How To Help Your Clients When A Data Breach Hits

6 steps to protect you and your family from a breach

By Eric Harrell

Another day, another data breach in the news. This time, it affects you. That could mean:

- As an individual, your personal information was exposed
- As an HR professional, some or all of your employees' information was exposed

Whatever the source of your concern, the first thing to realize is that taking quick and informed action is important. The sooner you act, the more potential problems you may be able to mitigate. This post will explain what a breach means and provide you with a short list of things you can do to protect yourself when a breach occurs.

If you're the individual whose privacy has been breached, follow this list. If you're an HR professional, share it with your employees and clients.

What is a Data Breach and What Does It Mean?

A data breach, in its simplest terms, is unauthorized access into one or more of a company's databases.

Keep in mind that a breach doesn't always mean that data was actually stolen. It just means that you need to be careful because potential problems such as fraud and identity theft could be headed your way.

The two basic components of a breach that are important to consider are what was exposed and when.

- **What information was accessed:** This could be usernames and passwords, Social Security numbers, address and phone numbers, personal records such as health and financial histories, credit card numbers and more. Often the company will know exactly which records were accessed. Sometimes, however, they'll report that the extent of the breach was "unclear." When this is the case, it's best to assume that any or all of your information stored there could have been stolen.

- **When did the breach occur:** Reports and news stories about breaches often break well after a breach has taken place. Look to see if the actual date when the breach occurred is explicitly stated. It's important to note that even if a breach occurred 24 months ago, the exposed information may not have resurfaced for sale on the dark web. Worse yet, some identity thieves wait a long period of time to commit fraud, so it happens when you least expect it.

With that in mind, to best protect yourself or your clients, follow these six steps:

6 Steps to Protect You and Your Family From a Breach

1. Keep an eye out for emails and physical mail regarding a breach

You may receive a communication from the company if you were affected. This communication might contain important information about what was accessed, whether your personal information was involved, and any steps they are taking to help you avoid any problems. If you don't normally view your mail daily, now is the time to do so.

2. Place a fraud alert with the credit bureaus to flag your report as potentially compromised

This is a quick and easy safeguard that requires vendors to verify an individual's identity before extending credit. The Federal Trade Commission

offers a simple guide to placing a fraud alert. These fraud alerts will protect your accounts for one year and can be extended another year if you choose to do so.

3. Review your PrivacyArmor® account for any alerts

If you have a PrivacyArmor account, your protection is already hard at work. Log in to the portal to see if you have any alerts — if you do, you will be able to see them upon logging in. Some of the alerts you could see on your PrivacyArmor dashboard include:

- Credit monitoring and suspicious activity alerts
- New account creation and credentialing alerts
- Financial threshold alerts (with any linked financial accounts you've added)
- Dark web monitoring alerts

While your account's Personally Identifiable Information (PII) is already being monitored on the dark web automatically, you'll want to make sure you've added additional important information you'd like us to protect. Here are step-by-step instructions for taking full advantage of dark web monitoring.

4. Use your PrivacyArmor account to pull your credit report (read below if you don't have one)

Using the instructions below, pull your report and view it in depth to make sure it's accurate. If you don't recognize an inquiry or account, report it immediately. If you're a PrivacyArmor member you can do so in-portal — if not, contact the credit bureau directly.

In PrivacyArmor, it's easy to pull a credit report:

- Click on "Credit Monitoring" in the menu
- Click the "View Credit Report" button below

If you're not a PrivacyArmor member yet, you can pull your report without penalty once a year from each of the three big credit bureaus. One of the simplest ways to do this is to go to each bureau's website:

- TransUnion.com
- Experian.com
- Equifax.com

5. If you used a password with the breached company, change it

Thieves often take advantage of people who wait before taking necessary precautions like changing a password. If you use the same or a similar password on other accounts, take care to change those as well. Whenever possible, activate two-factor authentication on your accounts — which add an extra security measure beyond a password — to help prevent possible theft after a breach.

6. If you have reason to believe a high-value piece of PII has been breached, take the necessary precautions

A piece of high-value PII would typically mean your Social Security number and/or medical data. These are high-value because they're the easiest for identity thieves and fraudsters to exploit — either now or in the future when you least expect it. PrivacyArmor's dark web monitoring technology and operatives scour hacker forums for any piece of PII you enter in this tool. If you're in the medical industry, you're especially vulnerable, which is why we can monitor for your National Provider Identifier and DEA numbers on the dark web.

How Privacy Armor protects you

There are many ways in which PrivacyArmor helps protect you when a company housing your data is breached. If your company is already a member, stay tuned and follow the steps above. If your company isn't, you can contact your broker for details on offering PrivacyArmor as a voluntary or sponsored employee benefit program. If you're a self-insured organization, reach out directly to the InfoArmor team for a demo and more information.

This article originally appeared here.

Eric Harrell is a Senior Vice President of Sales Strategy and Operations at InfoArmor.

Would you like to comment?

Submit Your Articles

InfoArmor

Not every **superhero** wears a cape.

Defend your organization with PrivacyArmor®, the most advanced identity theft protection available.

In-house **24/7** resolution

Seamless integration with **140+ platforms**

99% client satisfaction rate

Voluntary & sponsored programs, available through benefits brokers

Learn more