

FINANCIAL PLANNING NOTES CLIENT NEWSLETTER

IN THIS ISSUE:

INVESTING WITH THE RUSSIAN BEAR

6 NEW ONLINE SCAMS YOU NEED TO KNOW ABOUT 2

INVESTING WITH THE RUSSIAN BEAR

With the Russian Bear Market (copyright pending) on us, we have yet another opportunity to talk about the folly of market timing. As I am writing this article on May 21, 2022, capital markets have just concluded eight straight weeks of losses, with the S&P 500 passing the mystical 20% decline mark that prompts economists to declare that we are in a bear (downward-trending) market.

As our seasoned clients well know, we are invested for the long haul and see no reason to change our investment strategy. The risk of market timing, or moving to the sidelines when markets decline, is illustrated in the chart at right.

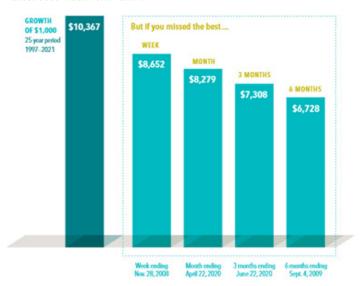
The chart tells us the return you would have gotten for a diversified investment in the largest 3,000 U.S. companies over the last 25 years—a tenfold return on your money! But just missing a few poorly timed days or weeks would have cost you severely, erasing large chunks of that total gain.

Now pay close attention to the specific dates that are excluded: One week in November 2008, March and April of 2020, March through June 2020, and March through September 2009. These four periods all occurred in the midst of the two steepest market declines on record for that 25-year period!

This is not a coincidence. Steep market declines signal periods of high market volatility, and during those periods, we expect markets to also intermittently show large increases. And that is just what happened in November

2008 after September and October saw markets in freefall following the collapse of Bear Sterns and a worldwide credit panic. It is also what we saw after markets finally hit the bottom of the Great Recession in March 2009 and quickly came roaring back over the next six months.

Exhibit 1. The Cost of Trying to Time the MarketRussell 3000 Index Total Return¹



1 In US dollars. For illustrative purposes. Best performance dates represent end of period (Nov. 28, 2008, for best week; April 22, 2020, for best month; June 22, 2020, for best 3 months; and Sept. 4, 2009, for best 6 months). The missed best consecutive days examples assume that the hypothetical portfolio fully divested its holdings at the end of the day before the missed best consecutive days, held cash for the missed best consecutive days, and reinvested the entire portfolio in the Russell 3000 Index at the end of the missed best consecutive days. Frank Russell Company is the source and owner of the trademarks, service marks, and copyrights related to the Russell Indexes.





Similarly, the other two time periods are overlapping and follow the "Month from Hell" at the beginning of the Covid pandemic and ensuing market panic in March 2020. As soon as that panic wore off, markets roared back with their best month in April and two more high-return months in May and June.

The bottom line is this: We have no evidence that market timing is an effective strategy for long-term investing success, but there is evidence it is even more foolhardy following a steep market downturn. While we have no guarantee of the future, we're better off staying invested, with reasonable expectations of outstanding performance to come.

For more on the Russian Bear and its potential investing impact, check out our article "Why Geopolitics Shouldn't Change Your Investment Strategy" (https://www.northstarplanners.com/blog).

—Steve Tepper

Chart provided by Dimensional Fund Advisors. Past performance is not a guarantee of future results. Indices are not available for direct investment. Their performance does not reflect the expenses associated with the management of an actual portfolio. Dimensional Fund Advisors LP is an investment advisor registered with the Securities and Exchange Commission.

6 NEW ONLINE SCAMS YOU NEED TO KNOW ABOUT

I've written many times about online frauds and scams, but sadly, there are always new, horribly creative scams popping up all the time. Here are a few newly popular illegal schemes you should be aware of:

1. The Overpayment: Beware of online transactions with strangers via Venmo, Zelle, or other cash apps. If you are selling something online for \$200, you may receive a payment of \$2,000. An innocent enough mistake, right? He just added an extra zero. The buyer will request you to send back \$1,800. Everything's hunky-dory, right?

Nope. The \$2,000 deposit the buyer made to your bank was fraudulent and will be reversed. The \$1,800 transfer you made, however, will not be undone because it went to the thief's account and was immediately transferred out.

Never, NEVER, give a refund to a stranger until the original transaction has posted and settled. Verify with your bank how much time is required to be sure the transaction will not be reversed.

2. Amazon Scam: The Federal Trade Commission says one-third of business-impersonator complaints involve Amazon.

There are different types of scams involved. One is the overpayment of a refund, as described in the previous scam. Another is to tell you your account was hacked, and somehow the only way to protect it is the gift card scam, described below.

If you are contacted by Amazon about a transaction or refund you aren't familiar with, call Amazon customer support directly at 888-280-4331.

3. Tinder Investing: Online investment scams are as old as the internet. They've traditionally taken the form of instant messaging, phishing emails, and robocalls.

But criminals have become far more insidious in their efforts. Realizing they can con far larger dollar amounts



through affinity, they've taken to the "long con" route of posting fake profiles of attractive women on dating websites, matching with wealthy men, and bombarding them with attention through constant chat and messages.

Once intimacy is established, they hit the victim up with time-sensitive investment opportunities, often involving cryptocurrencies. Of course, the investment is bogus, and once money is transferred, the perpetrator blocks the victim's account (unless they think they can get more money later).

Warning signs are numerous: Even though the profile says the woman is located nearby, she will claim she is in Hong Kong or Singapore but will return to the U.S. "soon." Photos will look generic as if they are from someone's social media account (because they are!). In chats, she will always agree with her target on every topic. And she will have an interest in investing and crypto that she will talk about many times before the "ask."

If the objective of the match isn't investing, it can also be to scrape information to breach the victim's accounts. Beware if your online romantic partner suddenly asks you what street you grew up on!

4. Recruiting Fraud: In the age of social media and chat, you can apply for a high-paying job, be interviewed, and get hired in just days or hours, all without ever stepping foot inside the company's offices or even meeting anyone from the company! Sound too good to be true? Well, often it is.

Ask Lara Lafferty, who recently went viral on TikTok with a video describing her recruitment experience with Delish, a food media site. In just one day, she submitted

an online application for a lucrative freelance job, was almost immediately contacted by someone claiming to be from Delish's HR department, had an online interview via Skype chat, and was offered the job.

During the process, Lafferty looked up the people she thought she was talking to—they were listed on LinkedIn as employees of Delish. Everything seemed to check out.

Then she was told they would send her an invoice for a work computer. That led her to call the HR department of Delish directly. The job listing was fake, and the people she was chatting with online were not from the company's HR department.

Lara didn't fall for the scam beyond the wasted time and emotional letdown. But many do. Beware of quick job offers, and verify the listing by calling HR directly.

5. Friend Needs Money: This is another long con employed by many fraudsters who have access to millions of email accounts but don't immediately act to monetize that access. They will monitor email activity and then impersonate someone you are regularly in contact with, asking for money.

This is not a new con but used to take the form of an emergency involving a friend or family member who was out of the country, couldn't communicate by phone, and needed money following a theft, accident, or arrest. Now the con is more brazen. A friend is at a store trying to buy a birthday present, and her credit card has been declined. Can you buy a gift card and write her back with the activation code?

If you trust that you are actually talking to your friend, you might just blow right by the many obvious red flags: Why

WHO WE ARE

ALLEN P. GIESE, ChFC[®], CLU[®], ChSNC[®] President, Investment Advisor Representative

STEVE TEPPER, CFP®, MBA

Vice President, Chief Operations Officer, Investment Advisor Representative

GARY S. GLANZ

Director of Business Development, Investment Advisor Representative

FELIPE MEJIA, CFP®

Senior Advisor, Investment Advisor Representative

CHARLES THOMAS

Associate Advisor, Investment Advisor Representative

GARY C. GONZALEZ

Investment Advisor Representative

STACY SAAVEDRA

Director of Client Services

RICHARD LOTTIER III

Client Service Specialist

LIAN TEPPER

Client Service Specialist



(954) 693-0030

1250 S. Pine Island Road, Suite 275 Plantation, FL 33324

northstarplanners.com

info@northstarplanners.com

is she emailing you, not calling? Why a gift card? She's your friend. You'd trust her with a credit card or debit card number. (Answer: Con artists prefer gift cards because they are harder to trace and offer little protection.)

Your best protection is to contact your friend via a different communication method to verify it's her.

6. Online Puppy Scam: According to the Better Business Bureau, online purchase scams posed the biggest threat to consumers in 2021, and believe it or not, the most popular purchase item is puppies. The scam is as simple as can be: You buy an item online and pay for it, and the seller sends you nothing.

While this is most common on made-up e-commerce websites, even the Amazons of the world have their share of bad actors.

Your two best methods of defense against an online purchase scam are to only buy through known, reliable online marketplaces and use a credit card for your purchase to limit your potential loss.

In summary, the best means of protecting yourself from online fraud, according to AARP, are:

- Don't commit to any investment without first knowing who you are investing with. Check any broker or advisor's credentials through brokercheck.finra.org.
- Ignore "act now" tactics. Take time to make an important decision about money.
- Never answer phone calls from unknown numbers. If it's important, the caller will leave a message.

— Steve Tepper

Sources:

"Beware: 8 Red-Hot Frauds" by Sari Harrar, aarp.org, April 11, 2022.

"Amazon Impersonators: What You Need to Know" by Maria Mayo, consumer.ftc.gov, October 20, 2021.

"The Latest Scams You Need to Be Aware of in 2022" by Louis DeNicola, Experian.com, March 31, 2022.

The CLU®, ChFC® and ChSNC™ are the property of The American College, which reserves the rights to their use, and are used by permission.

Certified Financial Planner Board of Standards Inc. owns the certification marks CFP®, Certified Financial Planner™, CFP® (with plaque design) and CFP® (with flame design) in the U.S., which it awards to individuals who successfully complete CFP Board's initial and ongoing certification requirements.

In accordance with rule 204-3(c) of the Investment Advisors Act of 1940, Northstar Financial Planners, Inc. hereby offers to deliver, without charge, a copy of its brochure (Form ADV Part 2) upon request. You may view, print or download our brochure at www.northstarplanners.com, request a copy by contacting us via email at info@northstarplanners.com, or by phone at 954-693-0030.