Aspiriant Cares
What to do if your identity is stolen

If you just discovered that you are a victim of identity theft, or believe you may potentially become a victim (e.g., your wallet was lost or stolen), it's important to act immediately to address the problem. Your first steps should be to stop current fraudulent activity and prevent new fraud. Next, take measures to improve the security of your personal information to reduce the risk of additional identity theft.

Stop and prevent fraudulent activity

Here's what you can do to get a jump start on addressing the problem:

- ❑ If you haven't already, immediately alert any member of your Aspiriant client service team, preferably the Portfolio Administrator. We will help you notify your account custodian (Schwab, TDA, Fidelity, etc.) and take steps to secure your Aspiriant accounts.
- ❑ If someone has hacked your email account:
  - ❑ Immediately change your password to a new, stronger one.
  - ❑ Report it to your email provider.
  - ❑ Notify every financial institution you do business with about the security breach.
  - ❑ Do not make any online purchases until you run full anti-virus and anti-spyware scans and delete all threats on your computer.
  - ❑ Check your email mailbox settings to ensure no unexpected email addresses or rules/forwarders have been set up on your account.
  - ❑ Notify your contacts that someone has hacked your email account and that they may have received emails from you that you didn't send.
  - ❑ Seek professional assistance. Information technology experts can inspect your computer for compromising malware. They can also help you with your email settings. Many national computer retailers (such as Best Buy, Staples, Office Max, etc.) now provide local tech help.
- ❑ Visit www.IdentityTheft.gov. This excellent website by the Federal Trade Commission allows you to report identity theft and provides an action plan and contact information for many types of theft and fraud, such as lost or stolen credit cards, a data breach of a company that has your personal information, tax return fraud, government benefits fraud, email fraud and more.

Improve your security

Once you have addressed the immediate threats, you should improve all the personal security protections you have in place to reduce your risk for future information breaches.

- ❑ Never use the same logon and password for multiple websites. All your logons should have a different and unique password.
- ❑ Give better and constant attention to protecting your personal information.
- ❑ Create stronger passwords for critical accounts — bank accounts, credit cards, investment accounts, social media, etc.
- ❑ Add stronger security access procedures to all critical accounts, where available.
- ❑ Consider a cloud-based password management program to keep track of your passwords and to create unique and strong passwords (e.g., Last Pass or eWallet).
- ❑ Consider using a confetti paper shredder to destroy documents containing personal information.
- ❑ Take steps to actively monitor your credit or use a credit monitoring service.

Also, look into adding identity theft insurance coverage to your homeowners policy. And see whether you already have limited identity theft monitoring or insurance coverage available through your credit card companies, bank or specialty insurance programs (e.g., AAA).

We understand that being a victim of identity theft is scary, costly and time-consuming. Don't hesitate to reach out to your client service team for further guidance on how to minimize damage.

Learn more

The Federal Trade Commission is a good resource to help you protect your personal information. You can find out more about:

- ❑ Protecting all your connected devices (cell phone, tablets, readers, etc.).
- ❑ Avoiding email, mail and phone scams.
- ❑ Creating strong passwords.
- ❑ Ransomware.
- ❑ Protecting your children online.

Visit www.ftc.gov/onguardonline.

ASPIRIANT
aspiriant.com