IDShield
Worry Less. Live More.

Being Part of a Data Breach Event

Have you ever received a notification that your personal data was exposed in a data breach? A better question might be, *"Who hasn't?"*

While it's not uncommon, it is a cause for concern and the questions then become, *"Just how concerned should I be?"* and *"How do I respond to this?"*

Breach notifications often do bring with them an offer of an identity theft product for 12 or 24 months, so some may think that offer of services is all they need (for that time period) to be best protected, reduce the risk of identity theft and respond if something happens.

However, the best response is to already have a product in place to be in the best position to detect and then, if necessary, respond to an event involving your personal identifiers.

> **It's imperative to note that any restoration services available through an offer from the breached entity may apply ONLY to a matter connected to the breach event itself and may be limited in scope.**

So if you found yourself the victim of an identity theft event unrelated to the breach, restoration services would not apply. Consider this example:

- You received an identity theft-related product for 24 months at no cost to you because of a breach event involving a cyber-attack on a database that contained your name, SSN and address. You then found yourself the victim of counterfeit and forged checks—someone obtained your personal information and made checks with your information on them and forged your signature to them.
- The product provided by the breached organization would not provide services to address and resolve the counterfeit and forged checks because that event is not related to the breach suffered by the organization.

Important tips to follow when you receive a data breach notice:

Data breach notifications have a tendency to elicit a wide range of responses—everything from anger and fear to complete apathy. But as the recipient of such a notice, the most important thing to do is remain calm and keep in mind there are positive steps that you can take:

First: don't over- or under-react. While a breach notice doesn't mean you are a victim of identity theft, it does mean that your information was apparently accessed by someone without authority to see it. So, it isn't something you should toss aside without thought, either.

Second: read the entire letter and answer these questions:

1. What entity sent the letter?
2. Why did they have data about you or what is their relationship to you?
3. What type of data was exposed? Was it your Social Security number, information on an existing financial account, or your email address? Each calls for a different response by you.
4. How did this happen? Was it an accident or an orchestrated attack on that entity for the purpose of stealing data?
5. Is the company offering credit monitoring, identity theft consultation, identity restoration, or other services to you?

- If you have doubts about the legitimacy of the letter, check the website of the entity sending the letter or call their headquarters to verify the event and any associated offers.

Be Cautious

Scammers may try to use this event to trick people into giving up personal information. If you receive an email or phone call from someone claiming to be from the business that notified you of the breach and asking for your personal information, do not respond to them. Call the affected business directly to determine if it was their actual representative who contacted you.

Already a LegalShield IDShield Plan Member?

If you're already a valued member of the LegalShield family, log in at idshield.com to ensure your monitoring services are active and up-to-date. By proactively monitoring your personal information, you have tools in place to know, firsthand, if there are potential signs of identity theft. That, coupled with the security of Licensed Investigators on your side, means you can worry less and live more.

Not a LegalShield IDShield Member yet?

Large events like this can be overwhelming to anyone who may potentially be affected. If you are currently not a member and would like to learn more about how you can protect you and your family against the growing threat of identity theft, please call 1-888-494-8519 or visit idshield.com.