

CYBER FRAUD RESOURCES

Investor protection checklist

The educational checklist presented below is designed to help you take appropriate action to better protect you and your family and mitigate risk of cyber fraud. Carefully review the items in each of the categories below to determine which apply to your unique situation.

TOPICAL AREA	ACTIONS TO CONSIDER	CHECK WHEN COMPLETED
Manage your devices.	<ul style="list-style-type: none">• Install the most up-to-date antivirus and antispyware programs on all devices and update these software programs as they become available. These programs are most effective when users set them to run regularly rather than just running periodic scans, which may not provide maximum protection to your device.• Access sensitive data only through a trusted device and secure internet connection; avoid use of public internet connections other than through a Virtual Private Network (VPN).• If you have children, set up a separate computer they can use for games and other online activities.• Keep operating systems and software up-to-date (PCs, laptops, tablets, smartphones). Many updates are made to resolve recently identified security risks.• Do not install pirated software. It often contains security exploits.• Frequently back up your data in case of ransomware attacks.	<ul style="list-style-type: none"><input type="checkbox"/> I've reviewed and understand all the items in this topical area.<input type="checkbox"/> I've taken action for those that apply to my situation.
Protect all passwords.	<ul style="list-style-type: none">• Avoid storing passwords in email folders or unencrypted files on your computer. Consider using a password manager program instead. These programs help generate and manage complicated passwords.• Use a personalized custom identifier for financial accounts you access online. Never use your Social Security number in any part of your login activity.• Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships, and avoid using a single password across multiple sites.• Utilize multi-factor authentication, especially for financial and email accounts.	<ul style="list-style-type: none"><input type="checkbox"/> I've reviewed and understand all the items in this topical area.<input type="checkbox"/> I've taken action for those that apply to my situation.
Surf the web safely.	<p>Exercise caution when connecting to the internet via unsecured or unknown wireless networks, such as those in public locations like hotels or coffee shops. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data directly, without the proper protection of a secure VPN connection.</p>	<ul style="list-style-type: none"><input type="checkbox"/> I've reviewed and understand all the items in this topical area.<input type="checkbox"/> I've taken action for those that apply to my situation.
Protect information on social media.	<p>Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birthdate, home address, and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays, or the loss of loved ones. Sharing too much information can make you susceptible to fraudsters and allow them to quickly pass a variety of tests related to the authentication of your personal information. Never underestimate the public sources that criminals will use to learn critical facts about people.</p>	<ul style="list-style-type: none"><input type="checkbox"/> I've reviewed and understand all the items in this topical area.<input type="checkbox"/> I've taken action for those that apply to my situation.

TOPICAL AREA	ACTIONS TO CONSIDER	CHECK WHEN COMPLETED
Protect your email accounts.	<ul style="list-style-type: none"> • Delete any emails that include detailed financial information beyond the time it's needed. In addition, continuously assess whether you even need to store any personal and financial information in an email account. • Use secure data storage programs to archive critical data and documents. • Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those warning that your computer is infected with a virus requesting that you take immediate action. • Establish separate email accounts for personal correspondence and financial transactions. • Choose a unique password and utilize multi-factor authentication. • Review all emails carefully before clicking on links or attachments. 	<ul style="list-style-type: none"> <input type="checkbox"/> I've reviewed and understand all the items in this topical area. <input type="checkbox"/> I've taken action for those that apply to my situation.
Safeguard your financial accounts.	<ul style="list-style-type: none"> • Consider contacting the three major credit bureaus to add a "security freeze" and prevent new accounts being opened in your name: <ul style="list-style-type: none"> – Equifax: 800-685-1111 – Experian: 888-397-3742 – Transunion: 888-909-8872 • Lock down personal credit reports with Experian®, TransUnion®, and Equifax®. Proactively enroll in an identity theft protection service to protect personal data. • Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held. • Never send account information or personally identifiable information over email, chat, or any other unsecured channel. • Suspiciously review any unsolicited email requesting personal information. Further, never respond to an information request by clicking a link in an email. Instead, type the website's URL into the browser yourself. • Avoid developing any online patterns of money movement, such as wires, that cyber criminals could replicate to make money movement patterns appear more legitimate. 	<ul style="list-style-type: none"> <input type="checkbox"/> I've reviewed and understand all the items in this topical area. <input type="checkbox"/> I've taken action for those that apply to my situation.