The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

ICI VIEWPOINTS

November 21, 2024

Verify, Then Trust: Preventing Online Investment Scams

Investment fraud is on the rise as scammers devise ever more sophisticated schemes that harm individual investors. Due to artificial intelligence (AI), these scams are getting easier to perpetrate and harder to spot. As International Fraud Awareness Week draws to a close, ICI is alerting investors to common online fraud schemes involving regulated funds and recommending steps to take if you encounter them.

Online Imposter Fraud

In this prevalent scheme, fraudsters try to trick unsuspecting investors into believing that they are legitimate money managers. They ply investors to turn over important information or their hard-earned savings for "investments," never to be seen again. Two common imposter fraud schemes, described below, take place through fake websites and fake chats or messages:

Cybersquatting

Cybersquatters are bad actors who establish websites that look nearly identical to ones from real asset managers. Instead, the websites phish for client information, such as Social Security numbers, account identification, and passwords. The bad actors then use the acquired information to misappropriate the investor's assets.

Social Media "Investment Group" Scams

This scheme takes much less effort but is just as effective. Bad actors use fund names and images on third-party platforms (*e.g.*, WhatsApp, Facebook, or Telegram) to set up "investment clubs," even using the names of real, high-profile portfolio managers to entice individuals to invest with them. Some imposters go so far as to cite a broker's registration number.

Investors may then send them real assets to invest, not knowing their monies go straight into the bad actors' pockets. Fraudsters often lure investors with the promise of cryptocurrency allocations through well-known firms or a guaranteed rate of return, so long as investors are willing to pay the "upfront" trading costs. While social media platforms may be aware of imposter activities, they often are not required to remove such links or posts from their site.

Account Takeovers

Online account takeovers, especially 401(k) account takeovers, are surging because they are easy to execute. Using sophisticated, readily accessible generative AI tools, scammers

can create fake identification documents and credentials. Armed with stolen personal data, scammers call retirement plan sponsors to update employee information; they then access and steal money from retirement accounts. Plan sponsors are stepping up their online and phone enforcement efforts with a digital ID verification process to deepen the protections in place for account holders.

Tips for Keeping Your Investments Safe

The SEC and other financial regulators are working to mitigate investment fraud, developing ways to enable digital authentication and verification to ensure the websites you visit and the messages you receive come from the investment firms and people they purport to be. While that project is underway, it will take some time to develop the necessary technology and obtain the regulatory approvals needed for implementation. Until then, follow these steps to protect your money:

1. **Treat the Website or Message Skeptically.** Before visiting a website or responding to a message, think about why this person is directing you to the website or sending you the message and whether such person would send the type of message you received. Is it unsolicited? Are there promises of massive returns with little risk? Is there a pressurized push to invest? Are you asked to pay by credit card, gift card, or through wires to foreign or personal accounts? These are signs the investment opportunity may be a scam.

2. **Never Share Your Personal Information via Social Media.** This includes your address, banking details, credit card data, or Social Security or Tax Identification Number. Reputable investment firms do not solicit this type of information via social media. They are obliged to safeguard your personal data.

3. **Look Out for Common Tactics Used by Fraudsters.** These include seeking upfront money to defer costs, stating the offer is only available for a certain segment of the investing public (such as seniors, first movers, those who support certain “social causes,” etc.), claims to move “fast” or “early” to avoid “losing out,” as well as promises or guarantees of future earnings.
.
4. **Look for Common Errors.** Fraudulent websites or messages often contain grammatical errors, misspellings, poor design quality, or urgent requests.
.
5. **Verify the Sender.** Check the domain name (like www.ici.org) of any website you visit or try to verify who sent the message. Always compare the source to a known legitimate website or phone number from bills, statements, or other reliable documents. You can conduct a separate internet search for firms that are broker-dealers and their registered representatives on FINRA’s Broker Check website or find information about registered investment advisers and their representatives on the SEC’s Investment Adviser Public Disclosure (IAPD) website. The IAPD also provides a list of actual websites that each registered investment advisory firm uses. If you cannot verify the sender, do not click any links directing you to another page and do not reply. Simply delete the message.
.
6. **Contact Regulators.** Both the SEC and FINRA encourage you to contact them if you have concerns about who you are dealing with. Contact the SEC’s Office of Investor Education at (800) 732-0330 or FINRA’s Complaints and Tips Office at (301) 590-6500.

By following these steps, you can ensure any contacts and investment requests you receive are legitimate. For more tips on recognizing investment fraud, explore these helpful resources:

- The SEC’s Red Flags of Investment Fraud Checklist
- Be Alert to Signs of Imposter Investment Scams
- Use Caution When Responding to Messaging Apps
