THE Wealth REPORT

INVESTMENT SCAMS ON THE RISE

Overview

In 2020, the U.S. Securities and Exchange Commission (SEC) issued an alert regarding a significant increase in investment scams. The sudden rise was attributed to the outbreak of the virus and subsequent market and economic declines. According to analysis of consumer complaint data by the Federal Trade Commission (FTC), there was a 70% upsurge in income scams during the second quarter of 2020 compared to the same period in 2019.[1]

The FTC reports that Americans lose more money on investment scams than any other type of income fraud. While the median loss is just above $16,000, people in their 50s and 60s — the age when many are motivated to make up for lost ground with retirement savings — lose an average of $24,000.[2]

One of the most potent schemes used by scammers is taking advantage of people who are vulnerable during times of fear and uncertainty. The current pandemic is one of those times.

Cyber Fraud

According to the Association of Certified Fraud Examiners, cyber fraud appears to be the fastest-growing concern. Law enforcement, corporations and individuals are reporting substantially more attempts at ransomware attacks and/or business compromise schemes.[3]

Another form of cyber fraud is "social engineering," in which scammers use human interaction to trick people into eschewing 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.

The following are some of the most prevalent financial scams being perpetrated during the pandemic.

Ponzi Schemes

In the 1920s, a man named Charles Ponzi duped people into investing in a postage stamp speculation scheme. What we refer to today as 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 — and the scam continues on like that. Along the way, the grifter skims some of the money for himself, making it a lucrative, sustainable scam with new money constantly flowing in.

Since Ponzi schemes tend to share common characteristics, the key is to identify certain red flags:[4]

- 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 most ripe environment for scammers to lure investors with fake certificates of deposit (CDs) that promise fixed-rate returns. In fact, they may go so far as to create online advertisements and websites (and URLs) that resemble those of legitimate financial institutions. Spoof websites selling fake CDs may:[5]

- 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 do 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.

- Verify the CD and financial institution are FDIC insured via the BankFind tool at https://research.fdic.gov/bankfind, or call 877.ASK.FDIC (877.275.3342). 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/ResearchCreditUnion.aspx, 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 that the broker's address matches the address for the financial product.

- Google the name of the offering financial institution followed by "complaint."

High-Yield Investments

Pandemic Opportunists
With various tests, cures and vaccines being developed for the coronavirus, people may be tempted to invest in pharmaceutical stocks to take advantage of the upsurge in manufacturing and distribution. However, be aware that fraudsters can boost the price of the stock of publicly traded companies by promoting that the products or services will help contain COVID-19. They may even claim to have "inside information" about a development that will be positive for the stock.

Pump-and-Dump Schemes
Be aware that these scammers may be engaging in a "pump-and-dump" scheme. The first phase of this scheme is to promote a specific stock so that lots of investors buy in, driving up the price of the stock. The second phase is when fraudsters sell their own shares while prices are high. Once the hype is over, prices drop and duped investors lose their money. Even though the stock and company may be legitimate, the promotion is a scheme designed to make money for the scammers.

HYIPs
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."[6] 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 advertisements, direct mail, newspapers, magazines and radio. However, publicly available information about microcap stocks is typically scarce, which makes it easier for fraudsters 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 (http://www.otcmarkets.com).[7]

Community-Based Financial Scams

Another way fraudsters make a lot of money quickly is by exploiting tight-knit communities that have an established trust and friendship. Once a scammer is able to ingratiate himself with a member of such a community, he can use that person as a referral to others who trust his judgment. Scammers often use this tactic to target groups with common ties based on ethnicity, nationality, religion, sexual orientation, work ties or age. For example:

- Military service members
- Seniors
- Small-business owners
- Members of the Amish, Mennonite, Hispanic and Haitian communities
- Deaf, hard of hearing, and hearing loss communities

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 also may 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 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 information for nearly every type of investment. In fact, the Federal Trade Commission reported that during the pandemic, 94% of fraudulent complaints that mentioned a social media website cited Facebook or Instagram. Also note that scammers are able to delete any negative comments posted regarding their ads or posts, so it may appear that everyone who interacted with the company had a positive experience.[8]

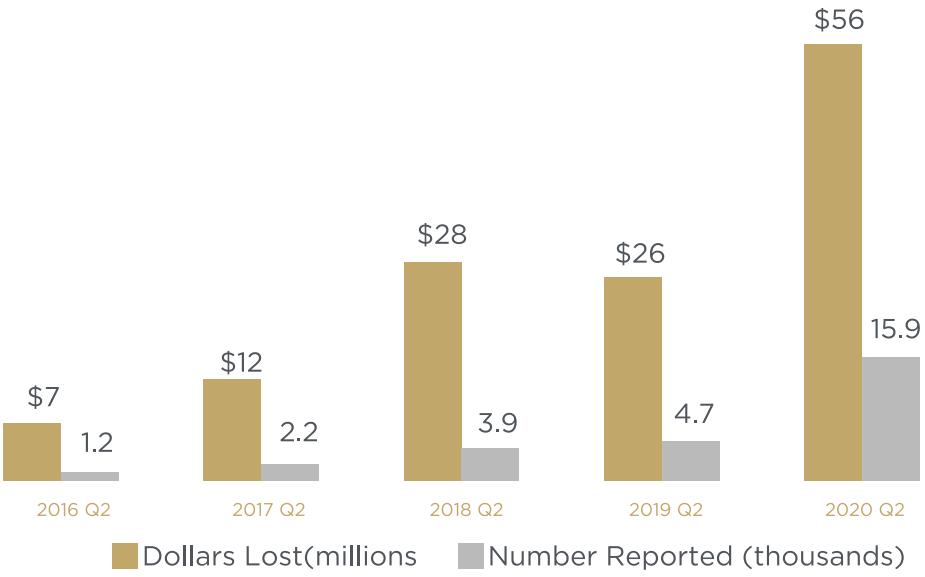
Recognize that it is relatively easy to create authentic-looking websites, news portals and other mediums for false information, and cyber criminals are quite expert at using new technology to create fraudulent schemes. They can reach a wide audience with minimal effort or expense through emails, a website or social media followers.

Always vet an investment "opportunity" — even before providing your contact information. Sometimes, those promotions are designed simply

to get personal information, which they can use later to create elaborate schemes or sell to 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.

People who reported scams that started on social media lost nearly $117 million in just the first half of 2020. Most of those fraudulent claims were related to the government's economic relief, income opportunities, online shopping that didn't deliver the goods and even dating scams.

Rise in Social Media Scams: 2016 – 2020[9]



"Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits."[10]

Final Thoughts

Yes, there are criminals out there who want to take your money. That is all the more reason to work with a trusted, experienced and registered financial advisor for all of your investment decisions — no matter how small those decisions may seem. It never hurts to have a second opinion, especially from a professional who works in the investment industry and has your best interests at heart. 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 the resources he or she has access to. All told, working with an advisor gives you a knowledge base from which to vet ideas, ask questions and make decisions based on your total financial picture.

Also, we recommend that you discuss investment and finance decisions with your spouse or partner or other family members. The more people involved, the more perspectives you get that can help prevent

inappropriate decisions or poor timing for your situation. After all, if something should happen to you, your loved ones need to know where your money is invested and understand when and why you made that decision. The more your financial advisor and partner know about your decisions, the more they can support them.

However, if you believe you have encountered or become a victim of fraud, contact the SEC, FINRA or your state securities regulator for assistance.

---

[1] *Greg Iacurci. CNBC. Dec. 15, 2020. "Ponzi schemes, other investment fraud on rise during pandemic, SEC says." https://www.cnbc.com/2020/12/15/ponzi-schemes-other-investment-fraud-on-rise-amid-pandemic-sec-says.html. Accessed Jan. 4, 2021.*
[2] *Ibid.*
[3] *Michael Cohn. Accounting Today. Sept. 11, 2020. "Fraud on the rise during coronavirus pandemic." https://www.accountingtoday.com/news/fraud-on-the-rise-during-coronavirus-pandemic. Accessed Jan. 4, 2021.*
[4] *U.S. Securities and Exchange Commission. 2021. "Ponzi Scheme." https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme. Accessed Jan. 4, 2021.*
[5] *U.S. Securities and Exchange Commission. March 27, 2020. "Beware of Spoofed Websites Offering Phony Certificates of Deposit — Investor Alert." https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/beware. Accessed Jan. 4, 2021.*
[6] *U.S. Securities and Exchange Commission. 2021. "High Yield Investment Programs." https://www.investor.gov/protect-your-investments/fraud/types-fraud/high-yield-investment-programs. Accessed Jan. 4, 2021.*
[7] *U.S. Securities and Exchange Commission. 2021. "Microcap Fraud." https://www.investor.gov/additional-resources/spotlight/microcap-fraud. Accessed Jan. 4, 2021.*
[8] *Emma Fletcher. Federal Trade Commission. Oct. 21, 2020. "Scams starting on social media proliferate in early 2020." https://www.ftc.gov/news-events/blogs/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020. Accessed Jan. 4, 2021.*
[9] *Ibid.*
[10] *FBI. March 20, 2020. "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic." https://www.ic3.gov/Media/Y2020/PSA200320. Accessed Jan. 4, 2021.*

1/21-1468123