THE Wealth REPORT

Scammers rely on fear, intimidation and manipulation of vulnerable people. Remain vigilant and alert to avoid becoming their next victim.

INVESTOR BEWARE

Avoiding fraud starts with knowing the signs of a scam

Overview

$1.03 trillion: That's how much scammers took from unsuspecting people worldwide between November 2023 and November 2024. Americans were hit especially hard, averaging losses of $3,520 per scam victim.[1]

One of the reasons for the big number is that many people didn't recognize the signs of the scam until it was too late. In the 2024 Global State of Scams study, 33% of survey respondents said they didn't know what a scam looks like.[2] The reason? Scammers are getting savvier — and it's getting increasingly more difficult to determine fact from fiction.

Protecting yourself from fraud starts by knowing the common types of scams and identifying the signs that you might be a scammer's next potential target.

Cyber Fraud

According to the Association of Certified Fraud Examiners, cyber fraud is still an area of high concern. Law enforcement, corporations and individuals have reported an increasing number of attempted ransomware attacks and/or business compromise schemes over the past few years.[3]

One common type of cyber fraud is "social engineering," in which scammers use human interaction to trick people into abandoning standard security protocols for a "friend." For example, a grifter may pretend to be a friend or colleague and encourage someone to open an email attachment that is infected with malware or to divulge confidential information. The scammer may use scare tactics to warn an individual that his computer is vulnerable to cyber attacks, urging him to install and run the malware they provide.

Of course, many successful fraud attempts don't rely on technology. In fact, some low-tech scams are highly lucrative — and they've stuck around for decades as a result. Here are some of the most common types of scams to avoid:

Ponzi Schemes

In the 1920s, a man named Charles Ponzi duped people into investing in a postage stamp speculation scheme.[4] Today, a "Ponzi scheme" is the ploy of soliciting investors with the promise of high returns and then using funds from subsequent investors to pay those returns. Along the way, the grifter skims some of the money, making it a lucrative, sustainable scam with a constant flow of new money.

Since Ponzi schemes tend to share common characteristics, one of the keys to avoiding them is to identify certain red flags:

- The promise of high returns with little to no risk
- Returns that are miraculously consistent year after year, regardless of market conditions
- An investment that is not registered with the SEC or state regulators, which require that investors receive information about the company's management, products, services and finances
- An investment sold by an unlicensed or unregistered seller
- Investments that tend to have account statement errors may signal that funds are not invested as promised
- Difficulty receiving payments or cashing out; you may be offered even higher returns for remaining invested

Fake CDs

Investors tend to look for "safe havens" during periods of market volatility. This is the ripest environment for scammers to lure investors with fake certificates of deposit (CDs) that promise fixed-rate returns. Fraudsters may even go so far as to create digital advertisements and websites that resemble those of legitimate financial institutions. Fraudulent websites selling fake CDs may:

- Offer higher-than-market interest rates with no penalties for early withdrawals
- Promote only CDs and offer no other banking or brokerage accounts or loan products
- Require high minimum deposits, such as $200,000 or more
- Instruct investors to wire funds to an account located outside the U.S. or to a U.S.-based account other than the financial institution claiming to sell the CD
- Claim that the CD is insured by the Federal Deposit Insurance Corporation (FDIC)
- Claim that their "clearing partners" are registered with the SEC

To avoid being duped into buying a fake CD, investors should consider doing some homework first. Even if you think you're buying from a reputable and recognizable financial institution, first check out these tips:

- Conduct an internet search for the financial institution offering the CD you are considering to see if the results lead to another website. Call the financial institution using a telephone number found somewhere other than the suspect website to verify its legitimacy.

The Wealth Report

- Verify the CD and financial institution are FDIC insured via the BankFind tool at https://banks.data.fdic.gov/bankfind-suite/bankfind. Confirm the exact name of the financial institution (not just something similar).
- If you are considering a CD offered by a credit union, verify via the National Credit Union Administration's (NCUA) "Research a Credit Union" webpage at https://mapping.ncua.gov or call the NCUA's Consumer Assistance Center at 800.755.1030.
- Use the Financial Industry Regulatory Authority (FINRA) BrokerCheck database at https://brokercheck.finra.org to confirm the broker's address matches the address for the financial product.
- Google the name of the offering financial institution followed by "scam" to see if there's been a recent rise of reported attempted fraud.

Unregistered Investments With High Yields
High-yield investment programs (HYIPs) are unregistered investments typically run by unlicensed individuals with a promise of incredible returns (e.g., 30% or more) at little or no risk to the investor. Some of these scams may use the terms "prime bank" or "microcap stocks."[5] A so-called prime bank instrument is one that promises a guaranteed high investment return with little or no risk.

Microcap stocks are actual, low-priced stocks issued by very small companies from emerging technologies or industries, such as Initial Coin Offerings (ICOs) and digital assets. Scammers promote the stocks via independent and unbiased sources such as investment research websites, investment newsletters, online ads, direct mail, newspapers, magazines and radio. However, publicly available information about microcap stocks is typically scarce, which makes it easier for scammers to spread false information and manipulate their prices. Microcaps tend to be less liquid and generally do not trade on a national securities exchange. To research microcap stocks, search for company information on the websites of DBOT ATS (https://dbottrading.com), Global OTC ATS (https://www.globalotc.com) and OTC Link ATS (https://www.otcmarkets.com).[6]

Community-Based Financial Scams
Another way fraudsters make a lot of money quickly is by exploiting tight-knit communities that have established trust and friendship. Once a scammer is able to ingratiate themselves with a member of such a community, they can use that person as a referral to others within their circle. Scammers often use this tactic to target groups with common ties based on ethnicity, nationality, religion, sexual orientation, employment, age or disabilities.

Also referred to as affinity fraud, a scammer often infiltrates a targeted group by enlisting the group leader(s) to recommend the product. Those leaders may also be victims because they do not realize the “investment” is really a fraud. The key is to always conduct your own due diligence, regardless of how much you trust a friend or family member’s recommendation. Check out https://investor.gov for search tools to investigate the seller’s background, license and registration status.

Social Media Scams
The internet and social media offer a plethora of opportunities for scammers to reach potential victims, especially since it’s easy to create authentic-looking websites and social media profiles. Fraudsters can reach a wide audience with minimal effort or expense through emails, a web page or social media followers. Always vet any investment “opportunity” advertised on the internet or social media before providing any contact information. Sometimes, promotions are designed simply to get your personal details, which scammers can later use to create elaborate schemes or sell to other scammers. Research investments through well-known, legitimate resources, and consult with a trusted financial advisor to find out more about investments promoted on the internet.

Final Thoughts

Scammers have existed for centuries — and they will continue to find new and innovative ways to part people from their money. That’s all the more reason to work with a trusted, experienced and registered financial advisor for your investment decisions, no matter how big or small the decision is. It never hurts to have a second opinion, especially from a financial professional who works in the investment industry and has the experience to help in these situations. Not only are two heads better than one, but you get even more from a responsive financial professional and may be able to benefit from all of their resources. Working with an advisor gives you a knowledge base from which you can vet ideas, ask questions and make decisions based on your total financial picture.

We also recommend discussing investment and finance decisions with your spouse, partner, adult children, or other trusted friend or family member. The more people involved, the more perspectives you get that can help prevent inappropriate decisions or poor timing for your situation. If you do fall prey to a scammer, contact the SEC, FINRA, state securities regulator and financial advisor for assistance.

Sources

[1,2] Betty Lin-Fisher. USA Today. Nov. 7, 2024. "Scam losses worldwide this year are $1 trillion. How to protect yourself." https://www.usatoday.com/story/money/2024/11/07/scam-victims-1-trillion-losses/75967565007/. Accessed Jan. 9, 2025.

[3] Association of Certified Fraud Examiners. "Occupational Fraud 2024: A Report to the Nations®." https://legacy.acfe.com/report-to-the-nations/2024/. Accessed Jan. 9, 2025.

[4] Jim Probasco. Investopedia. Nov. 16, 2024. "Who Was Charles Ponzi? What Did He Create?" https://www.investopedia.com/who-is-charles-ponzi-5216783. Accessed Jan. 9, 2025.

[5] Department of Financial Protection & Innovation. "High Yield Investment Programs (HYIPs) – Don't Get Scammed." https://dfpi.ca.gov/news/insights/high-yield-investment-programs-hyips-dont-get-scammed/. Accessed Jan. 9, 2025.

[6] Investor.gov. "Microcap fraud." https://www.investor.gov/additional-resources/spotlight/microcap-fraud. Accessed Jan. 9, 2025.