Fraud Prevention Guidance

Stay Alert Against Fraud And Suspicious Activity

At Fortis Capital Advisors, safeguarding our clients, prospective investors, vendors, and employees from fraud is a top priority. We exclusively communicate through verified and official channels, such as recognized phone numbers, company email addresses, and in-person meetings. We do not engage in business or provide investment advice via private messaging apps like WhatsApp, WeChat, Telegram, Signal, or similar platforms. Moreover, Fortis will never provide investment advice, ask for sensitive personal information, or request payments through these unofficial methods.

Unfortunately, scammers may attempt to impersonate our employees or misuse the Fortis name to deceive others. Below are some common types of fraud and important tips on how to protect yourself. Please remember Fortis will never ask for your user name or password for any service.

Common Types Of Fraud

Fraudsters often use advanced methods to impersonate legitimate companies, including Fortis, in attempts to exploit individuals and organizations. Be cautious of the following schemes:

Email Phishing

Fraudulent emails may appear to come from a trusted source, asking for sensitive information, requesting payments, or prompting you to click on harmful links. These scams can lead to malicious websites or the installation of malware on your devices.

Text Phishing

In addition to being aware of email phishing scams, you might also receive text messages phishing for information from seemingly reputable companies. These text requests might mention changes to your account or ask you to verify your identity. Do not click on any links sent via text and contact your advisor immediately.

Impersonation Of Fortis Employees

Scammers may try to imitate Fortis employees by using our logos, creating fraudulent websites, or contacting you via unofficial channels. Always verify the authenticity of communications by checking that they originate from Fortis' official domain.

Phone Scams (Telemarketing)

Fraudsters may use phone-based schemes, including AI-powered voice impersonation, to deceive victims. They may claim you've won a prize, threaten legal action, or ask for personal information under false pretenses.

Identity Theft

Cybercriminals may attempt to steal your personal or financial information, such as Social Security numbers, to access your banking, credit, or investment accounts for illicit gain.

Cryptocurrency Scams

Scammers may use fake relationships to lure victims into fraudulent cryptocurrency platforms or wallets. These schemes often result in significant financial loss, targeting those unfamiliar with digital currencies.

Charity Fraud

In the wake of major disasters or crises, scammers may pose as representatives of charitable organizations to solicit donations. Be especially cautious of unsolicited requests via social media or crowdfunding platforms.

"Don't tell your advisor" Scams

Look out for fraudsters trying to convince you to take action such as move money, sell securities, or transfer your account and urge you to not tell your advisor or their compliance department.

Warning Signs Of Fraud

Look out for these red flags:

- Unsolicited requests for personal information or money via phone, email, or text.
- Unexplained charges or withdrawals from your accounts.
- Urgent communications designed to pressure you into taking quick action, such as time-limited offers or threats of penalties.
- New or unfamiliar accounts or inquiries appearing on your credit report.
- Fraudulent "Officials" trying to convince you that your Fortis advisor might be the one who is scamming you, forcing you to hide the real scam from your advisor.
- Urgent requests to share or provide control of your computer screen.
- Requests for user names or passwords.

Steps To Protect Yourself

Being proactive is the best defense against fraud. Here's how you can protect your personal information and assets:

- Avoid opening attachments or clicking links from unfamiliar sources.
- Always verify calls by contacting the organization directly through a trusted number.

- Scrutinize email addresses and website URLs for slight misspellings or other inconsistencies.
- Use strong, unique passwords and update them frequently.
- Enable two-factor authentication (2FA) on your accounts where possible.
- Limit the amount of personal information you share online, particularly on social media.
- Block suspicious calls and texts.
- Consider using identity protection services offered by reputable credit bureaus.
- Never share or give control of your computer screen to a third party.

Reporting Fraud Or Suspicious Activity

If you believe you've encountered fraudulent activity involving Fortis Capital Advisors, please contact Fortis' compliance department at compliance@Fortiscapitaladvisors.com or 414-312-4579.