PARTRIDGE FINANCIAL

Has Your Data Been Compromised? Here's What to Know and What to Do

Periodically, companies will report massive data breaches, some impacting billions of records that contain personal information such as names, addresses, and Social Security numbers. Depending on the situation, it is possible that your information was compromised. Companies will often reach out to alert consumers about this potential risk once a data breach has been confirmed.

Unfortunately, there is also a possibility that your information may have been compromised from some other surreptitious conduct rather than a large-scale data breach. Regardless of how it happened, it never gets any easier or less worrisome when you realize something isn't quite right and you are at a loss as to what to do next. Thankfully, if your personal data is compromised, there are several steps you can take to help you regain control of your situation.

Change your passwords

Immediately change your passwords. Make them difficult and do not use the same password for multiple accounts. This is a mistake many people make because they feel it simplifies their lives to have one easy password for everything. However, if your information gets compromised and your identity is stolen, it can be a headache trying to fix it and can cost you more than just sleepless nights.

Freeze your credit and Social Security number and place a fraud alert on your credit report

Freezing your credit and Social Security number and initiating a fraud alert is a fairly easy process. It can help keep your identity and personal information secure in the event of a data breach. In some cases, this process can only be accomplished over the phone. However, make sure that you are the one initiating the call. If somebody calls you claiming to be one of the three credit bureaus attempting to solicit information, immediately disconnect the call. Never give information over the phone to a random caller.

If you are unsure of how to proceed, you can visit your local Social Security Administration office in your town or city, and they will provide you with a sheet of phone numbers and what to do. The phone numbers listed below are legitimate phone numbers retrieved from the Social Security Administration if you are interested in freezing your credit and Social Security number. The bolded numbers are for those whose data has been compromised.

Equifax

www.Equifax.com
Equifax Credit Information Services, Inc.
P.O. Box 740256, Atlanta, GA 30374
1-888-766-0008: Place Fraud Alert on Your Credit Report
1-800-685-1111: Credit Report Inquiries
1-866-493-9788: Credit Reports, Scores, and Identity Theft Monitoring
1-888-202-4025: Business Solutions

Experian

www.Experian.com
P.O. Box 9554, Allen, Texas 75013
1-888-397-3742: Credit Report / Dispute Information / Fraud & Identity Theft
1-877-284-7942: Triple Advantage Credit Monitoring Membership
1-888-243-6951: Business Credit Services

TransUnion

www.TransUnion.com
P.O. Box 6790, Fullerton, CA 92834
1-800-680-7289: Fraud Alerts and Identity Theft Information
1-800-493-2392: Credit Monitoring Services Inquiries
1-800-888-4213: Purchase a Credit Report or Get Free Annual Report
1-800-916-8800: Dispute Items on Credit Report and Status Checks
1-866-922-2100: Business Services Assistance

Review Your Credit Report

Access your credit report and review it carefully. Dispute anything that looks suspicious. This can be done for free on Experian and you can dispute it right there on the app or website. The app is very easy to use and can be initiated with facial recognition software. If you are concerned about something on your credit that you don't recognize, dispute the issue. When you dispute an issue, the company will ask you for a reason. Be aware that you can't use "identity theft" as a reason online or on the app. For that, you must call. Still dispute it online but put "the information listed isn't you" as the reason.

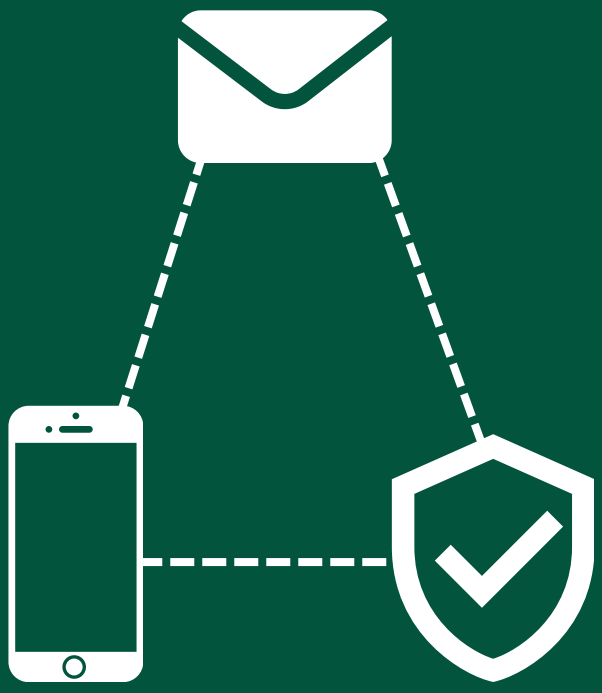
Generally, a regular dispute can take up to 30 days. However, you can also call the numbers listed above to the three credit bureaus and speak to a representative. Explain to them that your data was compromised and there is questionable activity on one of your credit reports. For example, maybe a new address was added that isn't you. The representative can also read through, for instance, the addresses listed to ensure there aren't other strange and suspicious additions to your credit report. If one or more of these addresses aren't you, then they will submit it as a called-in or over-the-phone dispute. The representative may notice you have also submitted a dispute online, and that is ok, but only they can mark the reason as identity theft.

Again, the suspicious issue may only appear on one of the three bureaus' credit reports. When you speak to a representative and they dispute it over the phone, they can list the reason as identity theft. This way the process is rapidly sped up and the bogus information can be removed from your credit report within 72 hours, if not sooner, instead of having to wait 30 days. If you feel your information is seriously compromised, credit agencies suggest filing a police report and then sending a copy of it to each of the three credit bureaus to keep on file. The addresses are listed above with the phone numbers.

Set up multi-factor authentication

Multifactor authentication (MFA) is a multi-step account login process that requires users to enter more information than just a password and may better safeguard you from ill-intentioned people out to steal your personal information. In some cases, users might be asked to enter a code sent to their email or phone. There might be a question with a pre-determined answer, for example, the name of your first pet, or your father's middle name.

There are also more advanced technological security measures like fingerprint scans or facial recognition. Multi-factor authentication is a step that goes beyond your initial password protection. It can often be set up for bank accounts, business-related programs, online shopping, and more. Having this extra layer of security works to thwart nefarious activity from potential hackers.



Stay alert for fraud or scams, especially after a data breach hits the news

It is imperative you remain on high alert for criminals attempting to steal your information. Be especially vigilant during times of newsworthy data breaches. Scammers take advantage of unfortunate events like these to manipulate worried individuals into divulging their personal information when it hadn't been compromised in the first place.

You might receive a phone call or an email suggesting that if you provide your personal information, they can check to see if your information was compromised or is on the dark web. Never provide any information to strangers who reach out in any way under the guise of helping you while asking for sensitive information. You should be proactive and reach out to the credit bureaus yourself.

☑ Consult your financial professional

If your data has been compromised, don't panic. Take the necessary steps that are in your control to safeguard your information. Consider consulting a financial professional to reassess your financial strategy and goals and to ensure nothing is compromised long-term. A financial professional can also be another set of eyes to stay vigilant for attempted scams or other dubious behavior.

Sources:
More than a Password | CISA
What is MFA? - Multi-Factor Authentication and 2FA Explained - AWS (amazon.com)