Data Breaches: What You Can Do

Preventative Tips To Help Navigate the Uncertainty

PERSONAL INFORMATION EXPOSED?

Hearing that your personal information could have been exposed in a data breach can be unnerving. Whether it is a big box retailer, bank, media conglomerate, medical insurance carrier or any other provider, data incidents have changed our perspective on information protection. Now it is more important than ever to protect your identity.

There may still be questions about the type of information that has been exposed or even whether or not your information was impacted in a recent data breach. Organizations that have experienced a data breach of subscriber or customer data are required to notify those impacted with written notification. Companies often offer credit monitoring for free to impacted subscribers but beware; credit is only one component of your identity that is at risk and you should also consider the additional protection of identity monitoring if you are not already protected.

Please review these steps if you suspect your information could have been involved in a data breach:

STEP 1: Review Your InfoArmor Account

Ensure your personal information is up to date. Also be sure to take advantage of additional features such as activating CreditArmor and inputting information into WalletArmor.

By updating your account information we can monitor the underground market and continue to watch for fraudulent activity using your information, ensuring that we alert you of any suspicious activity or help you begin the process of recovering from identity theft.

continued...

STEP 2: Change Your Passwords

Change your password of the email account that was used within the breached company's records and any profile passwords that are associated with this account (e.g. online banks, social media, etc.).

Your passwords should be at least eight characters long and a mix of upper and lowercase letters, numbers, and symbols. Your passwords should not be shared across more than one account.

STEP 3: Place Fraud Alerts With Credit Bureaus

Fraud alerts are good for 90 days, free of charge and renewable an infinite amount of times. An individual can place an alert with one of the bureaus and that bureau will notify the other two. To place a fraud alert please visit one of these links:

https://www.experian.com/fraud/center.html
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page

STEP 4: Let Your Bank And Credit Card Companies Know Immediately

Bringing your bank and credit card companies to attention of this breach can lock down your account against attacks. Banks and credit card companies will actually excuse you from any financial liability caused by data breaches. When dealing with identity thieves, a few minutes can be the difference between losing a dollar or losing everything in your checking account.

Additionally, if you have reason to believe your information has been used to commit fraud, complete the following steps:

Create an identity theft affidavit with the FTC

While you already have a police report in hand, you'll also want to contact the Federal Trade Commission to build an identity theft affidavit. This affidavit will help you assemble the facts about your case—when the identity theft happened, which accounts were affected, etc.—and get them dated, signed, and notarized. This provides a credible document that you can show to credit card companies, banks, and any other companies you need to in order the fix the damage caused by a data breach.

File a Police Report

For your protection against excessive financial liability, you need to file a report with your local police department as soon as possible. This makes your status as an identity theft victim official. It also creates an official document for you to show the credit bureaus to lock down any activity around your identity.

QUESTIONS?

If you have any questions, please feel free to contact one of our Privacy Advocates at (800) 789-2720.
We are available to help you Monday through Friday from 7:00 a.m. to 5:00 p.m. Pacific.