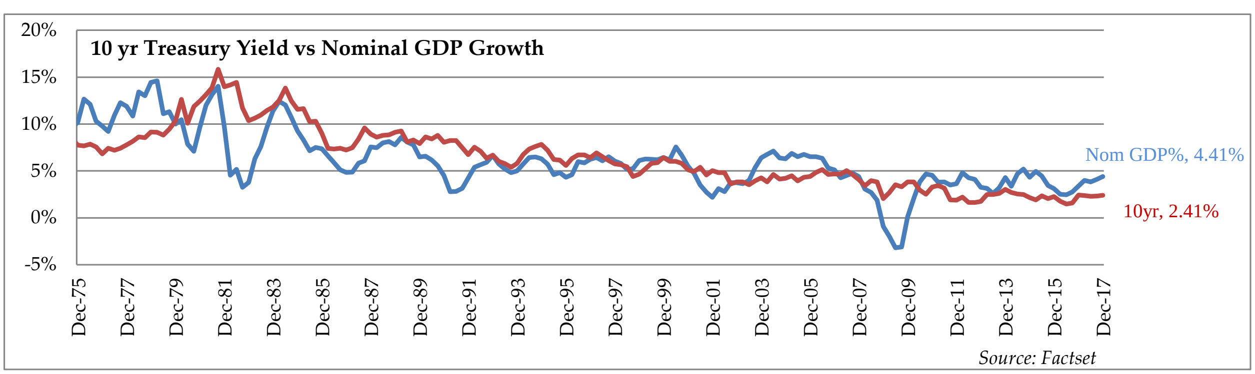
MID-QUARTER UPDATE – FEBRUARY 2018

If an investor had fallen asleep a la Rip Van Winkle on 12/31/17 and awoke today, a quick look at the major equity indices would suggest that the first two months of 2018 were uneventful. The S&P 500 is up about 3%, the Small Cap Russell 2000 and International MSCI EAFE are both up 1%, and the MSCI Emerging Markets index is 5% higher. After a strong 2017, stocks seem to have held steady. However, as the still drowsy investor scanned over to the fixed income side of the markets, there would start to be clues something was afoot. The Bloomberg Barclays Aggregate Index is 2% lower. The Merrill Lynch Investment Grade Bond Index is off a similar 2%, while the 7-10 year Treasury Index has declined 3%. The driving force behind this relatively poor bond performance is rising interest rates: the 10 year Treasury moved from 2.41% to 2.87%, and as interest rates rise, bond prices fall.

Regular readers of Grimes & Company communications are familiar with our ongoing observations about the financial markets. Interest rates and stock volatility are historically low because of central bank intervention, and stock valuations are above average. Thus, investors may not be properly compensated for the risk of investing, meaning that future returns may be disappointing to investors expecting a continuation of the returns achieved over the past several years.

The markets have begun to show signs of waking from their own slumber. After exceptionally low volatility in 2017, the markets went into full "melt up" mode in January, as the fear of missing out took over the fear of loss and investors rushed in as markets seemed to be setting new record highs on a daily basis. In February, this changed. Sparked by strong wage growth in the unemployment report on 2/6, bond yields rose and stock prices fell, as investors became concerned inflation pressures were finally appearing in the economic data. After two weeks of trading, the stock market declined more than 10% from its peak. The 10yr Treasury reached as high as 2.94%, and the CBOE Volatility Index (VIX), which had recently been sitting at historically low levels below 10, surged to over 50, a level not seen since the middle of the late 2008-2009 financial crisis.

The problem, ironically, is the strength of the economy: strong economic data raises concerns of rising interest rates, which causes stocks to fall. The reason for this is that interest rates tend to follow nominal economic growth. Nominal GDP is simply Real GDP, the number touted in the financial headlines, plus inflation. For example, 3% Real GDP plus 2% inflation equals 5% Nominal GDP growth. And as the chart below shows, over time the yield on the 10 year Treasury tends to be similar to Nominal GDP growth.



Source: Factset

The deviation from this relationship since 2009 can be attributed to central bankers buying bonds and pushing yields below where the market would otherwise price them. At the same time, concerns of the "new normal" of low growth and low inflation, say 2% growth and 1% inflation for 3% nominal GDP growth, allowed the market to accept these low rates as a possible sign that low nominal growth could be here for some time.

However, signs of growth have been emerging. In fact, last year's strong equity market returns were predicated on the best period of synchronized global growth since the recession in 2008. But the bond market was slower to respond as central bankers, who have been manipulating rates, were still waiting for signs of inflation to pick up. While most investors knew where interest rates probably should be, after nearly 10 years of central bankers pushing long term rates lower, few wanted to be on the wrong side of what has been a bull market for bonds. Thus the strong wage growth reported on 2/6 triggered a severe market reaction. The prospect of 3% GDP growth, 2% inflation, and a Fed selling, not buying, bonds, would suggest an equilibrium 10yr yield of 4% to 5%. Add in the expected increase in the deficit from tax reform, and thus more government borrowing, and the path of least resistance for interest rates seems to have shifted from lower to higher. There are many scenarios on how this could play out but here are two.

Assuming the economic data remains sound and the Fed continues to raise rates gradually (three hikes are expected in 2018), the expectation would be for a see-saw effect. On one side, good data leads to optimism on profits, pushing up stock prices. On the other side the economic optimism feeds concern on bonds, causing interest rates to move higher, creating a headwind for stocks. Considering the fiscal stimulus with tax cuts and the current trajectory this scenario seems very reasonable.

The more difficult scenario is, either due to inflation accelerating or deficits rising, the Fed is seen as losing control of the bond market and having to push rates higher regardless of profits. Higher rates despite reduced expectations for earnings would be problematic for stocks.

Overall, we see several trends that were historically abnormal working back to normal and this is a very healthy process. Volatility returning to the market is unquestionably a good thing. Investors need to be reminded about the risks of holding equities and the price movements it could bring. But such moves are not usually painless and can overshoot in the opposite direction. Our advice, as always, is that investors should position their portfolio to reach their long term goals, while recognizing and being able to handle periodic bouts of market volatility along the way. A properly constructed portfolio thus allows the investor to tune out the day-to-day noise of the markets and sleep well, like Rip Van Winkle.

Operational Notes

- **An important note regarding checks**: **Please include your account number in the memo section on any checks that are sent to us for deposit.** If you do not know your account number, please feel free to call the office for this information. As always, checks should be made payable directly to the custodian (Fidelity, TD Ameritrade or Charles Schwab) and never made payable to Grimes & Company. Unfortunately, we will be required to return any checks that are not filled out properly.

All the best,

Kevin T. Grimes, CFA, CFP®
President/Chief Investment Officer

*Please see Important Disclosures on final page

Cybercrime and fraud are serious threats and constant vigilance is key. Cyber criminals exploit our increasing reliance on technology. Methods used to compromise a victim's identity or login credentials – such as malware, phishing, and social engineering – are increasingly sophisticated and difficult to spot. A fraudster's goal is to obtain information to gain access to your account and assets or sell your information for this purpose. Fortunately, criminals often take the path of least resistance. Following best practices and applying caution when sharing information or executing transactions makes a big difference.

While our firm plays an important role in helping protect your assets, you can also take action to protect yourself and help secure your information. The below outline summarizes common cyber fraud tactics, along with tips, best practices, and actions to take if you suspect that your personal information has been compromised.

- Communicating with our Office:
  - Keep us informed regarding changes to your personal information.
  - Expect us to call you to confirm email requests to move money, trade, or change account information.
  - When sending us confidential information, utilize our secure email service or securely upload via our website: http://www.grimesco.com/upload-documents
- Exercise Caution when Sharing Information
  - Be aware of suspicious phone calls, emails, and texts asking you to send money or disclose personal information. If a new or unknown service representative calls you, hang up and call back using a known phone number.
  - Never share sensitive information or conduct business via unsecured email, as accounts are often compromised.
  - Never enter confidential information in public areas. Assume someone is always watching.
  - Check your email, account statements, and credit reports regularly for suspicious activity.
- Protect your Computer and Network
  - Don't open links or attachments from unknown sources. Enter the web address in your browser.
  - Protect your computer against new viruses or other attacks with anti-virus and anti-spyware software, and configure all software for automatic updates. The anti-virus and anti-spyware software included in operating systems requires frequent updates to keep pace with new risks.
  - Use the latest version of your web browser. Strong encryption protects your information as it travels over the Internet.
  - Do not allow software to be loaded on your computer if you're not completely familiar with it. If you share your PC with anyone, including your children, make sure they know the rules for downloading and installing software.
  - Check security settings on your applications and web browser. Make sure they're strong.
- Create Secure Passwords and Protect them
  - Use a combination of letters and numbers for passwords you create (i.e. 4funcallC3po, Il9vemyd1g).
  - Don't use personal information as part of your login ID or password
  - Never share login credentials
  - Create a unique, complex password for each website, and change it every six months. Consider using a password manager to simplify this process.
  - Log out completely to terminate access when exiting all websites.
  - Do not enter username/password data on public computers or free Wi-Fi. Use a personal Wi-Fi hotspot or a Virtual Private Network (VPN).

- What to do if you suspect a breach
    - Call our office immediately so we can watch for suspicious activity and help with necessary steps to protect your investment accounts. TD Ameritrade, Fidelity Investments, and Charles Schwab have online fraud policies in place that pledge to reimburse assets stolen due to unauthorized online transactions.
    - Clean your computers of any malware. There are some reliable anti-virus programs available that you can run yourself, or you can take the computer to a trusted professional in your area to have it cleaned.
    - Change your passwords for all services, including e-mail, social networking sites (e.g.: Facebook), financial sites, etc.
    - Consider placing a fraud alert with Experian, TransUnion, or Equifax.
- Know the Threats
    - Identity Theft - using a person's personal or financial data to commit fraud—is one of the most rapidly growing global crimes. The targets of this crime are personal information, financial information, and access to online accounts. The personal information often targeted includes: name, address, date of birth, Social Security number, driver's license number, passport and/or signature. The financial information often sought is User IDs and passwords, account numbers and ABA numbers, credit card numbers, ATM / Debit cards and/or checks.
    - Phishing—sometimes also referred to as pharming—opens the door to identity theft and computer security breaches. Phishing is when someone attempts to steal personal or financial information. It usually starts with an email asking for sensitive information, such as your User ID or user name, your password, or your account information.
    - Spyware - As its name suggests, spyware is software that is used to "spy" on your computer. It poses two problems: invasion of privacy and adversely affecting your computer's performance.
    - Viruses - A virus is computer code that infects your computer when you take a certain action, such as double clicking on an email attachment. A virus typically embeds itself in your existing software and uses it to reproduce and spread.
    - Worms - Unlike viruses, worms are stand-alone programs. They do not embed themselves into software, but spread by duplicating themselves without any intervention from you.
    - Trojans - A Trojan is a stand-alone program that spreads by masquerading as a harmless file or program and tricking the user into installing it on his or her machine. Many Trojans arrive under the guise of a picture, screensaver, or email attachment. Once a user opens the file, the Trojan installs itself on the computer and may take over the computer's email program or use its own email program for malicious purposes.

110 Turnpike Road, Suite 100 • Westborough MA 01581
Tel. (508) 366-3883 • Fax (508) 366-0999 • E-mail: advisors@grimesco.com

Sources include eSignal.com, Bureau of Economic Analysis, Bureau of Labor Statistics and FactSet
Not a substitute for tax or legal advice.