Remaining Process Driven

Steve Goodman

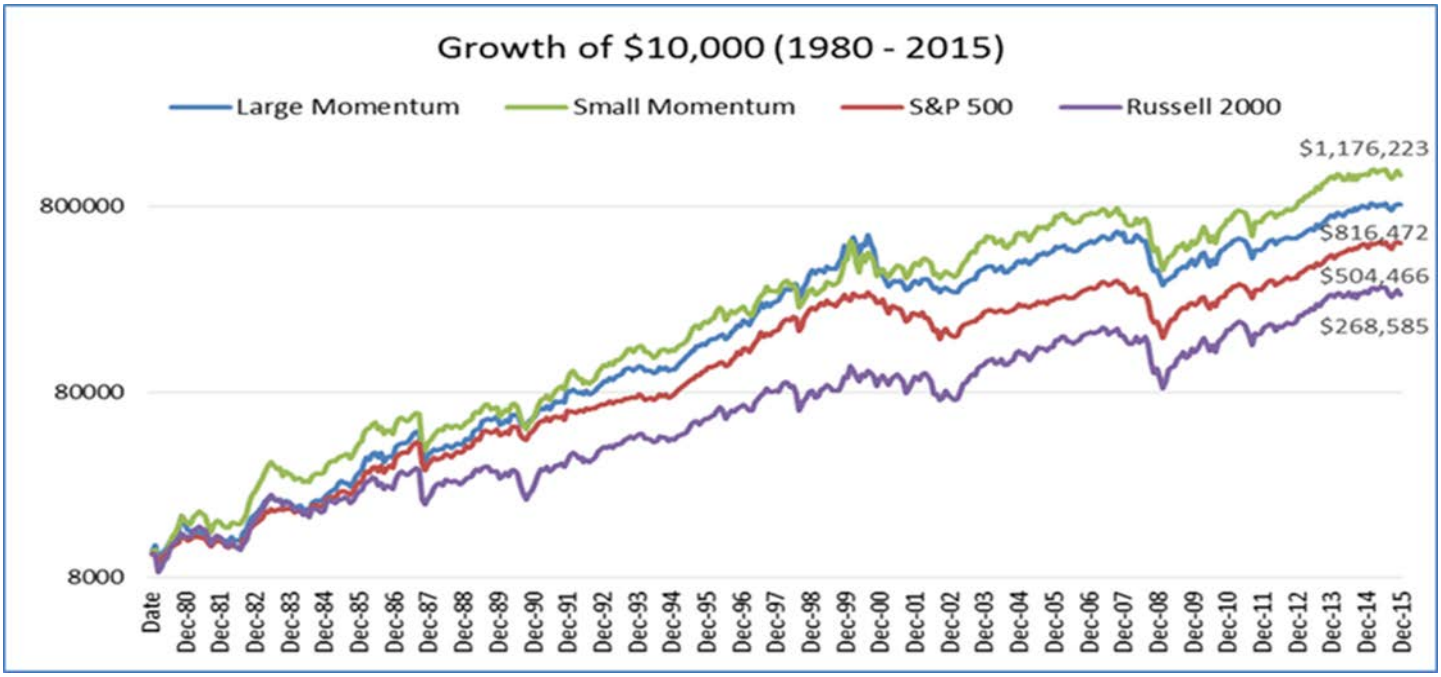
As the volatile first quarter ends, we would like to focus on one of our investment principles:

Investing decisions are based on a process

Some of our strategies are driven by a momentum process. Momentum is a powerful and persistent market strategy; the evidence supporting this assertion is overwhelming. The idea that buying past winners and selling past losers (from 1-12 months) can lead to outperformance, though, is still bewildering to many. It's not intuitive to believe that past performance in security prices can actually be indicative of future results.

But indeed it is. That is not to say that momentum investing is "easy" or that it "always works". The same can be said for any strategy, it works until it doesn't work for a while. Far from it. It must be executed in a systematic fashion, with discipline and without emotion. And like value and other strategies, momentum returns are inherently cyclical. That means there are periods of above-market performance and periods of underperformance. Therein lies the problem for many investors when it comes to strategies. They tend to chase performance, reducing or eliminating the benefits of the strategy itself. The notion is particularly perplexing when it comes to momentum investing because while chasing security prices in a systematic fashion works over time, chasing the return stream from that chasing does not.

Chart courtesy of Pension Partners



An example will make this point clearer. An investment of $10,000 in 1980 would have grown to $1,176,223 by 2015 in Small Cap Momentum, far outpacing the $268,585 in the Russell 2000 Index (14.2% annualized vs. 9.6%). Meanwhile, a similar investment in Large Cap Momentum would have grown to $816,472 versus $504,466 in the S&P 500 (13.0% annualized vs. 11.0%).

While momentum widely outperformed from 1980-2015, there were many periods in which momentum underperformed. In looking at rolling 1 and 3-year returns, Large Cap Momentum outperformed the S&P 500 62% and 63% of the time, respectively. This means that 37%-38% of the time it was deemed to be "not working." Would you stick with it through such hard times, including the recent 30% underperformance from March 2009 through February 2012? Maybe, but most would not.

The lesson here for investors: to reap the full benefits of a strategy, you cannot chase the performance of the strategy itself. In order to reap the benefits, you must be willing to accept the fact that there will inevitably be times when the strategy is "not working." And if we have learned nothing else from market history, sticking with a long-term investment plan is paramount to investment success.

A special thank you to Pension Partners for their permission to use their research for this article.

How to Prevent Identity Theft: TAKE CHARGE

John Dankovich

Picture this: You're sitting at your desk or kitchen table, pouring over your budget and bills, when you open your credit card bill to discover a $1,200 charge you're certain you never authorized. Someone's taken your name and used it for their own purposes. You've been the victim of an ever-growing crime and you didn't know it until now.

According to a 2015 Identity Fraud Study, almost 13 million Americans had their identities stolen in 2014; a new identity fraud victim every 2 seconds! Michigan ranked 6th in identity fraud by State in 2014! Each of us must elevate our awareness and learn how to provide ourselves with additional levels of protection.

Three types of identity theft

Medical – Use of your personal information to find your insurance information and use it to have procedures done under your name and insurance. Your medical record will reflect procedures and conditions that are not yours. The next time at your Doctor's you could get medications or treatment you don't need. You will also be responsible for the bills the insurance did not cover and it may increase your rate.

Criminal – ID thieves commit a crime using your name. You can be arrested and charged with a crime you didn't commit.

Financial – Once ID thieves have your information they can gain access to your credit cards, bank accounts and brokerage accounts. They will open new credit card accounts and take money from your accounts.

How They Get Your Information

Hacking into your PC: Hackers can put a virus on your computer called Key Strokes, more widely known as a Trojan Horse. This allows them to see what you are typing, giving them access to your accounts and passwords without needing your address or Social Security Number (SSN).

Skimmers: Small electronic devices known as Skimmers are used to copy information from a credit card or ATM card. Thieves will hide one over an ATM machine or gas pump and when you put your card in to access your account or pay for gas, it copies and stores all your information giving them access to your accounts.

Phishing: This is where you receive an email that looks like it came from your bank or any other company that you may do business with asking for your personal information (e.g. amazon2@yahoo.com). When you fill it out it connects to a hacker who gets your information and who may install a spyware program on your P.C. Don't be fooled by a business logo in an email. Always go to a business website independently of any link in an email you receive.

Dumpster Diving: The easiest way to go through your trash to get your personal information – your trash is their treasure. Get a document shredder and use it

Some Ways to Protect Yourself

- Monitor your credit card report. Everyone has a right to a free credit report annually, which can be obtained at www.creditreport.com or by calling 1-877-322-8228.
- Be careful to whom you give your personal information. The more places that have your information the easier it is to get. Opt out of information sharing. Get off the pre-approved credit lists @ www.optoutprescreen.com or 1-888-567-8688. Get off junk mail lists at www.dmaconsumers.org (go to Consumers Assistance page). Enroll in the do-not-call registry at www.donotcall.gov.
- Be careful shopping online
    1. Only provide personal and credit card information when the merchant is using SSL (Secure Socket Layer). You can tell when you are on a site using SSL because the website will start with https:// (versus http://) or will have the tiny SSL lock symbol located at the bottom of the web browser. SSL means your information is encrypted when it is sent over the internet.
    2. Know what information the merchant is collecting about you, how it will be used, and if they share it with or sell it to others. You can do this by checking the website to make sure there is a privacy policy posted and that you are comfortable with the way your personal information is treated under that policy. Be cautious if you are asked to supply personal information not needed to make a purchase such as Social Security Numbers or personal bank account information.
    3. It is a good practice to pay with credit cards because under federal law (and your credit card agreement) your liability for an unauthorized charge is limited to $50. If you use an ATM card and the information is stolen and money is withdrawn, there is no such protection.
    4. Keep your passwords safe and do not share them with people. Use more complex passwords by combining letters (upper and lowercase), numbers and symbols. Microsoft is currently recommending that 12 is the optimal number of characters for a password. Do not use your birth date. Change them regularly (some experts suggest every 6 months).
- Remove information from old computers by taking out the hard drive and destroying it. There are companies, such as Data Killers (www.datakillers.com), that securely and completely purge or destroy hard drives, back-ups, CD memory devices, etc.

- Install anti-spyware, anti-virus and firewall programs on your computer and keep them current. Norton and McAfee are well known anti-virus and firewall programs and you can download McAfee anti-spyware programs at www.mcafee.com. Beware of free virus and anti-spyware program offered on the internet. They are themselves often viruses and spyware…and sometimes aren't even free.
- Use precautions when using WIFI (wireless internet found at places like hotels and Starbucks). When you are on a public WIFI network do not access your bank accounts and any other sensitive information sites (brokerage accounts). This would also apply to sites like Facebook if you sometimes send sensitive information that you don't want exposed.
- Freeze your credit, making it harder for people to access your credit report. One company to check into for this service is LifeLock (www. Lifelock.com, or, 1-800-543-3562).

We are sure there are other things you can do, but there will always be risk of theft. The best thing is to stay vigilant and make sure to review all your transactions and update your credit report once a year.

You should be receiving statements at least quarterly from Fidelity or other custodians of your accounts. If you are not receiving these statements, please contact us and your custodian immediately.