2017 1st Quarter

James A. Braziel, CFP®
Registered Principal, NPB

Braziel & Associates, LLC

PERFORMANCE WEIGHTED ASSET ALLOCATION REPORT

1074 East Avenue, Suite L | Chico, California 95926
(530) 895-3344 | (800) 675-3344 | Fax (530) 895-3141

James H. Braziel, CFP®
Registered Principal, NPB

ADVISORS' THOUGHTS

The first two months of 2017, for stock market investors, were a continuation of the positive momentum that was in place since the election. However, since around March 1st the market has paused with daily ups and downs but no real movement in any one direction. For the quarter as a whole, stock market investors have done well.

The S&P 500 gained 5.53% in the first quarter, as noted in the Benchmark Returns Table reflecting an optimism that the US economy and earnings would continue to grow. Earnings are projected to see a big rebound in the first quarter when the final numbers are counted. According to Factset Earnings Insight report dated April 13, 2017, "...the blended earnings growth rate for the S&P 500 is 9.2%. If 9.2% is the actual growth rate for the quarter, it will mark the highest (year-over-year) earnings growth for the index since Q4 2011...". Strong earnings are a huge driver for the stock market over the long term and current earnings are doing well.

Stock market gains were not limited to the US in the first quarter. For the first three months of 2017 the MSCI EAFE increased 6.16%. This index of developed markets outside the US reflects some improvement in the global economy. In fact, some of the improvement in US earnings is actually a reflection of improvements overseas. According to Factset, S&P 500 companies that generate more than 50% of their earnings overseas have an earnings growth rate of 15.7% compared to companies that generate most of their earnings in the US with a 6.0% growth rate.

(Continued on Page 4)

BENCHMARK RETURNS THROUGH 03/31/2017

	3 Mo.	6 Mo.	12 Mo.
DJIA	4.56%	12.86%	16.84%
S&P 500	5.53%	8.97%	14.71%
Russell 2000	2.12%	10.73%	24.81%
MSCI EAFE	6.16%	5.37%	8.53%
MSCI Emerging Markets	11.20%	6.08%	14.53%
Barclays US Aggregate Bond	0.86%	-2.30%	0.47%
ML High Yield Bond	2.71%	4.61%	16.75%

Source: Wall Street Journal and Morningstar Principia
Does not include reinvestment of dividends

DJIA: A price weighted average of 30 stocks.

S & P 500: A market value weighted index of 500 stocks.

Russell 2000: A market value weighted index of 2000 stocks.

MSCI EAFE: A stock market index designed to measure the equity market performance of developed markets outside US and Canada.

MSCI Emerging Markets: A stock market which captures large and mid cap representation across 21 Emerging Market countries..

Barclays US Aggregate Bond Index: An index that measures the investment grade, US dollar-dominated, fixed-rate taxable bond market.

ML High Yield Bond: An index of non-investment grade corporate bonds.

PROTECTING YOURSELF ONLINE

Cybercrime has grown to be a major global problem and taking precaution upfront may save a lot of aggravation later. Whether browsing on the internet or reading your email, there are hidden risks to being online.

ONLINE RISKS

One broad type of risk is called **malware**. Malware is a term that describes any malicious software used to disrupt a device (computer, phone or tablet), gain access to any device, gather sensitive information, or even display unwanted advertising. Malware can be installed on your device when we unsuspectingly click on a website pop-up or email link that is implanted with malware.

One particularly brutal example is called **ransomware**, where the user's computer becomes infected and the user is prevented from accessing it. In order to reclaim their machine and retrieve the data, a ransom (money) must be paid to the perpetrators.

Another common use of malware is to install a **keylogger** on the device. This allows the hacker to track all keystrokes on your machine making it easy to learn your personal financial information. Anything you type becomes vulnerable. Passwords, account numbers, credit card numbers etc. may all be compromised.

Because the potential damage that may be caused from being hacked is so great, one should remain vigilant in their online behavior to minimize the possibility of becoming a victim. Here are some ways to protect yourself.

PASSWORDS ARE YOUR FIRST LINE OF DEFENSE

Stop hackers at the door with your password. Passwords are an important first step to protecting your personal information online. Here are some tips to create a strong defense against hackers from learning your password.

Don't reuse the same password. Using a different password for each account will minimize the damage if that one password is stolen. While it is definitely more inconvenient to have different passwords, when it comes to your personal financial data it is probably worth the inconvenience.

Don't just use words. Hackers use dictionaries of various languages, names and linguistic patterns to identify password roots. If it's in a dictionary then it is probably in a password breaking software program.

Longer passwords are better. There are various opinions about the number of characters that a strong password should contain, but it appears that eight is probably the minimum. Note that the longer the better because the method used to steal your password may be a high speed computer that randomly generate passwords to try and guess the correct one. The more characters in the password the longer it will take.

Include capital letters, numbers and symbols. An eight character password that includes these is more difficult to break than just letters. Consider using symbols to increase the number of keystrokes needed to hack your password.

Never use personal information in your password. Your name, address, and date of birth are pieces of information that numerous people and businesses know about you. If one of them is hacked your password is now vulnerable. Furthermore, information that one may be able to find out about you online, such as through social media, should not be part of your passwords. Posting pictures of your dog Rover and having your password be some version of "Rover" is not a good idea.

Consider password manager programs. There are a number of password manager web services or programs that create very strong passwords for each of your sites. It accomplishes this by randomly generating the passwords and having that information encrypted. By utilizing a password manager, it allows you to not have to remember a unique password for each one. However, you will still need to know one password to access the password manager and this better be a strong password because if it is ever stolen hackers will have access to all of your accounts. Furthermore, if you forget your password you will be locked out of all your accounts.

Periodically update your passwords. Never changing the password allows a hacker indefinite access to that account and your information. It is a good habit to periodically change passwords.

MORE WAYS TO PROTECT YOURSELF

Keep your operating system and software updated. All programs and software are subject to vulnerabilities that hackers are continually looking to exploit. These security issues are continually being identified by the companies that wrote them. Whether you're talking about Microsoft Windows or Office, Google Chrome or Adobe's PDF Reader, they all need to be updated. Regularly updating means as vulnerabilities are identified and fixed your system stays as protected as possible.

Use anti-virus and anti-malware software. These programs can run in the background and provide real-time protection against known viruses or malware. They may prevent or identify any security issues with incoming email or websites you click on. Pay close attention to any warnings or issues identified and promptly remove any quarantined item.

Never click on a link in an email until you validate the source. This is a common technique of cybercriminals to put links in emails to try and get you to click on them. One example may say your order has been shipped (although you never ordered it) and they need to verify something to track your package, and they ask you to click the link. Another example will appear to be from your bank and they want you to confirm or verify some transaction or account information. They may even say your account has been hacked. It will appear to be for something legitimate, however when you closely examine the link it is directing you to a bogus website. You can see where the link is redirecting you by hovering your cursor (without clicking on it) over the link. It may only be one letter different than the legitimate web address, so be careful! If there is ever any doubt to the authenticity of a website go directly to the legitimate website or contact the company with a known correct phone number, such as from your account statement.

Be wary of emails from people you know that appear out of character. Just because you know the sender the email still may not be safe. They may have had their account hacked. When in doubt be old fashioned and give them a phone call.

Only enter personal information on secure websites. When conducting business online make sure the web address begins with **https://**. Hyper Text Transport Protocol Secure provides encrypted transmission to and from the Web server. If it merely begins with **http://** the transmission is not encrypted and your personal information can be viewed by others.

Use multi-factor authentication whenever possible. It is much harder to steal your information if two unique forms of identification are required. This is the same concept when you use your ATM. That transaction requires your debit card and your pin number. An online example is when logging into your bank account from a different computer than you normally use it will send a text message to your phone to enter in to the website. This is in addition to you entering the password to log in.

Carefully close anything that pops up on your screen. A pop up ad or warning may contain something harmful (virus, malware etc.) that requires just one wrong move to infect your machine. Therefore, never click on anything in the pop up ad or warning including the ads or warnings close button. Instead, close it by clicking on the red X in the upper right corner. Note that warnings are an excellent way to create a sense of urgency to prompt an immediate response by you.

Avoid leaving an online trail for hackers. Log out after using any website that requires you to log in first to ensure your session is closed. This is especially important for your financial accounts or where you are making an online purchase. It is also a good idea to clear your data cookies and browser cache. These leave pieces of information that hackers can find to exploit.

(Continued on Page 4)

ADVISORS' THOUGHTS (continued from Page 1)

Investment grade bond returns were modest in the first quarter with the Barclays Aggregate Bond index gaining 0.86%. Interest rates remain near historical lows, but some change appears to be on the horizon.

Short-term rates that are determined by the Federal Reserve are beginning to rise. For the second time in three months the Fed raised the federal funds rate a ¼ percent to a range of ¾ to 1%. This is beginning to impact short-term savings rates and we are starting to see a rise in money market fund yields above zero. Rising rates are a positive for savers and a reflection of a growing confidence in the economy by the Federal Reserve.

Investment markets have been on hold recently waiting for further clarity on corporate profitability, the economy and political events. With no immediate sign of recession, a prolonged downturn in stock prices appears unlikely. This is a time for investors to remain patient with the slow improvements that are occurring in the economy. Growing profits should lead to growing stock prices over time.

PROTECTING YOURSELF ONLINE (continued from Page 3)

PUBLIC Wi-Fi: CONVENIENT FOR YOU AND HACKERS

The availability of internet access through free public Wi-Fi hotspots has grown rapidly in recent years. Restaurants, hotels, airports and coffee shops nearly all offer this convenient service. However it is precisely the simplicity and ease of free public Wi-Fi that makes it desirable for hackers.

Hackers can position themselves between you and the connection so instead of talking directly to the hotspot you are sending your information to the hacker, who then relays it on. This provides the hacker with complete access to everything you send out. Important emails, credit card numbers and passwords are all visible to the hacker. Once in possession of that information he can access your system at any time.

There are steps you can take to limit your risk of using free public Wi-Fi.

Avoid or limit what you do. If you are merely surfing the internet, then you are probably not at much risk. But if you check your email, go on Facebook or log into anything, now you have opened the door of opportunity for a hacker.

Use a VPN. A virtual private network (VPN) for connecting to your office should be used. The data transferred here will be encrypted. Even if the hacker was able to intercept the data it would be unreadable. They could possibly decrypt it, but why not move on to an easy target sending unencrypted data.

Enable "Always Use HTTPS" on websites you use. This will add a layer of encryption if you do not have a VPN.

Keep Wi-Fi off when not needed. Many devices are constantly searching for available Wi-Fi networks to access. If you are not going to use it, then don't have it turned on.

A FINAL WORD

A final word for your online safety. No one can be 100% safe online from hackers or cybercrime just as no one can be safe using traditional mail. The key is to take the precautions you can and remain vigilant for anything unusual online.