39th Edition 1st Quarter 2024

TILIA NEWS

INVESTMENT MANAGEMENT | FIDUCIARY ADVICE | RETIREMENT PLANNING

Tilia Fiduciary Partners Regulatory Updates

As of March 18th 2024, Tilia Fiduciary Partners recently updated its regulatory information with the U.S. Securities and Exchange Commission (SEC).

Per SEC guidelines, Tilia Fiduciary Partners is required to notify you of material changes to the business practices. The updates are as follows:

Tilia now provides **financial planning services for a fixed fee** depending on client complexity, and **consulting services for an hourly rate**. We do not monitor the investments made as a result of a fixed fee financial plan, unless you have hired us for portfolio management services.

Existing client relationships are not impacted by these changes!

Please find our updated ADV Form Part 2 and Form CRS available 24/7 on our website.

Beware: Spoofed Websites & Imposters

It is no secret that cyberattacks pose an increasing threat to investment advisors worldwide. With 75% of advisors reporting cyberattacks in some capacity, it is clear that cybercriminals continue to find ways to breach the seemingly secure systems holding your valuable information.

One of the fastest-growing scams investment advisors and their clients are facing involves “spoofed” websites. Simply put, cybercriminals are creating fake websites that appear to be run by the businesses you know and trust. These fraudsters purchase “sponsored links” to fake sites to increase their visibility in search engines such as Google, thus increasing the likelihood that unsuspecting users click on their links.

These malicious websites also use sophisticated techniques to deceive users, such as replicating branding elements, using similar website domain names, and copying security features. These deceptive sites can pose serious risks to investment advisors and clients by exposing them to potential malware, identity theft, and financial loss.

In addition to an increase in spoofed websites, fraudsters are now impersonating representatives of financial institutions via phone calls, emails, and text messages. These impostors use social engineering to get users to provide usernames and passwords. Once they have successfully breached your account, there is little stopping these cyber criminals from initiating unauthorized transactions.

The good news is that you can take steps to protect yourself.

- **Look for URL Errors:** Spoofed website addresses often contain misspellings or unusual domains. One letter out of place or an "O" replaced with a "0" might mean you are on a fake website.
- **Look for Grammar and Spelling Mistakes:** Trusted websites owned by legitimate companies take care to avoid errors. If you spot a grammar or spelling mistake in a website's content, that may be a clue it is not a legitimate website.
- **Do Not Share Login Information:** Financial institutions, such as Charles Schwab, do not ask you to provide account login information over the phone. Avoid sharing your login information, even if you think you are talking to an authorized representative.
- **Verify Security Features:** Authentic financial websites prioritize security measures, such as SSL certificates. Look for the padlock icon in the website's address bar to verify these security indicators.
- **Enable Multi-Factor Authentication (MFA):** Extra authentication is never a bad thing when it comes to protecting your identity and assets! Enabling this extra layer of security, such as opting to receive a security code via text message, can lower the risk of unauthorized account access.
- **Call Before Acting:** If you have concerns about a website, email, or text message, It is always best to call Tilia Partners at (910) 679-4093 before taking any action or clicking any links.
- **Report Suspicious Activity:** If it looks suspicious, it probably is! Both successful and prevented fraud attempts should be reported immediately to Tilia Partners and by calling Schwab Alliance at (800) 515-2157.

Sources: https://www.schwab.com/schwabsafe/avoid-imposter-scams

https://www.sec.gov/oiea/investor-alerts-and-bulletins/fraudsters-posing-brokers-or-investment-advisers-investor-alert

https://www.finra.org/investors/insights/be-alert-signs-imposter-investment-scams#:~:text=Bad%20actors%20behind%20imposter%20websites,investors%20to%20the%20imposter%20sites