Investor.gov
U.S. Securities and Exchange Commission

Investor Alert: Identity Theft, Data Breaches and Your Investment Accounts

The SEC's Office of Investor Education and Advocacy is issuing this Investor Alert to provide investors with important steps to take regarding their investment accounts if they become victims of identity theft or a data breach. Investors should always take steps to safeguard their personal financial information (e.g., social security number, financial account numbers, phone number, e-mail address, or usernames and passwords for online financial accounts). However, if identity theft or a data breach compromises your personal financial information, here are some important steps to take immediately.

Contact your investment firm and other financial institutions immediately. If you think your personal financial information has been stolen, contact your broker-dealer, investment adviser or other financial professional immediately to report the problem. You should also contact any other financial institutions where you have accounts that may be impacted by the loss of your personal financial information. These may include banks, credit card companies, or insurance companies. Please remember to document any conversations with your investment or financial firms in writing.

Change your online account passwords. Immediately change the password for any investment or financial accounts associated with the compromised personal financial information. Always remember to use strong passwords that are not easy to guess, consisting of at least eight or more characters that include symbols, numbers and both capital and lowercase letters.

Consider closing compromised accounts. If you notice any unauthorized access into your investment account, you may want to ask your investment firm to close the account and move the assets to a new account. You should consult your investment firm about the best way to handle closing an account, if you choose to do so.

Activate two-step verification, if available. Your brokerage firm or investment adviser may offer a two-step verification process for gaining access to your online accounts. With a two-step verification process, each time anyone attempts to log into your account through an unrecognized device (i.e., a device you have not previously authorized on the account), your investment firm sends a unique code to either your e-mail or cell phone. Before anyone can gain access to your account, they must enter this code and your password. Activating this added layer of security may help reduce the risk of unauthorized access to your accounts by identity thieves.

Monitor your investment accounts for suspicious activity. Closely monitor your investment accounts for any suspicious activity. Look out for any changes to your account information that you do not recognize (e.g., a change to your address, phone number, e-mail address, account number, or external banking information). You should also confirm that you authorized all of the transactions that appear in your account statements and trade confirmations. If you find any suspicious activity, immediately report it to your investment firm. Please remember to document any conversations with your investment firm in writing and provide a copy to your investment firm.

Place a fraud alert on your credit file. Placing an initial fraud alert in your credit file provides notice to potential creditors (e.g., banks and credit card companies) that you may have been a victim of fraud or identity theft and will help reduce the risk that an identity thief can use your personal financial information to open new accounts. Contact any of the three credit bureaus listed below and ask them to add an initial fraud alert to your credit file.

Experian	Transunion	Equifax
1-888-397-3742	1-800-680-7289	1-800-525-6285
www.experian.com	www.transunion.com	www.equifax.com

You only need to contact one of the credit bureaus to add the alert to your credit file at all three credit bureaus. The credit bureau you contact will notify the other bureaus about the alert. The initial fraud alert will last for 90 days, and can be renewed every 90 days. Requesting an initial fraud alert and renewing the alert are both free.

Active duty members of the military may elect to add an "active duty alert" to their credit file. Active duty alerts are the same as initial fraud alert except they last for 12 months.

If you have been a victim of identity theft, you may also consider placing an extended fraud alert or credit freeze in your credit file. An extended fraud alert is similar to an initial fraud alert except that it lasts for seven years. A credit freeze stops any new creditors from accessing your credit file until you remove the credit freeze from your credit file. Since most businesses will not open new credit accounts without checking your credit report, a freeze can stop identity thieves from opening new accounts in your name, but it does not stop them from taking over existing accounts. For additional information on extended fraud alerts and credit freezes, please visit the Federal Trade Commission's (FTC) identity theft website at www.identitytheft.gov.

Monitor your credit reports. After you place an initial fraud alert in your credit file, you are entitled to obtain a free copy of your credit report from each of the credit bureaus. Check each of your reports for signs of fraud, such as an unknown account, a credit check or inquiry to your credit file that you do not know about, an employer you have never worked for, or unfamiliar personal information.

Consider creating an Identity Theft Report. If a breach in your personal financial information results in identity theft, you may want to consider creating an identity theft report. An Identity Theft Report helps you deal with credit reporting companies, debt collectors, and business that opened accounts in your name. You can use the report to:

· Get fraudulent information removed from your credit report

· Stop a company from collecting debts that result from identity theft

· Place an extended fraud alert on your credit report

· Get information from companies about accounts the identity thief opened or misused.

Creating an Identity Theft Report involves three steps:

1. Report the identity theft to the Federal Trade Commission (FTC) by completing the FTC's online complaint form at https://www.ftccomplaintassistant.gov or by calling the FTC at 1-877-438-4338, and obtain an FTC Identity Theft Affidavit. If you decide to use the FTC's online complaint form, please remember to print out your completed form before leaving the website since you will be unable to retrieve it once you leave the FTC's website.

2. Contact your local police department about the identity theft and provide them with:

· A copy of your FTC Identity Theft Affidavit

· A government-issued ID with a photo

· Proof of your address (mortgage statement, rental agreement, or utilities bill)

· Any other evidence you have of the identity theft (bills, IRS notices, etc.)

· A copy of the FTC's Memo to Law Enforcement on identity theft

Ask for a copy of the police report.

3. Attach your FTC Identity Theft Affidavit to your police report to make an Identity Theft Report.

Additional information on Identity Theft Reports and identity theft in general, is available on the FTC's website at www.identitytheft.gov.

Document all communications in writing. Remember to document, in writing, and keep copies of any communications you have related to your identity theft.

Related Information

For additional educational information for investors, see the SEC's Office of Investor Education and Advocacy's homepage and the SEC's Investor.gov website. For additional information about safeguarding online investment accounts, data breaches and identity theft, also see:

- A recent SEC enforcement case regarding an investment firm's cybersecurity policies located at http://www.sec.gov/litigation/admin/2015/ia-4204.pdf
- SEC Investor Bulletin: "Protecting Your Online Brokerage Accounts from Fraud"
- SEC Publication: "Online Brokerage Accounts: What You Can Do to Safeguard Your Money and Your Personal Information"
- FINRA Investor Alert: "Protect Your Online Brokerage Account: Safety Should Come First When Logging In and Out"
- FTC OnGuardOnline.gov webpage: "Tips for Using Public Wi-Fi Networks"
- FTC IdentityTheft.gov webpage: www.identitytheft.gov

The Office of Investor Education and Advocacy has provided this information as a service to investors. It is neither a legal interpretation nor a statement of SEC policy. If you have questions concerning the meaning or application of a particular law or rule, please consult with an attorney who specializes in securities law.