877 308 9169

www.idresolution.net