LeTort Trust
Lana Burkhardt
3130 Morningside Drive
Camp Hill, PA 17011
lburkhardt@letorttrust.com

Data Breaches: Tips for Protecting Your Identity and Your Money

A data breach is an incident in which private, personal information is exposed, viewed without authorization, or stolen.

Large-scale data breaches are in the news again, but that's hardly surprising. Breaches have become more frequent — a byproduct of living in an increasingly digital world. During the first six months of 2019, the Identity Theft Resource Center (ITRC), a nonprofit organization whose mission includes broadening public awareness of data breaches and identity theft, had already tracked 713 data breaches, with more than 39 million records exposed.[1] Once a breach has occurred, the "aftershocks" can last for years as cyberthieves exploit stolen information. Here are some ways to help protect yourself.

Get the facts

Most states have enacted legislation requiring notification of data breaches involving personal information. However, requirements vary. If you are notified that your personal information has been compromised as the result of a data breach, read through the notification carefully. Make sure you understand what information was exposed or stolen. Basic information like your name or address being exposed is troubling enough, but extremely sensitive data such as financial account numbers and Social Security numbers is significantly more concerning. Also, understand what the company is doing to deal with the issue and how you can take advantage of any assistance being offered (for example, free credit monitoring).

Even if you don't receive a notification that your data has been compromised, take precautions.

Be vigilant

Although you can't stop wide-scale data breaches, you can take steps to protect yourself. If there's even a chance that some of your personal information may have been exposed, make these precautions a priority.

- **Change and strengthen passwords.** Create strong passwords, at least 8 characters long, using a combination of lower- and upper-case letters, numbers, and symbols, and don't use the same password for multiple accounts.
- **Consider using two-step authentication when available.** Two-step authentication, which may involve using a text or email code in addition to your password, provides an extra layer of protection.
- **Monitor your accounts.** Notify your financial institution immediately if you see any suspicious activity. Early notification not only can stop a potential thief but may help limit any financial liability.
- **Check your credit reports periodically.** You're entitled to a free copy of your credit report from each of the three national credit reporting agencies every 12 months. You can get additional information and request your credit reports at annualcreditreport.com.
- **Consider signing up for a credit monitoring service.** It's not uncommon for a company that has suffered a data breach to provide free access to a credit monitoring service. As the name implies, this service tracks your credit files and alerts you to changes in activity, such as new accounts being opened or an address change.
- **Minimize information sharing.** Beware of any requests for information, whether received in an email, a letter, or a phone call. Criminals may try to leverage stolen information to trick you into providing even more valuable data. Never provide your Social Security number without being absolutely certain who you are dealing with and why the information is needed.

Fraud alerts and credit freezes

If you suspect that you're a victim of identity theft or fraud, consider a fraud alert or credit freeze.

A fraud alert requires creditors to take extra steps to verify your identity before extending any existing credit or issuing new credit in your name. To request a fraud alert, you have to contact one of the three major credit reporting bureaus. Once you have placed a fraud alert on your credit report with one of the bureaus, your fraud alert request will be passed along to the two remaining bureaus.

A credit freeze prevents new credit and accounts from being opened in your name. Once you obtain a credit freeze, creditors won't be allowed to access your credit report and therefore cannot offer new credit. This helps prevent identity thieves from applying for credit or opening fraudulent accounts in your name.

To place a credit freeze on your credit report, you must contact each credit reporting bureau separately. Keep in mind that a credit freeze is permanent and stays on your credit report until you unfreeze it. If you want to apply for credit with a new financial institution in the future, open a new bank account, apply for a job, or rent an apartment, you'll need to "unlock" or "thaw" the credit freeze with all three credit reporting bureaus. Each credit bureau has its own authentication process for unlocking the freeze.

Recovery plans

The Federal Trade Commission has an online tool that enables you to report identity theft and to actually generate a personal recovery plan. Once your personal recovery plan is prepared, you'll be able to implement the plan using forms and letters that are created just for you. You'll also be able to track your progress. For more information, visit identitytheft.gov.

[1] Identity Theft Resource Center, Data Breach Reports, June 30, 2019

IMPORTANT DISCLOSURES

LeTort Trust does not provide tax or legal advice. The information presented here is not specific to any individual's personal circumstances. To the extent that this material concerns tax matters, it is not intended or written to be used, and cannot be used, by a taxpayer for the purpose of avoiding penalties that may be imposed by law. Each taxpayer should seek independent advice from a tax professional based on his or her individual circumstances. These materials are provided for general information and educational purposes based upon publicly available information from sources believed to be reliable—we cannot assure the accuracy or completeness of these materials. The information in these materials may change at any time and without notice.