STIFEL

HELPFUL TIPS FOR IDENTITY THEFT PROTECTION

What You Can Do If Your Personal Information Has Been Compromised

Stifel is issuing this information to provide clients with important steps they can take to safeguard their non-public personal identifying and financial information. Also included in this document are helpful measures clients should consider if they believe their personal information has been stolen or compromised, or believe they've been a victim of data breach.

Q: How can I protect myself from identity theft?

A: It is highly recommended that you never disclose your full social security number (SSN), credit card information, bank or investment account numbers, date of birth, passwords, and/or mother's maiden name to any person with whom you did not initiate contact and without having an established relationship with the requestor or the firm they represent. If you receive a call that you did not initiate from someone alleging they are "your credit card company or bank/investment firm," end the call and dial a known phone number (i.e., call the number on the back of the credit card or the statement) to validate the request. Never put this information in an e-mail communication. Do not reply to e-mails requesting this information. Links and attachments provided in unsolicited e-mail may route you to fake websites or contain viruses that can steal information from your computer.

The link below to the Federal Trade Commission (FTC) also has many important tips to prevent identity theft and provides steps to take if you have been the victim of identity theft.

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
https://www.identitytheft.gov/

Q: What if I have been the victim of identity theft?

A: 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, and other financial professionals immediately to report a 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.

Change your e-mail and/or online account passwords. Immediately change the password for all investment or financial accounts associated with potentially 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 or financial accounts, you may want to ask your firm to close the account and move the assets to a new account. You should consult your investment/banking firm about the best way to handle closing an account, if you choose to do so.

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 financial institution.

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**
(888) 397-3742	(800) 680-7289	(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.

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.

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

Q: What actions should I consider if my personal e-mail account was compromised or hacked by an unauthorized third person?

A: You should first regain control over your e-mail account by changing your password to a new, unique password. As your personal e-mail account may have non-public private information contained in e-mail messages received or sent, you should first take inventory of the contents of the communications in your inbox, outbox, and trash box e-mails. If there was any non-public identifying information, you may assume the unauthorized person has most likely seen the information. In a typical scenario, a hacker gains unauthorized access to your e-mail account, searches contents to locate an e-mail to or from an investment firm or bank, and replies to the message acting as you to gain information regarding the account and may attempt to illegally withdraw funds. Follow the above instructions to protect your information and accounts with firms with whom you do business.

Q: What actions should I consider if my personal cell phone was compromised or hacked by an unauthorized third person?

A: In addition to notifying your cell phone provider, similar steps to the above identity theft guidelines should be followed. As many people today utilize the technology contained in their cell phones to do so much more than just making phone calls and sending texts, it is essential to make sure that all of your bases are covered if the security of your device is compromised. After contacting your cell phone provider, you should take inventory of all of the ways you use your phone for financial transactions and communication. This would include but is not limited to: banking, investing, and shopping apps as well as any social media or other communication apps that could grant the hacker access to your financial information or contact lists. Once you have an idea of what apps may expose your personal data if infiltrated, go through each one and change the password. As stated above in the identity theft steps, you will then want to contact any financial or commerce company on your list to make them aware of any potential unauthorized transactions and have a fraud alert placed on your credit profile.

Q: What about the devices themselves? Should I take any additional steps to avoid residual affects?

A: Yes! You should consider taking your compromised device (phone, laptop, PC) to an authorized repair person and have it "scrubbed" for malware, trojans, or any other viruses the hacker may have installed. It is also recommended that users install (or update) antivirus software on their device.