



Wealth Care LLC May 2026 Commentary

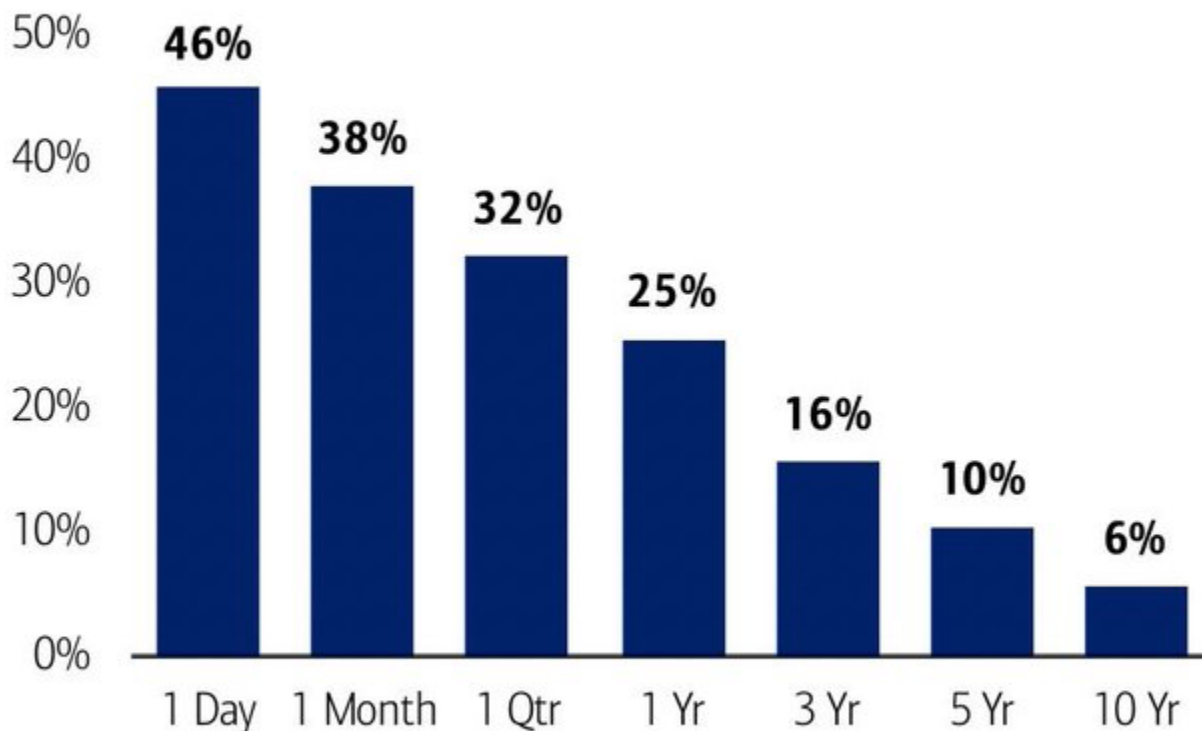
Investing Thoughts

Being patient is a crucial part of investing success. Just under half of all days in the markets are at a loss (and we feel a loss much more than a gain). But as time progresses, our likelihood of losing money begins to disappear. During this long slow time, it is so very easy to be derailed by emotions.

Have Patience

Exhibit 2: As time horizons grow, equity losses fall off

Probability of negative returns, based on S&P 500 total returns from 1929-present



Source: S&P, Bloomberg, BofA US Equity & Quant Strategy

BofA GLOBAL RESEARCH



Bond Risks

Fixed income carries its own risks—primarily what we call “credit risk” and duration risk. Credit risk is the chance that the borrower cannot repay some or all of what they borrowed from you (or don’t pay the interest as promised). Think “junk bonds” as an example. But duration risk can be a killer also. Say you lend someone money for a long time period. You assume both some credit risk (things change even with currently solid borrowers) but you also risk losing out on higher returns if interest rates rise, and you lose as inflation erodes the value of both your income stream and the eventual return of your investment. Here is an extreme example—The nation of Austria issued 100 year bonds in the midst of the Covid pandemic. Remember that interest rates were almost zero at that time, and this bond promised a 2.1% per year return.

Austria's Century Bond Has Plunged From Its Peak

Long maturity, low coupon mean security is highly volatile

— Austrian bond maturing in 2120



Source: Bloomberg

Bloomberg

Presumably the credit risk is/was low—Austria should stick around. But the people that bought these bonds are now stuck for another 95 years getting an interest rate less than inflation. Usually, shorter term bonds pay a lower interest rate as their duration risk is lower (you get your money back earlier than with a longer term bond and can reinvest if interest rates are higher). At times however, shorter term rates are close to long term rates and the lender/investor should think about their duration risk (this is the current situation).



Gold

It is only in the past few months that gold's inflation-adjusted value turned positive at all. Prior to that, 1980's generation of gold bugs had been under water in real terms for close to half a century. Much more to the point, the price level of the S&P 500 has gone up 13 times more than has gold's price only because we've ignored dividends, which stocks produce in ever-increasing amounts while gold produces...nothing. Counting reinvested dividends, the S&P has compounded at 12% annually since January 1980, yielding the following comparison of the current values of \$800 invested in both assets: Gold: \$3,800 S&P 500: \$141,303 Mainstream U.S. equities continue to be the most efficient long-term inflation killer that has ever existed. -Nick Murray

Miscellaneous

Fraud Warning (from Oblivious Investor blog)

What Does a Thief Need to Access Your Financial Accounts? It's Likely Less Than You Think

A long-time *Oblivious Investor* reader recently wrote in to share that he and his spouse had fallen victim to a fraud that resulted in a theft from one of their IRAs at Fidelity (which, as discussed below, was not reimbursed). The total loss was "only" about \$4,000. But it absolutely could have been much worse.

Here's how it played out.

John and Rachel (not their real names) had just returned from a trip abroad. Rachel received the following text:



Fidelity ®: Did You Attempt A Transaction Of \$374.52 At MODERN FEMME FASHIONS 12/02/2025 (EDT). Reply (YES)if Recognized Reply (NO) if Unauthorized, A Call Will Be Generated To You Momentarily

No

Fidelity ®: Thank you for confirming. Please hold for the next available agent to assist you.

If you can't see the image, the conversation reads as follows:

Incoming text:

Fidelity ®: Did You Attempt A Transaction of \$374.52 At MODERN FEMME FASHIONS 12/02/2025 (EDT).

Reply (YES) if Recognized.

Reply (NO) if Unauthorized, A Call Will Be Generated To You Momentarily

Outbound text:

No

Incoming text:

Fidelity ®: Thank you for confirming. Please hold for the next available agent to assist you.

After that text exchange, Rachel received a phone call as indicated. At the outset of that call, the agent said that, in order to confirm her identity, Fidelity was going to send her a 6-digit code and asked her to please read it back to them. Rachel received the code and read it back to the agent on the phone.

And that was it. As of that moment, the fraudster was able to access her Fidelity account.

The thief promptly initiated a few money transfers out of the account. Fortunately, John promptly noticed what was going on and contacted Fidelity. Fidelity was able to recover one of



the transfers, but the other two (totaling ~\$4,000) were not recovered. And because the theft involved the victim unintentionally sharing login information with the thief, Fidelity did not reimburse John and Rachel for the theft.

Why was it only \$4,000 that was stolen, when there was much more in the account? (Even the cash balance at the time far exceeded \$4,000.) I'm not entirely sure. I think the thief must have intentionally chosen a low amount to hopefully not trigger any alerts on Fidelity's end. But the situation clearly could have been much worse.

How the Fraud Worked

When we log into an account (if not using a passkey, which is a topic for another day), we provide username, password, and the multi-factor authentication (MFA) code. So we might think of all three as being necessary.

But the thief didn't need Rachel's username or password at all. All they needed was the six-digit MFA code.

If that sounds surprising to you, take a look at the password-reset forms for any number of financial institutions. ([Here's Vanguard's](#) for instance. [Here's Fidelity's.](#)) Take a careful look at the information they ask for. For many financial institutions, the form requires:

- Name,
- Date of birth,
- Social Security number (or last 4 digits of Social Security number), and
- Zip-code.

After you enter that info, they send you a 6-digit code. And after entering that code, they let you reset your username and/or password, or perhaps they display your username on the screen in plain text and allow you to pick a new password.

And, unfortunately, for most of us, *all of that information is available for purchase* on the dark corners of the internet, due to large-scale security breaches that have already happened. In the [2017 Equifax breach](#) alone, approximately 147 million Americans had their name, DoB, SSN, home address, and phone number stolen. That's roughly 43% of the U.S. population in just one data breach. And there have been tons of other breaches.



In other words, for most of us, a thief has everything they need to get into our accounts, other than a 6-digit multi-factor authentication code.

We deal with MFA codes so often that they feel commonplace, mundane, disposable. But they're the keys to the kingdom. It's not an exaggeration to say that MFA codes should be guarded *more closely* than your Social Security number.

“We’re Contacting You About Fraud” Is Itself a Red Flag for Fraud

“We’re contacting you about a suspected fraud” is itself a great way to defraud somebody, for two reasons.

Firstly, it gives the fraudster a plausible reason for the initial contact to the targeted person.

And secondly, it puts the targeted person in a mindset of wanting to *take prompt action*, in order to stop the supposed fraud — thus making it easier for the fraudster to get the target to follow instructions. It might even be effective enough to generate a panic/fear response in the target, thereby inhibiting clear thought.

What To Do When You’re Contacted

When a financial institution with whom you have a relationship reaches out to you (whether about a suspected fraud or about anything else):

- If it's a phone call, take down whatever information they give you. (Or frankly just don't answer the phone if it's from a number you don't know. Just listen to the voicemail, if they leave one.)
- Regardless of method of contact, do not give them any information. No information whatsoever. Not your date of birth. Not your Social Security number. And absolutely not a multi-factor authentication code. Give them nothing. Truly, nothing. If it's a text, do not reply. If it's an email, do not reply to the email.
- If it's an email, do not click on any links in the email.
- Then reach out to a trusted phone number that you already have for that financial institution. If it's your bank, call the number on the back of your credit/debit card. Or directly type in [schwab.com](https://www.schwab.com) (or whatever is the applicable website), and find the applicable phone number there. And once you know you're actually in contact with the right organization, ask them for details on the situation.



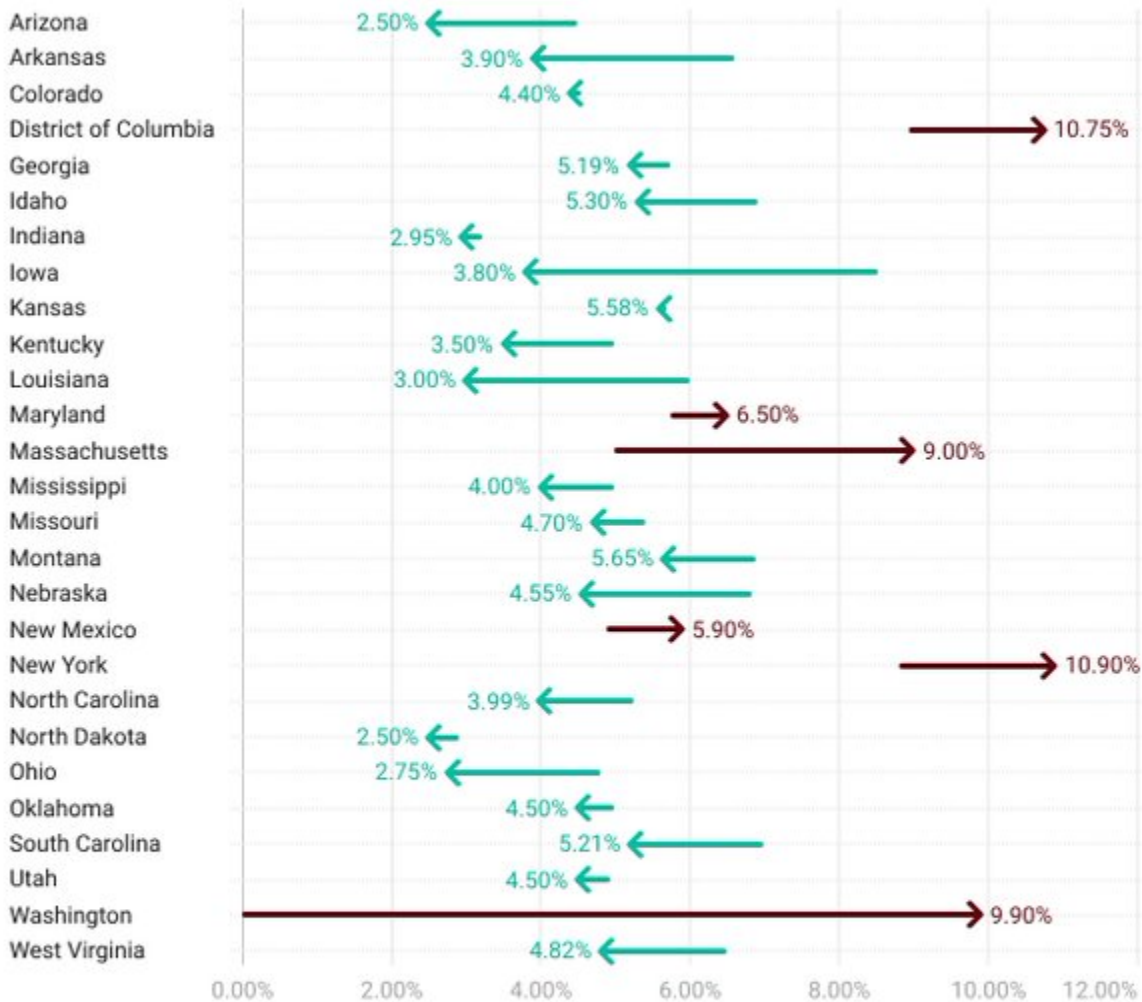
To summarize:

- Don't respond to any inbound messages that appear to be from financial institutions. Don't give them any information.
- Separately reach out to a phone number that you know is genuine, to ask about what's going on.
- Treat multi-factor authentication codes with the utmost security and caution. If you accidentally give one to a thief, that's quite possibly all they need to get into your account.



State Income Tax Rates are Diverging

Change in Top PIT Rate by State, 2020-2026, Including Pending SC and WA Legislation



Note: Only includes top ordinary rate on individual income. Includes legislation that has passed both chambers in South Carolina and Washington, pending governors' signatures. Does not include uncapped non-UI payroll taxes in California, Massachusetts, or Washington, or changes to rates on capital gains income. Several states reduced lower rates but not the top rate and are not included here, and two states eliminated taxes on interest and dividend income and are likewise omitted.

Created with Datawrapper

Random Notes

In these markets, diversification matters. Beer, whisky, vodka, and tequila have helped me forget about my portfolio.-D Boneparth

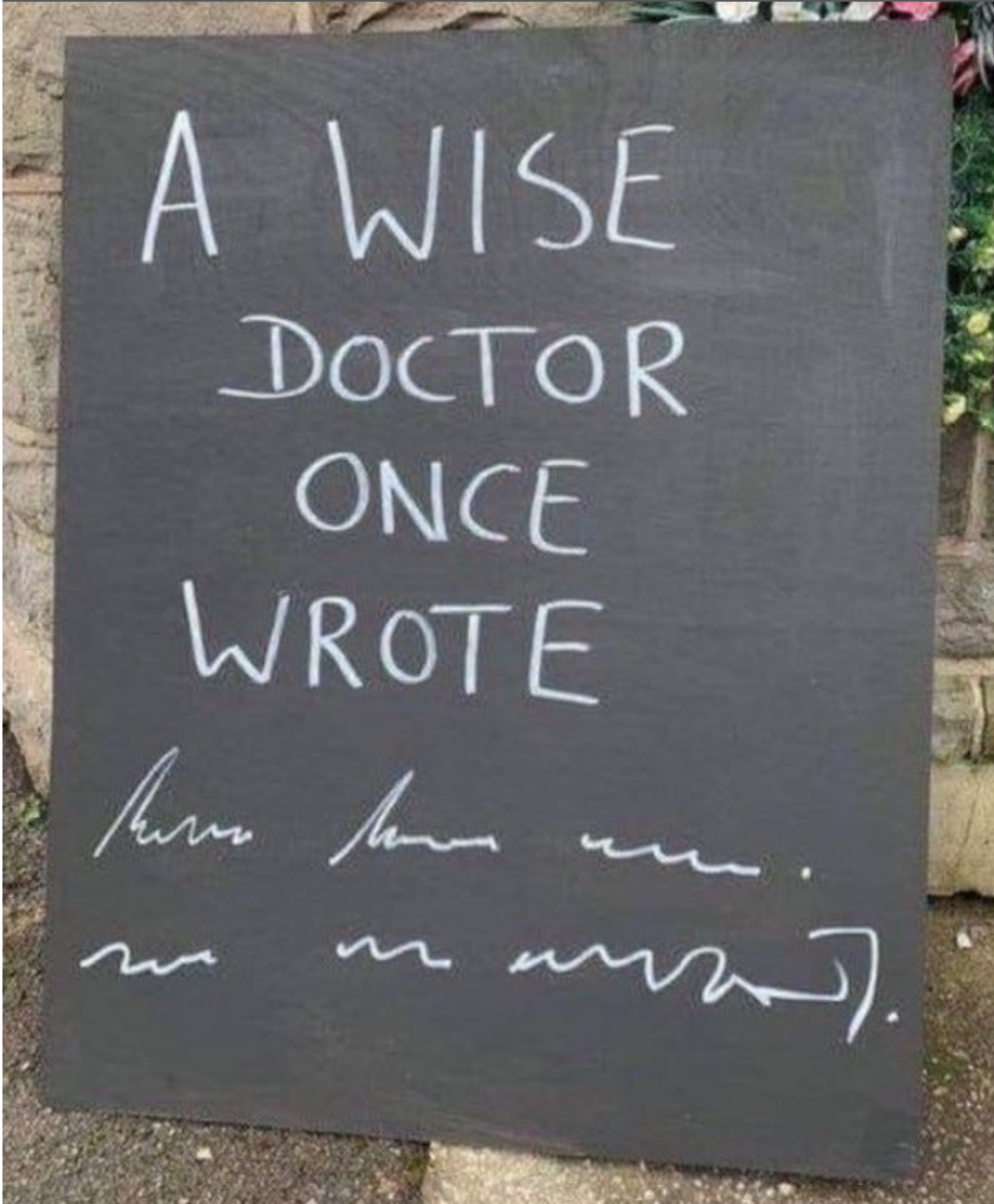


*One day you'll find someone
that's obsessed with you.*

*It's probably going to be a dog
but it is what it is.*

iPhone cleaner app

<https://www.cleverfiles.com/clever-cleaner/>



The Wealth Care LLC Team May 1, 2026

WWW.WEALTHCARELLC.COM | F. 815.301.3777