APOLLON

Cybersecurity & Fraud Prevention

Disclosure

This report is intended for the exclusive use of clients or prospective clients of Apollon Wealth Management, LLC (Apollon). The information contained herein is intended for the recipient, is confidential and may not be disseminated or distributed to any other person without the prior approval of Apollon. Any dissemination or distribution is strictly prohibited. Information has been obtained from a variety of sources believed to be reliable though not independently verified. Any forecasts represent future expectations and actual returns; volatilities and correlations will differ from forecasts. This report does not represent a specific investment recommendation. Please consult with your advisor, attorney and accountant, as appropriate, regarding specific advice. Past performance does not indicate future performance and there is a possibility of a loss.

Important Steps for Cybersecurity

PREVENT

1. **Strong Passwords:** Use a combination of numbers, symbols and letters to form a long, complex password. Use unique passwords for each online login and regularly change all passwords.
2. **Multi-Factor Authentication:** If available, enable two-factor authentication for email, social media, financial accounts, etc. This functionality sends a one-time code to a mobile device to verify access, thus preventing unauthorized parties from accessing your account without the code.
3. **Secure Wi-Fi Network:** Avoid unsecure access to public Wi-Fi networks, such as in coffee shops, airports, hotels, etc. A virtual private network (VPN) creates a personal, private network across public networks.
4. **Cautiousness with targeted telephone calls:** Avoid divulging any banking or personal information to a caller over the phone and do not give in to pressure to take immediate action. The IRS and law enforcement agencies will not call you. Beware of the question "can you hear me" which leads to the recording of you saying "yes" to authorize unwanted charges, etc.
5. **Safe Surfing:** Only open emails, attachments and links from people you know. Pay attention to a website's URL; hover over any links to see where they lead. Only visit trusted websites.

DETECT

1. **Account Review:** Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately.

2. **Review Your Credit Report:** By law, you can obtain a free credit report every 12 months from www.annualcreditreport.com. According to the Federal Trade Commission, this is the only authorized source for the free annual credit report (though it will not include your FICO score). You should review your credit report for any discrepancies (unauthorized accounts, etc.).

REACT

If you have been a victim of identity theft:

- File a report with the local law enforcement agency.
- File Form 14039 (Identity Theft Affidavit) with the Internal Revenue Service.
- Contact one of the three credit bureaus (Equifax, Experian, TransUnion) to report the crime and freeze credit. Once one of the credit bureaus issues a fraud alert, the other two bureaus are automatically notified.

Source: BBB Scam Alert – If callers asks, "Can you hear met?" just hang up
https://www.bbb.org/article/scams/5691-bbb-warning-if-caller-asks-can-you-hear-me-just-hang-up

Practical Steps to Guard Against Fraud

Spot imposters	Scammers often pretend to be someone you trust, like a government official, a family member, a charity or a company you do business with. Don't send money or give out personal information in response to an unexpected request — whether it comes as a text, a phone call or an email.
Don't believe caller ID	Technology makes it easy for scammers to fake caller ID information, so the name and number you see aren't always real. If someone calls asking for money or personal information, hang up. If you think the caller might be telling the truth, call back to a number you know is legitimate.
Consider how you pay	Credit cards have significant fraud protection built in, but some payment methods don't. Wiring money is risky because it's nearly impossible to get your money back; that's also true for reloadable cards (like MoneyPak or Reloadit) and gift cards (like iTunes or Google Play). Government offices and honest companies won't require you to use these payment methods.
Be skeptical of free trial offers	Some companies use free trials to sign you up for products and bill you every month until you cancel. Before you agree to a free trial, research the company and read the cancellation policy. Always review your monthly statements for charges you don't recognize.
Opt out of solicitations	Discuss opting out of solicitations to limit interaction with scammers. Registering phone number(s) on the Do Not Call Registry[5] to eliminate unwanted phone calls and contact the Direct Mail Association[4] to opt-out of receiving unsolicited mail.

If you spot a scam, report it at ftc.gov/complaint. Your reports help the FTC and other law enforcement investigate scams and bring criminals to justice. **If you or anyone you know has been a victim of exploitation, consider reporting this to** the Department of Justice National Elder Abuse Hotline **or to the** FBI Internet Complaint Center.

[1]*Source: FTC – 10 Things You Can Do to Avoid Fraud– https://www.commonlit.org/en/texts/10-things-you-can-do-to-avoid-fraud/*

[2]*Source: FTC – Report to help Fight Fraud - ReportFraud.ftc.gov*

[3]*Source: FTC – Scams – https://consumer.ftc.gov/scams*

[4]*Source: Direct Mail Association – Opt Out Service – https://www.dmachoice.org/*

[5]*Source: FTC – National Do Not Call Registry - https://www.donotcall.gov*

Questions to Ask an Apollon Advisor

How do I stay educated on trends in fraud?

Follow reputable news sources that report on fraud and cybersecurity issues, as these sources provide valuable insights into emerging scams and fraud trends.

Subscribe to newsletters or blogs from organizations which specialize in fraud prevention. Examples include newsletters from government agencies, financial institutions or cybersecurity companies.

What steps should I take if I suspect fraudulent activity?

Carefully review all bank and credit card statements for any unauthorized transactions.

Reach out to a credit bureau to verify your credit report is accurate. If you find any fraudulent activity, file a police report. Remember to keep a copy of the report as it may be needed when disputing charges.

After reporting to the police, contact your financial institution to report the activity.

How can I protect my personal information from being stolen?

Update passwords regularly, only visit safe and secure websites, and avoid giving out any personal information unless required.

If you suspect fraudulent activity on your account or would like more information on what you can do to prevent it, reach out to your financial advisor.

APOLLON

Apollon Wealth Management, LLC (Apollon) is a registered investment advisor. This document is intended for the exclusive use of clients or prospective clients of Apollon. Any dissemination or distribution is strictly prohibited. Information provided in this document is for informational and/or educational purposes only and is not, in any way, to be considered investment advice nor a recommendation of any investment product or service. Advice may only be provided after entering into an engagement agreement and providing Apollon with all requested background and account information. Please visit our website for other important disclosures.
www.apollonwealthmanagement.com