# FINANCIAL CONNECTIONS
GROUP INCORPORATED

*1st Quarter 2015, 4/16/2015*

## FIRST QUARTER UPDATE

The U.S. and Global indices had small positive returns (other than commodities' continued decline) with an increasing amount of anxiety—waiting for the Federal Reserve to finally increase interest rates.

Investors have been waiting for the Fed to act for the last couple of years yet interest rates continue to decline with the 10-year Treasury yielding 1.87%!

Incremental rises in interest rates are not closely associated with bear markets. In fact, they usually rise because rising interest rates are a sign of a healthy economy. The Fed no longer believes an artificial stimulus is necessary. Companies and their stocks tend to perform well in healthy economies.

Positive Numbers

The U.S. is less dependent on foreign oil than at any time since 1987, with a continued trend toward independence. Energy, in general, is cheaper now than it has been in several decades, making our lives, and the production of goods and services, less expensive.

More Americans are working. U.S. unemployment (5.5%) is trending lower and is now reaching levels that are actually below the long-term norms. Unemployment today is lower than the rate for much of the booming 90s and is approaching the lows of the early 70s.

Real GDP increased to 2.4% in 2014 after rising 2.2% in 2013. Slow growth is not necessarily a bad thing. In the past, rapid growth often precedes recessions where excesses need to be corrected. It may be boring, but it is certainly not bad news.

Upcoming Concerns

The strong dollar will have a negative effect on corporations that have significant business overseas. The dollar is back to the level it was in 2002. Dr. David Kelley, Chief Strategist at JP Morgan, expects the strong dollar to cost us 0.07% of GDP annually.

*Continued inside*

### Inside This Newsletter



Included with this package are your portfolio reports for the first quarter 2015 along with our current ADV (disclosure statement) and Privacy Statement. Please let us know if you have any questions about its content.

## REFLECTIONS

Below is a poem printed in the April 2015 newsletter from *The Woods*, a senior community in Little River. Jill and Bonnie have a vacation home in the park. No author was identified but Jill enjoyed the sentiment and the humor and thought others might too.

*I look in the mirror and what do I see*
*A strange-looking person who cannot be me,*
*For I am much younger and not nearly so fat,*
*As that face in the mirror I'm looking at.*

*Oh, where are the mirrors I used to know?*
*Like the ones that were made thirty years ago.*
*Now all things have changed and I'm sure you'll agree,*
*Mirrors aren't as good as they used to be.*

*So never be concerned if wrinkles appear,*
*For there's one thing I've learned that is very clear,*
*That should your reflection seem less than perfection,*
*It's merely the mirror that needs correction.*

## *FIRST QUARTER UPDATE*
***(continued)***

While the oil decline somewhat offsets the strong dollar, his corollary is "oil is in the basement and the dollar is in the attic."

Wage growth continues to be slow, squeezing workers on Main Street.

The stock market is expensive in absolute terms but not as much in relative terms (compared to interest rates).

If you would like to review or modify your portfolio strategy, please let us know. If you would like to create or update your financial plan, don't hesitate to give us a call.


## FINANCIAL CONNECTIONS GROUP, INC.

This newsletter is written quarterly by Financial Connections Group, Inc. Please contact Financial Connections Group, Inc. if there are any changes in your financial situation or investment objective(s). Remember, past performance may not be indicative of future results. Different types of investments involve degrees of risk, and there can be no assurance that the future performance of any specific investment, investment strategy, or product made reference to directly or indirectly in this newsletter, will be profitable, equal any corresponding indicated historical performance level(s) or be suitable for your portfolio. Information herein should not be construed as tax or legal advice.

**Jill D. Hollander**, CFP®, CRPC ℠, ADPA™, Financial Advisor
**Brian Pon**, EA, CFP®, Financial Advisor

Financial Connections Group, Inc.
21 Tamal Vista Blvd., Suite 105
Corte Madera, CA 94925
415.924.1091

Berkeley Office:
2608 Ninth Street, Suite 302
Berkeley, CA 94710
510.849.4667

EMAIL: client@FinancialConnections.com
WEBSITE: http://www.FinancialConnections.com

## CYBERSECURITY – STEPS TO TAKE

We wrote previously about some steps you can take to protect your identity. What follows is a more comprehensive discussion. The checklists are individual pages so you can keep them in a handy location.

Keeping your information secure is a top priority of Financial Connections. To better protect you and your accounts from cybersecurity threats, we continuously review our security procedures to ensure that we are following best practices recommended by the custodians, financial institutions, and industry experts with whom we work.

While we feel we are taking clear and actionable steps in our own security measures, cyber fraud continues to escalate, is becoming more sophisticated, and is ever changing. The various threats include email scams (e.g., phishing), where criminals obtain a person's identity and use that information to commit various forms of wire fraud. Add to that the absence of care by corporations to safeguard information (e.g., Anthem) and it is apparent we must be more active on our own behalf.

As a fiduciary to your financial accounts, we are encouraging our clients to embrace a series of measures to help protect your identity and mitigate potential security risks. We've included our ***Investor Protection Checklist***, which outlines some best practices for investors across six key areas to help you:

- Manage your devices
- Protect all passwords
- Surf the Web safely
- Protect information on social networks
- Protect your email accounts
- Safeguard your financial accounts

Please carefully review this checklist with all members of your household. We also ask that you do the following:

- If you change your address or other contact information, notify us so that we can update our records.
- If you suspect that your email account and/or confidential information have been compromised, refer to our ***Responding to Fraudulent Activity Checklist***, also in this packet, which provides actionable steps and contact information to organize your response.

**Common Tactics Used to Steal Your Identity and Login Credentials**

Criminals use a number of tactics to compromise a victim's identity or to access important login credentials. After gaining access to an investor's personal information, criminals can use it to commit various types of fraudulent activity. The most common tactics are described below:

*Continued next page*

***CYBERSECURITY – STEPS TO TAKE***
***(continued)***

**Malware**
Using malicious software (hence, the prefix "mal" in malware), criminals gain access to private computer systems (e.g., home computers) and gather sensitive personal information such as Social Security numbers, account numbers, usernames and passwords, and more.
*How it works:* While malware can be inserted into a victim's computer by various means, it often slips in when an unwary user clicks an unfamiliar link (opens attachment).

**Phishing**
In this ruse, the criminals attempt to acquire sensitive personal information from you via email. Phishing is one of the most common tactics observed in the financial services industry.
*How it works:* Masquerading as an entity with which the victim already has a financial relationship (e.g., a bank, credit card company, brokerage company, government agency, or other financial services firm), the criminals solicit sensitive personal data from unwitting recipients either by prompting the victim to provide personal information or by unknowingly installing malware on the computer (when a link or attachment is clicked on), which then compromises the computer's security going forward.

**Social Engineering**
Via social media and other electronic media, criminals gain the trust of victims over time, manipulating them into divulging confidential information.

*How it works:* Typically, these scammers leverage something they know about the person—like their address or phone number—to gain their confidence and get them to provide more personal information, which can be used to assist the criminal in committing fraud. Social engineering has increased dramatically, and many times fraudsters are contacting investors by telephone.

## NEW ACCOUNT FOR PEOPLE WITH DISABILITIES

Starting this year a new tax-free savings account called ABLE (acronym for Achieving a Better Life Experience) is available for the disabled. The requirements for disability are:

- Diagnosed before age 26
- Must be a long-term physical or intellectual disability

Who can contribute?

- Family members and friends
- Nondeductible contribution up to $14,000 annually

Funds must be used for such items as housing, education, transportation, job training and dental care. The withdrawals are tax-free and do not affect Medicaid eligibility. However, a balance of $100,000 or more *will* affect SSI benefits.

Jill D. Hollander

Brian Pon

FINANCIAL CONNECTIONS
GROUP INCORPORATED

FINANCIAL CONNECTIONS
GROUP INCORPORATED

## Investor Protection Checklist

The educational checklist presented below is designed to help you take appropriate action to better protect you and your family and mitigate the risk of cyber fraud.* Carefully review the items in each of the categories below to determine which apply to your unique situation.

| TOPICAL AREA | ACTIONS TO CONSIDER |
|---|---|
| **Manage your devices** | ⇒ Install the most up-to-date antivirus and antispyware programs on all devices (PCs, laptops, tablets, smartphones) and install updates as they become available. These programs are most effective when users set them to run regularly rather than just running periodic scans, which may not provide maximum protection to your device.<br>⇒ Activate the computer's firewall to protect your computer from hackers.<br>⇒ Access sensitive data only through a secure location or device; never access confidential personal data via a public computer, such as in a hotel or cybercafé.<br>⇒ If you have children, set up a separate computer they can use for games and other online activities. |
| **Protect all passwords** | ⇒ Use a personalized custom identifier for financial accounts you access online. Never use your Social Security number in any part of your login activity.<br>⇒ Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships.<br>⇒ Avoid storing passwords in email folders. Consider using a password manager program. |
| **Surf the Web safely** | ⇒ Do not connect to the Internet via unsecured or unknown wireless networks, such as those in public locations like hotels or cybercafés. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data. |
| **Protect information on social networks** | ⇒ Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birthdate, home address, and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays, or loss of loved ones. Sharing too much information can make you susceptible to fraudsters and allow them to quickly pass a variety of tests related to the authentication of your personal information. Never underestimate the public sources that individuals will use to learn critical facts about people. |
| **Protect your email accounts** | ⇒ Delete any emails that include detailed financial information beyond the time that it's needed (don't forget to delete these emails from your deleted mail folder as well).<br>⇒ Continuously assess whether you even need to transmit and store personal and financial information via your email account. Think of your emails as postcards - would you want strangers having access to the information being exchanged?<br>⇒ Use secure data storage programs to archive critical data and documents.<br>⇒ Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those that warn that your computer is infected with a virus and request that you take immediate action.<br>⇒ Establish separate email accounts for personal correspondence and financial transactions. |
| **Safeguard your financial accounts** | CONTINUED NEXT PAGE |

***Investor Protection Checklist (continued)***

| TOPICAL AREA | ACTIONS TO CONSIDER |
|---|---|
| **Safeguard your financial accounts** | ⇒ Contact your financial institutions and ask about establishing two-factor login authentication for your online accounts.<br>⇒ Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held.<br>⇒ Never send account information or personally identifiable information over email, chat, or any other unsecure channel.<br>⇒ Suspiciously review any unsolicited email requesting personal information. Further, never respond to an information request by clicking a link in an email. Instead, type the web site's URL into the browser yourself.<br>⇒ Avoid developing any online patterns of money movement, such as wires, that cyber criminals could replicate to make money movement patterns appear more legitimate. |

*Please note that this list is not exhaustive and cannot guarantee protection against cyber fraud.

## Responding to Fraudulent Activity - Checklist and Contact Information

Always act quickly when you suspect you are a victim of cyber fraud. Below are some resources to help organize your response.

| FRAUD TYPE | ACTIONS TO CONSIDER |
|---|---|
| **Receipt of phishing email** (but did not click links or respond with confidential information) | ⇒ If you suspect an email is a phishing scam, notify the legitimate company right away.<br>⇒ If a suspicious email purports to come from Financial Connections Group or TD Ameritrade, contact Financial Connections immediately.<br>⇒ If email purports to come from the Securities and Exchange Commission, alert the SEC by submitting a tip online at https://denebleo.sec.gov/TCRExternal/disclaimer.xhtml<br>⇒ Consider reporting the scam to the FBI's Internet Fraud Complaint Center at http://www.ic3.gov/<br>⇒ Permanently delete the email from your mailbox (after deleting the email from your Inbox, go to your Deleted folder and delete the email again). |
| **Email account compromises** | ⇒ Immediately contact your brokerage firm, credit card issuers, and other financial institutions for next steps.<br>⇒ Notify national credit bureaus to file a fraud alert for you.<br>⇒ Check accounts for fraudulent transactions and work with your financial institutions to close any accounts fraudulently opened or used.<br>⇒ Contact your email account provider and follow their suggested next steps (i.e., changing your login credentials).<br>⇒ Change your login credentials for all financial accounts. |
| **Fraudulent account activity** (i.e., unauthorized withdrawals) | ⇒ Immediately contact the financial provider where the fraud occurred.<br>⇒ For Financial Connections managed accounts within business hours, contact Financial Connections first. Financial Connections will facilitate next steps with TD Ameritrade.<br>⇒ If it's after Financial Connections business hours, proceed in calling TD Ameritrade directly then notify Financial Connections. |
| **Suspected identity theft** | ⇒ If you think your personal information has been stolen, visit the Federal Trade Commission's feature on identity theft at http://www.ftc.gov/idtheft for information on how to control the damage or call their FTC Identity Theft hotline at 1-877-438-4338. |

FINANCIAL CONNECTIONS
GROUP INCORPORATED

## Contact Information

## Investor Protection and Responding to Fraudulent Activity

**Financial Connections Group**

Telephone: (415)924-1091 or you may email us at client@financialconnections.com.

*Note: If you are unable get a person at Financial Connections, please call TD Ameritrade (see below).*

**TD Ameritrade Institutional**

Telephone: (800) 431-3500 Option 2. You will need your account number or Social Security number. TD Ameritrade will ask security questions. Their hours are 5:30 AM – 5:00 PM Pacific Time Monday through Friday.

**National Credit Bureaus**

Equifax: 1-888-766-0008 or www.equifax.com

Experian: 1-888-397-3742 or www.experian.com

Trans Union: 1-800-680-7289 or www.transunion.com

**FTC Identity Theft Hotline**

1-877-438-4338 or http://www.ftc.gov/idtheft