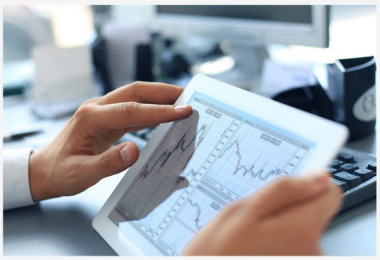
# How to Respond to a Data Breach



Time is of the essence, whether your personal data has been compromised as part of a larger targeted cyberattack, or you are the victim of an individual cybercrime. You'll need to take immediate action to minimize the impact. These are steps you should take within specified timeframes after discovering your data has been breached.

## Within the first 24-48 hours

1. Call your advisor, regardless of where or how the breach occurred, so he/she can watch for any suspicious activity in your accounts and collaborate with you on extra precautions to take in verifying your identity prior to any fund transfers.

2. Call the **Social Security Administration's fraud hotline at 800-269-0271** if you suspect your Social Security number has been compromised. The Office of the Inspector General will take your report and investigate activity using your Social Security number. The Social Security Administration also provides helpful materials, such as the pamphlet ***Identity Theft and Your Social Security Number***.

3. Contact the **Federal Trade Commission (FTC), either at** www.identitytheft.gov**, by calling 1-877-IDTHEFT** (TTY 1-866-653-4261), or by visiting www.ftc.gov. Click on **Report Identity Theft** to access the **Identity Theft Recovery Steps**. This one-stop resource for victims of identity theft will guide you through each step of the recovery process, from reporting the crime to creating a personal recovery plan and putting your plan into action.

4. Visit the **IRS website** https://www.irs.gov/uac/taxpayer-guide-to-identity-theft if you're the victim of tax fraud. You'll be able to access the ***Taxpayer Guide to Identity Theft***, which provides education on tax-related identity theft, tips to reduce your risk, and steps for victims to take.

5. Call your **advisor** if you suspect you're a victim of fraud. Coldstream will investigate your case and take necessary precautions to prevent further unauthorized debits.

## Within the first 24-48 hours (continued)

6. Call your **advisor** if you suspect you're a victim of identity theft to discuss general identity theft questions or specific questions.

7. If appropriate, close any compromised or unauthorized accounts.

8. Run reputable anti-virus/anti-malware/anti-spyware software to clean your computer.

9. Once you've ensured your computer is virus/malware/spyware free, you should change passwords on your accounts. Make each password unique, long, and strong, and use multi-factor authentication when available.

---

## Within the first week

1. If the breach occurred at a firm with whom you do business, be sure to follow the legitimate directions provided by that firm. If it offers credit protection services, sign up for the service.

2. Report the crime to your local police, even though the incident may cross multiple jurisdictions. Your local police will file a formal report and may be able to refer you to additional resources and agencies that can help.

3. Report your stolen money and/or identity to one of the three main credit bureaus. Provide the credit bureau with your police report number and ask them to place a fraud alert on your account to prevent additional fraudulent activity. Once the fraud alert is activated, the two other credit bureaus will receive automatic notification and the fraud alert on your credit report will be in place for seven years with all three credit bureaus. (Without your police report number, the alert will only be in place for 90 days.)

| Equifax | Experian | TransUnion |
|---|---|---|
| **1-800-525-6285** | **1-888-397-3742** | **1-800-680-7289** |

4. Put a freeze on your credit report with each of the main credit bureaus to prevent the unauthorized opening of accounts. Executing a freeze with one credit bureau will NOT automatically update the others. You can easily unfreeze your credit report when needed. Contact the credit bureaus using this contact information for freezes.

| Equifax | Experian | TransUnion |
|---|---|---|
| **1-800-685-1111** | **1-888-397-3742** | **1-888-909-8872** |
| www.freeze.equifax.com | www.experian.com/freeze/center.html | www.transunion.com/securityfreeze |

## Within the first week (continued)

5. Review all recent account statements for unauthorized activity and report any suspicious transactions to the business where the unauthorized or suspicious activity occurred.

6. Consider what other personal information (e.g., birth date, social security number, PIN numbers, account numbers and passwords) may be at risk and alert the appropriate businesses.

7. Begin collecting and saving evidence such as account statements, canceled checks, receipts, and emails that may be useful if an investigation is warranted regarding the cybercrime.

## Within the next 30 days and beyond

1. Carefully review statements on all accounts as soon as they arrive. Look for unauthorized activity and report any suspicious transactions to the business where the unauthorized or suspicious activity occurred.

2. Notify your friends, family, business associates, and other relevant parties in your contact list that you were hacked. Tell them to beware of emails that may have been sent to them from your account.

3. Report back to your advisor once the issue has been resolved, so they can remove any blocks placed on emails from the compromised account.

4. Speak with your advisor regarding precautions you'll jointly take to enhance the identity verification process when you want to execute financial transactions.

5. If you're a victim of Social Security fraud, go to: www.socialsecurity.gov/myaccount and create an online Social Security account. This will enable you to access and review your statement online and verify its accuracy.

6. Request a credit report every six months to check for unauthorized activity. It will NOT affect your credit score.

**Be diligent for the next year in taking precautions to avoid further security incidents.**