On Course Financial Planning
Facing the Future with Optimism and Courage
July 2026
Vectors
geo@oncoursefp.com
425-861-9997

Active Managers' Report Card

Another school year has ended, and students' report cards are in the mail. S&P's Indexes Versus Active (SPIVA) Scorecard is a semiannual report card that compares the performance of actively managed mutual funds to their S&P benchmark index. The latest SPIVA Scorecard, covering the 20 years ending December 2025, notes that in 2025, 79% of large-cap active funds underperformed the S&P 500 Index - the fourth worst year for large-cap fund managers in the 25 year history of the SPIVA Scorecard. Additionally, 80% of actively managed domestic stock funds underperformed the S&P 1500 Total Market Index last year.

Fund Asset Class	1 YR	3 YRS	5 YRS	10 YRS	15 YRS	%
Large-Cap Growth	F	F	F	F	F	0%
Large-Cap Value	P	F	F	F	F	13%
Mid-Cap Growth	F	F	F	F	F	13%
Mid-Cap Value	F	F	F	F	F	10%
Small-Cap Growth	P	P	F	F	F	10%
Small-Cap Value	P	P	P	F	F	7%
Domestic REITs	F	F	F	F	F	9%
Int'l Large Stocks	F	F	F	F	F	7%
Int'l Small Stocks	F	F	F	F	F	15%
Emerging Market Stocks	F	F	F	F	F	6%

This is the year-end 2025 SPIVA report card for active fund managers. The far-left column lists ten popular stock asset classes. The next five columns give a pass or fail grade to active managers in each asset class for the past 1, 3, 5, 10 and 15 years. If more than 50% of actively managed funds in an asset class outperformed their benchmark S&P index, they get a passing grade of P for that period. If fewer than 50% outperformed, they get a failing grade of F. The last column shows the percentage of funds in each asset class that survived and outperformed their benchmark index over the past 20 years. Note: this does not mean that these funds outperformed in each of the past 20 years.

The data is unequivocal, active management's persistent failure to outperform benchmark indexes is not a temporary aberration, but a decades long ongoing reality.

Competition among index fund providers has driven fund management fees to unprecedented lows. Today, you can own the Vanguard Total Stock Market Index ETF (VTI) with no sales commission and an annual management fee of just $3 per $10,000 invested. The number of index investors has increased in the past twenty years, shrinking the pool of amateur investors that active managers can exploit. Additionally, a fund manager with too many F grades on his report card will soon be looking for a new line of work. According to the latest SPIVA Scorecard, of the 2,456 actively managed domestic stock funds available to investors on Jan. 1, 2016, 870 (35%) were closed or merged into more successful funds by year end 2025. The removal of less talented fund managers leaves the surviving fund managers in an increasingly competitive environment, making it more difficult to outsmart the competition and earn that rare P grade.

Active fund management is a high-pressure occupation, and those who undertake it seek to generate good long-term returns for their shareholders. But they also must produce good short-term performance to keep current investors happy and attract new ones. Unfortunately, trying to generate short-term performance from long-term assets involves active trading that is likely to harm their shareholders' long-term interests. The wise investor will forget about trying to beat the market and put the odds of investment success in their favor by matching the returns that the capital markets freely offer by using low-cost, tax efficient index funds.

The Phantom Hacker Scam

The FBI has released a public service announcement concerning one of the fastest growing financial scams today, known as the "Phantom Hacker" scam. It has cost Americans, especially senior citizens, hundreds of millions of dollars. Victims have suffered the loss of entire banking, savings, retirement, or investment accounts under the guise of protecting their assets. Here's how it typically works –

- You receive a text message, email, or pop-up from a scammer posing as a tech or customer support representative from a legitimate company, the Federal Reserve or other government agency warning you that your computer, bank account, or investment account has been compromised. A phone number is provided for "technical support."
- When you call, a friendly representative directs you to download a software program which allows remote access to your computer. The scammer pretends to run a virus scan on your computer and falsely claims that your computer has been or is at risk of being hacked and that your money is no longer safe. Using remote access, the scammer requests you to open your financial accounts to determine whether there have been any unauthorized charges. This is how the scammer determines which account is the most lucrative target. The scammer then tells you that you will receive a call with further instructions from the fraud department of the financial institution that holds that account.
- Soon thereafter, you receive a call from a "representative" of the financial institution where your account is located. They inform you that a foreign hacker has accessed your financial accounts and that you must transfer the money via wire transfer, cash, or cryptocurrency to a "safe" third party account immediately. You may be instructed to send multiple transactions over a span of days or months. Finally, the scammer tells you not to inform anyone at the financial institution of the reason for the transfer because they may be in league with the hacker. Of course, there is no hacker. The only criminals involved are the people on the phone. Once you have transferred your funds to the "safe" account," the money is moved through a complex network of accounts, making it hard to trace and almost impossible to get back.

There are few public cases that identify individual Phantom Hacker victims by name because law enforcement agencies generally protect victims' privacy. However, several documented cases provide specific details about what happened –

- An 82-year-old woman in Massachusetts received a pop-up message on her computer claiming it had been compromised. She called the number provided and spoke with someone posing as a Microsoft technician. She was then transferred to individuals claiming to represent her bank and the Federal Reserve. The callers convinced her that hackers had infiltrated her accounts and instructed her to withdraw nearly $400,000 and turn the money over to a courier who claimed he was working for the federal government. She complied, believing she was helping protect her assets. Federal investigators later determined the courier was part of a international criminal organization.
- In another case, the victim first received a call supposedly from Amazon regarding fraudulent purchases. The call escalated through several "officials," including fake representatives of the Federal Trade Commission and federal law enforcement. The scammers persuaded the victim to transfer more than $600,000 into accounts they controlled.
- Law enforcement agencies in Arizona have reported multiple cases in which retirees were instructed to withdraw savings from brokerage and bank accounts, purchase hundreds of thousands of dollars in gold bars, deliver the gold to someone posing as a federal courier. Victims were told the gold would be stored in a secure federal vault until the "hackers" were arrested. Instead, the gold was stolen.
- A California retiree was convinced that foreign hackers had gained access to his bank accounts. The scammers spoofed legitimate government telephone numbers, provided fake badge numbers, warned the victim not to tell bank employees because the investigation was "classified." The victim liquidated retirement investments and wired the proceeds into accounts controlled by the criminals.
- A retired Florida couple responded to what appeared to be a Microsoft security warning. Over several weeks they spoke to people who posed as employees of Microsoft Security, their bank's fraud department, the Federal Reserve, and the FBI. Each caller reinforced the previous caller's story, convincing the couple they were participating in a government operation to protect their savings. They ultimately wired several hundred thousand dollars overseas before realizing they had been defrauded.

When hearing about victims of investment scams, it's easy to think of them as being greedy and/or foolish. But this is not usually the case. Scammers are con artists who win trust by exploiting their victims' emotions, vulnerability, fears, and desperation when attempting to safeguard their wealth. The con artist often counterfeits trustworthiness and expertise by claiming to represent a well-known company, investment firm, or government agency. They are experts at posing as a benefactor, someone who presents a solution to your financial distress. False credentials add to the deception. New retirees are frequent targets because scammers know they often have substantial retirement savings and may be less familiar with today's sophisticated cyber frauds. To protect yourself, remember these simple rules:

- Do not click on unsolicited popups, links sent via text messages, or e-mail links or attachments and do not call the telephone number provided in them.
- Your bank, brokerage firm, or government agency will never ask you to transfer money to a supposedly "safe" account, purchase gold, or buy cryptocurrency to protect it from hackers.
- Never download software at the request of an unknown individual or allow an unsolicited caller to remotely access your computer.

- Be suspicious of any request that requires immediate action or if you are told not to discuss the matter with family members or financial institution employees.
- If you receive an alarming message, contact your financial institution using the phone number on your statement or the institution's official website—not the number provided in the message.
- Today's scams are increasingly reliant on impersonation as a shortcut to gaining your trust. No matter how likable or trustworthy someone seems, check their credentials. Do online checks on them and their firm.
- Before moving significant assets, call a trusted family member or your financial advisor for a second opinion.

Scammers rely on fear, urgency, and confusion more than sophisticated technology. The best defense is to slow down. If someone pressures you to act immediately to "save" your money, that's your signal to stop, verify the story independently, and seek advice from someone you trust.

The IPO Illusion

Probably the biggest financial story last month was the hype around the SpaceX IPO. An Initial Public Offering (IPO) is the process by which a private company sells shares to the public for the first time, becoming listed on a stock exchange. Prior to this, stock ownership is typically limited to founders, employees, and private investors like venture capital firms. Once a company "goes public", anyone with a brokerage account can buy and sell its stock. Investors get the chance to own a piece of a company at an early stage of its public life, with the hope of significant stock price appreciation. High-profile IPOs come with excitement and press coverage, which can drive strong early demand. Hype around IPOs is nothing new. All it takes is a bull market, a company with obvious upside potential and a FOMO public eager to buy.

A limited supply of shares, an attractive offering price, and high demand from eager buyers create the price pop that is common on the first day of trading. But subsequent performance usually leaves much to be desired. An analysis by University of Florida finance professor Jay Ritter covering 9,253 IPOs from 1980 through 2024 revealed that the average IPO produced a first-day return of 18.9%. But few retail investors can buy shares at the initial offer price. Ritter's research revealed that investors who bought shares at the first day's closing price, usually after the first day price pop didn't do so well. The average IPO netted just a 5.5% annualized return from the first day's closing price over the next 3 years and just 3.6% over the next 5 years – both well below the stock market's average return. A significant factor in the poor performance is lock-up expirations. Company insiders are usually restricted from selling shares for a set period (often 90–180 days) after the IPO. When that lock-up expires, a wave of selling can put downward pressure on the stock price. Also, IPO pricing is set by the underwriter's expectation of demand for the stock, not always by economic fundamentals, which can mean paying a premium relative to the company's actual earnings or growth prospects.

Time Period	VTI	IPO
Total Return Since Inception of IPO (Oct 2013)	+403%	+209%
5-Year Total Return	+78%	-9%
3-Year Total Return	+75%	+84%
1-Year Total Return	+23%	+32%
Growth of $10,000 Since IPO Inception (Oct. 2013)	$50,148	$30,829

Note: Returns are with dividends reinvested as of 6/30/2026. Source: Morningstar

This chart shows the performance of the Vanguard Total Stock Market Index ETF (VTI) and The Renaissance IPO ETF (IPO), a fund that holds shares of newly issued IPOs. Since the inception of IPO in October 2013, VTI delivered roughly twice the total return. VTI's broad diversification (more than 3,400 companies) proved more rewarding than IPO's concentrated portfolio of 52 stocks (as of 6/30/2026 according to Morningstar). The volatility of the IPO ETF may be a bit too much for most people's risk tolerance. Although it gained 52% in 2023, that followed a decline of 57% in 2022.

Ritter's research is the gold standard in IPO performance analysis and the verdict for long term investors is sobering. The IPO market rewards issuing firms, the investment banks that bring the shares to the public and short-term institutional share flippers who get shares at the offering price. They exploit and profit from over-optimistic FOMO investors who fail to distinguish between hype and reality. We are likely to see more IPO frenzy when AI giants Anthropic and OpenAI have their IPOs in the not too distant future. Caveat emptor.