HAAS Fydroski Financial Services, Inc.
Investments - Planning - Education

IPE Insights

APRIL 2014

JIM'S JOURNAL

James H. Fydroski CFP® , President
President, Haas Financial Services Inc.

Look Back—1st Quarter 2014

"Being slow and steady means that you're willing to exchange the opportunity of making a killing for the assurance of never getting killed." – Carl Richards

After strong gains in 2013 that were fuelled primarily by the Federal Reserve's massive stimulus program, expectations for a repeat performance in the first quarter 2014 were very high. This proved not to be the case as all the major market averages were negative at the end of January. Domestic markets rallied back in February and early March, lost momentum in mid-March but rallied again at the very end to squeak out positive gains for most of the major markets. The exception was the DOW which ended slightly negative for the quarter.

The underperformance of the key averages in the first quarter 2014 was the weakest in the past four years. In 2012 and 2013 the S&P 500 was up +12% and +10% respectively in quarter one. On March 31, 2014, the S&P 500 was up +1.3% and this topped the major averages. The NASDAQ came in second with a gain of +0.5% and the DOW was down -0.7% (Source: Wall Street Journal 4-1-2014).

Diversified stock and stock/bond mutual funds matched the S&P 500 with an average gain of +1.3%. Real Estate lead the sector funds with a +9.0% rate of return. Utilities came in second with an average return of +7.4%. The category leader across the board was Gold Oriented Funds with a whopping return of +12.2% in the first quarter. However, we should not forget that even with this outstanding quarter, Gold Oriented Funds were still down -31.0% over the last year. The return on Taxable Bond Funds ranged from +1.5% for the Intermediate U.S. category to +3.0% for Long-Term bonds. The average taxable Bond Fund was up +1.7% in the first quarter 2014 (Source: Wall Street Journal 4-7-2014).

Volatility has increased in 2014. As often happens when the market pulls back, the sectors of the market that had been doing well frequently get hit the hardest. One of the more interesting stories from the first quarter came out of the Health/Biotechnology sector. Health/Biotech ended 2013 with an average return of +48.8%. This sector continued its winning ways in 2014 until about mid-March. Around that time a Congressional Committee asked Biotech Company Gilead Sciences to justify the price it was charging for Sovaldi, the company's blockbuster hepatitis C drug. It was as if someone opened the flood gates. Biotech and Healthcare stock and mutual fund prices started dropping like rocks and continued to drop into April. Gold Oriented Funds also dropped substantially at that time after a strong start to the year. The Money Management Program held partial investment positions in these sectors. The positions were sold a few days after the initial downturn and losses were experienced but not to the extent of the full downturn.

With the Federal Reserve's near-zero interest rate policy and quantitative easing that has infused billions into the economy over the last several years, stocks have remained in bull market territory. However, investors and traders have become jittery as of late that the Fed's easy monetary policies may finally be winding down and moving toward an end. New Federal Reserve Chairwoman, Janet Yellen, unsettled the markets and caused a brief sell-off after the Fed's March meeting when she suggested the Federal Funds Rate could be raised as early as the middle of next year. That "rookie" mistake was later "corrected" to clarify that rate hikes would not come sooner than expected. Stock prices are historically based upon whether a company is making money or has the prospect of making money. This snafu by Yellen was just another example of how the stock market has been driven over the last several years by government monetary policy and not by corporate profitability. In the history of our country there has never been a stimulus program equal to the magnitude of the last few years. We still do not know how it will all unwind. Personally, it does not elicit a feeling of comfort and confidence in me since big government spending programs seem to get it wrong more often than not.

This month's guest article about online financial transactions is from the Financial Planning Association. With the many security breaches that have taken place recently, we need to take all the steps that we can to protect ourselves when using the internet. HELLO SPRING. I'm glad that you are finally here. I spent Easter weekend up north and on the tractor tending the chestnut trees. It was a wonderful feeling to be walking around without a heavy coat and hat. Take good care!!!

Know Your Protections and Risks When Banking Online

As Americans increasingly migrate toward conducting banking and other financial transactions on line, the threat of falling victim to ever-more sophisticated cyber-crimes continues to rise. Financial services companies are keenly aware of the potential security risks posed by online money transfer. That is why the industry as a whole has developed a series of standard security protocols designed to ensure that customers' assets and personal information is kept safe.

Following is a list of common security features offered by most banks and financial institutions. Be sure to compare these measures with what your own bank, credit card companies, and other financial vendors have in place.

Anti-malware software. Anti-malware is a term commonly used to describe various software products used to prevent, detect, block and remove malicious software products that are intended to damage or disable computer or computer systems. Anti-malware software may also be referred to as anti-virus or anti-spyware.

Transaction monitoring/anomaly detection. Network monitoring software has been in use by financial institutions for a number of years. Similar to the way in which the credit card industry detects and blocks fraudulent credit card transactions, systems are now available to monitor online banking activity for suspicious funds transfers. For instance, too many incorrect login attempts will signal the system to lock a user out of their account until positive account verification can be confirmed. Transaction amounts (specifically withdrawals) that fall outside the customer's normal or pre-established limits are also scrutinized.

Multilayered authentication. Many online banking/financial systems now require multiple layers of user identification, or authentication, that only those authorized can provide. For instance, some authentication protocols verify the device the customer is using to access the bank's website. If the device does not match the banks records, additional authentication measures, such as one or more challenge questions will be presented to the customer. Similarly, a number of institutions are requiring "out of band" authentication, which requires a transaction initiated via one delivery channel (e.g., Internet) to be re-authenticated via a different channel (e.g., telephone) in order for the transaction to be completed.

Firewalls. Firewalls are software-or hardware-based security systems that create a secure barrier between your bank's internal network, where your information is stored, and the unsecured internet. The data "traffic" flowing in and out of the bank's network is monitored and analyzed to determine its legitimacy.

Encryption. Encryption scrambles information being transmitted between your device and the bank's network into a code that is virtually impossible to decipher, thereby protecting against unauthorized access. Many financial institutions now use 128-bit encryption, an advanced encryption technology.

Customer Education: The Lynchpin of Any Security Program.

In the final analysis, even the most sophisticated security measures are no substitute for well-informed customers. Toward that end the Federal Financial Institutions Examination Council (FFIEC), a body of the federal government made up of several U.S. financial regulatory agencies, issued guidance suggesting that, at a minimum, a financial institution's customer education efforts should include:

- An explanation of protections provided, and not provided to account holders relative to electronic funds transfers.
- An explanation of under what, if any, circumstances through what means the institution may contact a customer on an unsolicited basis and request confidential account-related credentials.
- A list of risk-control measures that customers may consider implementing to mitigate their own risk.
- A list of appropriate contacts for customers to use if they notice suspicious account activity or experience security-related events.

Source: The Federal Financial Institutions Examination Council (FFIEC), "FFIEC Supplement to Authentication in an Internet Banking Environment," June 29, 2011.

ADVISORY SERVICES OFFERED THROUGH HAAS FINANCIAL SERVICES, INC.

21415 CIVIC CENTER DRIVE, SUITE 117A, SOUTHFIELD, MI 48076

HTTP://WWW.HAASFSI.COM/ PH 248-728-0028 Fax 248-499-1972 Jim@haasfsi.com