North Carolina
Department of the Secretary of State
Hon. Elaine F. Marshall, Secretary
Securities Division

PO Box 29622 | Raleigh NC | 27626-0622 | (919) 733-3924 | (800) 688-4507 | www.sosnc.com

January 2012 NEWSLETTER. Vol. 4, No. 1

Resolve to Check Before You Invest in 2012

NC Securities Division Offers Resources to Help You Achieve Your Financial Goals and Learn about Investing

The first weeks of the New Year are "make-it-or-break-it" for resolutions to lead a healthier lifestyle in 2012. It is not too late to resolve to improve the health of your finances. The North Carolina Securities Division can help you give your investments a check-up.

The vast majority of investment scams can be discovered by a simple check. Resolve to always call the Securities Division at (800) 688-4507 or (919) 733-3924 before you invest to make sure your broker or financial adviser is properly registered and that great investment opportunity is not a scam.

Visit the Securities Division's website at www.sosnc.com to find a wealth of information to help you review your investment goals and set new ones for the year. The Securities Division offers free online brochures that outline the risks and rewards of investing in today's markets and how to protect yourself from scams and frauds.

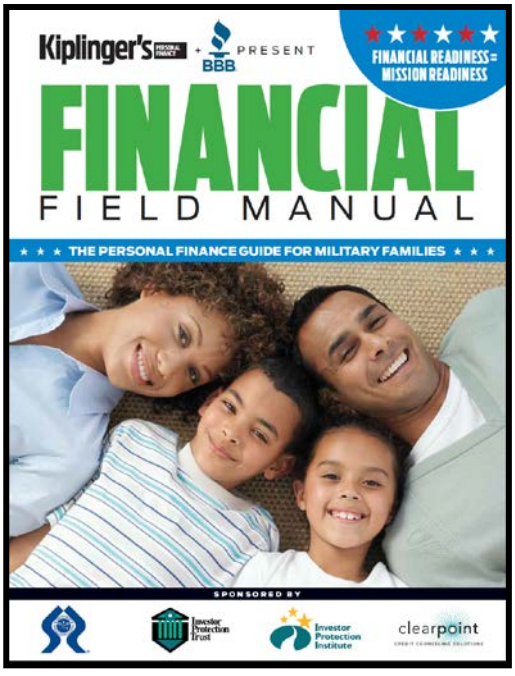
Education is the best medicine to prevent investment fraud. Resolve to attend an investor education event sometime during 2012. Chances are good a program will be held near you this year. Check out the Calendar of Upcoming Events page in each newsletter. Better yet, resolve to help others by calling John Maron (919-807-2106) or Barbara Bennett (919-807-2015) to schedule an investor education event for your organization.

HOT Off the Press!

Just in time for **Military Saves Week** (February 19–26, 2012), the North Carolina Securities Division has received a huge shipment of the ***Financial Field Manual***, a 20-page personal finance guide for military families produced by *Kiplinger's Personal Finance* magazine in association with the Better Business Bureau.

The ***Financial Field Manual*** recognizes that military personnel and their families face unique financial challenges and opportunities. Its goal is to inform military personnel about these financial issues so that they may make better informed decisions.

The Securities Division will be distributing copies of the ***Financial Field Manual*** to military bases around the state. However, if you or someone you know would like a free copy, contact John Maron (919-807-2106) or Barbara Bennett (919-807-2015). Please be sure to include your name and mailing address and the number of copies you would like to have.



The following information was originally published by the U.S. Securities and Exchange Commission (SEC) and is reprinted here solely for informational purposes.

Investor Alert: Social Media and Investing - Avoiding Fraud

The SEC's Office of Investor Education and Advocacy is issuing this Investor Alert to help investors be better aware of fraudulent investment schemes that may involve social media. U.S. retail investors are increasingly turning to social media, including Facebook, YouTube, Twitter, LinkedIn and other online networks for information about investing. Whether it be for research on particular stocks, background information on a broker-dealer or investment adviser, guidance on an overall investing strategy, up-to-date news, or to simply discuss the markets with others, social media has become a key tool for U.S. investors.

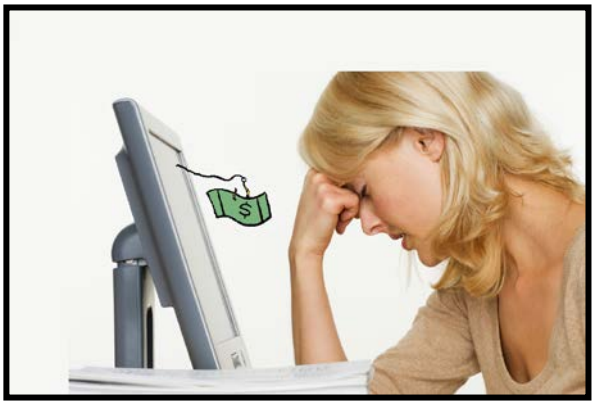
While social media can provide many benefits for investors, it also presents opportunities for fraudsters. Social media, and the Internet generally, offer a number of attributes criminals may find attractive. Social media lets fraudsters contact many different people at a relatively low cost. It is also easy to create a site, account, email, direct message, or webpage that looks and feels legitimate – and that feeling of legitimacy gives criminals a better chance to convince you to send them your money. Finally, it can be difficult to track down the true account holders that use social media. That potential for anonymity can make it harder for fraudsters to be held accountable. As a result, investors need to use caution when using social media when considering an investment.

What You Can Do To Protect Yourself - Tips to Help Avoid Fraud Online

So, what can individual investors do to use social media, while at the same time protecting themselves?

The key to avoiding investment fraud on the Internet is to be an educated investor. Below are five tips to help you avoid investment fraud on the Internet:

1. **Be Wary of Unsolicited Offers to Invest**
   Investment fraud criminals look for victims on social media sites, chat rooms, and bulletin boards. If you see a new post on your wall, a tweet mentioning you, a direct message, an e-mail, or any other unsolicited – meaning you didn't ask for it and don't know the sender – communication regarding a so-called investment opportunity, you should exercise extreme caution. ***An unsolicited sales pitch may be part of a fraudulent investment scheme.*** Many scams use spam to reach potential victims. For example, with a bulk e-mail program, spammers can send personalized messages to millions of people at once for much less than the cost of cold calling or traditional mail. If you receive an unsolicited message from someone you don't know containing a "can't miss" investment, your best move is to pass up the "opportunity" and report it to the SEC Complaint Center.



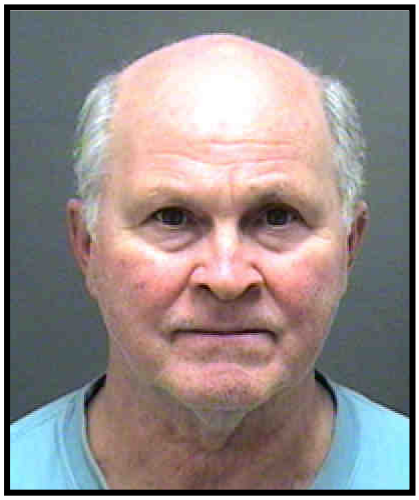
(Continued on p. 3)

(Continued from p. 2)

2. Look out for Common "Red Flags"

Wherever you come across a recommendation for an investment – be it on the Internet or from a personal friend (or both), the following "red flags" should cause you to use extreme caution in making an investment decision:

- **It sounds too good to be true**. Any investment that sounds too good to be true probably is. Compare any promised return with the returns on well-known stock indexes. Any investment opportunity that claims you'll receive substantially more than that could be highly risky – or be an outright fraud. Be extremely wary of claims on a website that an investment will make "INCREDIBLE GAINS" or is a "BREAKOUT STOCK PICK" or has "HUGE UPSIDE AND ALMOST NO RISK!" Claims like these are hallmarks of extreme risk or outright fraud.



The Face of Affinity Fraud

Sidney S. Hanson of Charlotte crafted his investment scam to appeal to victims through their deeply held religious beliefs. Hanson pled guilty to securities and mail fraud in 2009 and was sentenced to 22 years in federal prison in March 2011.

- **The promise of "guaranteed" returns.** Every investment entails some level of risk, which is reflected in the rate of return you can expect to receive. If your investment is 100% safe, you'll most likely get a low return. Most fraudsters spend a lot of time trying to convince investors that extremely high returns are "guaranteed" or that the investment "can't miss." Don't believe it.

- **Pressure to buy RIGHT NOW.** Don't be pressured or rushed into buying an investment before you have a chance to think about – and investigate the "opportunity." Be especially skeptical of investments that are pitched as "once-in-a-lifetime" opportunities, particularly when the promoter bases the recommendation on "inside" or confidential information.

3. Look out for "Affinity Fraud"

Never make an investment based solely on the recommendation of a member of an organization or group to which you belong, especially if the pitch is made online. An investment pitch made through an online group of which you are a member, or on a chat room or bulletin board catered to an interest you have, may be an affinity fraud. Affinity fraud refers to investment scams that prey upon members of identifiable groups, such as religious or ethnic communities, the elderly, or professional groups. Even if you do know the person making the investment offer, be sure to check out everything – no matter how trustworthy the person seems who brings the investment opportunity to your attention. Be aware that the person telling you about the investment may have been fooled into believing that the investment is legitimate when it is not.

4. Be Thoughtful About Privacy and Security Settings

Investors who use social media websites as a tool for investing should be mindful of the various features on these websites in order to

(Continued on p. 4)

(Continued from p. 3)

protect their privacy and help avoid fraud. Understand that unless you guard personal information, it may be available not only for your friends, but for anyone with access to the Internet – including fraudsters.

For more information on privacy and security settings, as well as other guidance regarding setting up on-line accounts with an eye toward avoiding investment fraud, see the SEC's Investor Bulletin *Social Media and Investing: Understanding Your Accounts*.

5. Ask Questions and Check Out Everything

Be skeptical and research every aspect of an offer before making a decision. ***Investigate the investment thoroughly and check the truth of every statement you are told about the investment.*** Never rely on a testimonial or take a promoter's word at face value. You can check out many investments using the SEC's EDGAR filing system or your state's securities regulator. You can check out registered brokers at FINRA's BrokerCheck website and registered investment advisers at the SEC's Investment Adviser Public Disclosure website. See our publication "Ask Questions" for more about information you should gather before making an investment.

A Few Common Investment Scams Using Social Media and the Internet

While fraudsters are constantly changing the way they approach victims on the Internet, there are a number of common scams of which you should be aware. Here are a few examples of the types of schemes you should be on the lookout for when using social media:

"Pump-and-Dumps" and Market Manipulations

Beware of unsolicited callers or emails touting "secret" investments.

"Pump-and-dump" schemes involve the touting of a company's stock (typically small, so-called "microcap" companies) through false and misleading statements to the marketplace. These false claims could be made on social media such as Facebook and Twitter, as well as on bulletin boards and chat rooms. Pump-and-dump schemes often occur on the Internet where it is common to see messages posted that urge readers to buy a stock quickly or to sell before the price goes down, or a telemarketer will call using the same sort of pitch. Often the promoters will claim to have "inside" information about an impending development or to use an "infallible" combination of economic and stock market data to pick stocks. In reality, they may be company insiders or paid promoters who stand to gain by selling their shares after the stock price is "pumped" up by the buying frenzy they create. ***Once these fraudsters "dump" their shares and stop hyping the stock, the price typically falls, and investors lose their money.***

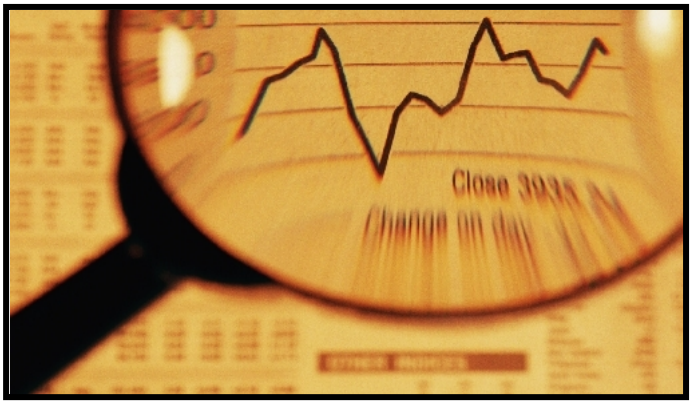
For an example of an actual case, see Securities and Exchange Commission v. Carol McKeown, Daniel F. Ryan, Meadow Vista Financial Corp.,and Downshire Capital, Inc., Civil Action No. 10-80748-CIV-COHN (S.D. Fla. June 23, 2010).

(Continued on p. 5)

(Continued from p. 4)

Fraud Using "Research Opinions," Online Investment Newsletters, and Spam Blasts

While legitimate online newsletters may contain useful information about investing, others are merely tools for fraud. Some companies pay online newsletters to "tout" or recommend their stocks. Touting isn't illegal as long as the newsletters disclose who paid them, how much they're getting paid, and the form of the payment, usually cash or stock. But fraudsters often lie about the payments they receive and their track records in recommending stocks. Fraudulent promoters may claim to offer independent, unbiased recommendations in newsletters when they stand to profit from convincing others to buy or sell certain stocks – often, but not always, penny stocks. **The fact that these so-called "newsletters" may be advertised on legitimate websites, including on the online financial pages of news organizations, does not mean that they are not fraudulent.** To learn more, read our tips for checking out newsletters.



Numbers Can Lie

Remember that research can be faked.

For an example of an actual case, see Securities and Exchange Commission v.Wall Street Capital Funding LLC, Philip Cardwell, Roy Campbell, and Aaron Hume, Civil Action No. 11-cv-20413-DLG (S.D. Fla. February 7, 2011).

High Yield Investment Programs

The Internet is awash in so-called "high-yield investment programs" or "HYIPs." These are unregistered investments typically run by unlicensed individuals – and they are often frauds. The hallmark of an HYIP scam is the promise of incredible returns at little or no risk to the investor. A HYIP website might promise annual (or even monthly, weekly, or daily!) returns of 30 or 40 percent – or more. Some of these scams may use the term "prime bank" program. ***If you are approached online to invest in one of these, you should exercise extreme caution - they are likely frauds.***

For an example of an actual case, see Securities and Exchange Commission v. David Tanner, individually and d/b/a Capital Enhancement Club, Rocky D. Spencer, Marroc Corp. and Richard P. Kringen, Defendants, and Margaret Spencer, Omnibus LLC,Vectra Resources LLC and Dynamic Environmental Solutions, Inc., Relief Defendants, Civil Action No. 05-4057-SAC, (United States District Court; District of Kansas; Topeka Division May 4, 2005).

(Continued on p. 6)

(Continued from p. 5)

Internet-Based Offerings

Offering frauds come in many different forms. Generally speaking, an offering fraud involves a security of some sort that is offered to the public, where the terms of the offer are materially misrepresented. The offerings, which can be made online, may make misrepresentations about the likelihood of a return. For example, in a recent case, Securities and Exchange Commission v. Imperia Invest IBC (listed below), the fraudsters allegedly used a website to offer investors a "guaranteed return" of 1.2% per day. Other online offerings may not be fraudulent *per se*, but may nonetheless fail to comply with the applicable registration provisions of the federal securities laws. While the federal securities laws require the registration of solicitations or "offerings," some offerings are exempt. ***Always determine if a securities offering is registered with the SEC or the North Carolina Securities Division, or is otherwise exempt from registration, before investing.***

For an example of an actual case, see Securities and Exchange Commission v. Imperia Invest IBC, Civil Action No. 2:10-cv-00986-B (D. Utah). See also In the Matter of Migliozzi and Flatow, SEC Rel. 9216 (June 8, 2011) (settled order).

Where can I go for help?

Investors who learn of investing opportunities from social media should always be on the lookout for fraud. If you have a question or concern about an investment, or you think you have encountered fraud, please contact the SEC, FINRA, or the North Carolina Securities Division (800-688-4507) to report the fraud and to get assistance.

U.S. Securities and Exchange Commission
Office of Investor Education and Advocacy 100 F Street, NE Washington, DC 20549-0213 Telephone: (800) 732-0330 Fax: (202) 772-9295

Financial Industry Regulatory Authority (FINRA)
FINRA Complaints and Tips 9509 Key West Avenue Rockville, MD 20850 Telephone: (301) 590-6500 Fax: (866) 397-3290

North Carolina Securities Division
PO Box 29626, Raleigh, NC 27626-0622 Telephone: (800) 688-4507 Fax: (919) 807-2183
For information about filing a complaint, click here.

Related Information

For additional educational information for investors generally, see the SEC's website for individual investors, Investor.gov. For additional information about securities fraud, see:

NASAA Informed Investor Advisory: Social Networking
Operation Broken Trust
Avoiding Fraud
Stopping Affinity Fraud in Your Community
FINRA Warns Investors of Social Media-Linked Ponzi Schemes, High-Yield Investment Programs

The following INVESTER ALERT was issued by the Financial Industry Regulatory Authority (FINRA) and is reprinted here for informational purposes.

Email Hack Attack? Be Sure to Notify Brokerage Firms and Other Financial Institutions

Anyone who has experienced an email account intrusion or "hacking" knows how frustrating it can be to deal with the aftermath—from telling friends in milder cases that you didn't send the flurry of bogus emails they received to regaining access to a blocked account. In the most serious cases, a compromised email account can lead not only to identity theft, but also to theft of your money. That's why one of the most important first steps you should take if your email account has been hacked is to notify your brokerage firm and other financial institutions.

FINRA has received an increasing number of reports involving investor funds being stolen by fraudsters who first gain access to the investor's email account and then email instructions to the firm to transfer money out of the brokerage account. In addition to issuing a Regulatory Notice to firms, we are issuing this Alert to warn investors about the potential financial consequences of a compromised email account and to provide tips for safeguarding your assets.

How Cons Use Compromised Email Accounts to Wire Money Out of Accounts

The Federal Bureau of Investigation (FBI), Financial Services Information Sharing and Analysis Center (FS-ISAC) and Internet Crime Complaint Center (I3C) recently issued a joint fraud alert describing a similar trend in which hacked email accounts are being used to facilitate wire transfers. These frauds tend to follow a typical pattern. For example, in some of the instances FINRA has seen, the perpetrators appear to have obtained the investor's brokerage information by accessing the investor's email account and searching contact lists or emails in the "sent" folder. The fraudster then typically sends an email to the investor's broker or brokerage firm (using the investor's personal email account) with instructions to wire funds to a third-party account, often overseas. The instructions may be accompanied or followed by a fraudulent letter of authorization, which also is emailed from the compromised email account.

In some instances, firms have released funds after unsuccessfully attempting to verify emailed instructions by phone. In at least one case, the fraudulent email stressed the urgency of the requested transfer, pressuring the brokerage firm to release the funds before verifying the authenticity of the emailed instructions. As the FBI/FS-ISAC/I3C alert notes, these fraudsters can be quite creative and persuasive with their excuses, fabricating tales of woe involving a death in the family or some grave illness that keeps the investor from contacting the firm via phone or whatever channels the investor ordinarily uses, while seeking the expedited transfer of assets.

(Continued on p. 8)

(Continued from p. 7)

How to Spot a Hack Job

Tell-tale signs that you've been the victim of an email account intrusion include reports of spam from people in your "contacts" folder or a slew of "bounced" email messages from people you don't know. You might find that your password or other account settings have been changed—or that your email provider has blocked you from accessing your account. For information on staying safe online, visit the Federal Trade Commission's Identity Theft and Data Security website as well as I3C at ic3.gov.

What to Do if Your Email Account Gets Hacked

If your email account gets hacked—or if for any reason you think that your personal financial information has been stolen—immediately contact your brokerage firm and other financial institutions, including credit card issuers, to notify them of the problem. You should also notify the credit bureaus to put a fraud alert on your file.

Check your brokerage account for unauthorized transactions—especially withdrawals or wire transfers to an account that is not yours—and ask the firm to investigate if you find any. It will take time to determine what happened, and the firm will likely need your help in identifying anyone who might have access to your account.

In the meantime, be sure to change your username, password and PIN for your financial accounts—and also change your password to your email account. For additional tips on staying safe online, read our alert, Keeping Your Account Secure: Tips for Protecting Your Financial Information. One of the best defenses against hacking is having a subscription to antivirus software that is installed, active and kept up to date.

If a Problem Occurs

If you believe you have been defrauded, please send us a written complaint. And if you suspect that someone you know has been taken in by a scam, be sure to give us that tip. Here's how:

Online:

File a complaint with FINRA or File a complaint with the NC Securities Division (for you)
Send a Tip (for others)

Mail or Fax:

FINRA Complaints and Tips
9509 Key West Avenue
Rockville, MD 20850
Fax: (866) 397-3290

Additional Resources

- FINRA Regulatory Notice 12-05, Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts
- FINRA and SIFMA Investor Alert, Keeping Your Account Secure: Tips for Protecting Your Financial Information
- FINRA Investor Alert, "Phishing" and Other Online Identity Theft Scams: Don't Take the Bait

Calendar of Upcoming Events

A representative from the Securities Division will be giving an anti-fraud presentation on the following dates and locations. Dates and times are subject to cancellation (although cancellations are rare), so please call the contact number listed to confirm the event is still on before leaving for it. All presentations are free and open to the public unless otherwise indicated. If you would like to schedule a speaker for your church, business, group or organization, please contact John Maron or Barbara Bennett at (800) 688-4507.

Date	City	Details
02/07/12	Asheville	Asheville Civitan, Trinity Episcopal Church, 60 Church Street. Time: Noon – 1:00 PM. Open to Civitan members and their guests. For more information, contact Norma Messer at (828) 253-2392, X100.
02/07/12	Asheville	Deerfield Episcopal Retirement Community, 1617 Hendersonville Road. Time: 2:30 PM – 3:30 PM. Open to Deerfield residents and their guests. For more information, contact Betsy Cantrell at (828) 505-8381.
02/16/12	Pinehurst	NC Bar Association's 2012 Business Law Institute CLE, Pinehurst Resort, 80 Carolina Vista Drive. Time: 12:55 PM – 5:00 PM. Registration required. For more information, follow the link above.
02/21/12	Currituck	Currituck County Senior Center, 2793 Caratoke Hwy. Time: 1:00 PM -- 3:30 PM. For more information, contact Debora Sheard at (252) 426-5753, X-225.
02/21/12	Smithfield	Kiwanis Club of Smithfield, Becky's Log Cabin Restaurant, 2491 Hwy. 70. Time: 6:30 PM -- 7:30 PM. Open to Kiwanis members and guests only. For more information, contact Paul Dorman at (919) 390-4691.
02/22/12	New River	Anti-fraud presentation, New River Marine Corps Air Station. Time: 1:00 PM – 2:00 PM. Open to servicepersonnel and their families only. For more information, contact Marilyn Nakamura at (910) 449-5259.
02/23/12	Raleigh	"Basics of Saving & Investing" presentation for teachers, Atlantic Coast Business Marketing, & IT Education Conference, Hilton Hotel, 3415 Wake Forest Rd. Time: 10:15 AM – 11:05 AM. For more information, click the link above.
02/29/12	Winston-Salem	Elder Investment Fraud and Financial Exploitation (EIFFE) Prevention Program, Forsyth County Department of Social Services, 741 North Highland Avenue. Time TBD. For more information, contact LeShana Baldwin at (919) 733-3818.
03/06/12	Durham	Little River Senior Center, Little River Community Complex, 8305 Roxboro Road. Time: 10:30 AM -- 11:30 AM. For more information, contact Corrie Smith at (919) 477-6066.
03/07/12	Rural Hall	The Living Well Center for Lifelong Learning, 7105 Broad Street. Time: 1:00 PM -- 3:30 PM. For more information, contact Barbara Benge (336) 408-3954.
03/13/12	Dunn	Scam Jam, Dunn Enrichment Center, 610 East Johnson Street. Time: 8:30 AM – Noon. For more information, contact (910) 892-3807.
03/13/12	Raleigh	Whitaker Mill Senior Center, 401 E. Whitaker Mill Road. Time: 9:15 AM -- 10:15 AM. For more information, contact the Center at (919) 856-6444.
03/14/12	Salisbury	Scam Jam, Oak Park Retirement Community, 548 White Oaks Drive. Time: 1:45 PM – 4:00 PM. For more information, contact Martha Smith at (540) 520-8345.
03/20/12	Louisburg	Louisburg Senior Center, 127 Shannon Village. Time: 10:00 AM – 11:00 AM. For more information, contact Debbie Conner at (919) 496-1131.

On The Docket

The following cases are ones in which the Securities Division has had some involvement, either as the lead investigative agency or in a supporting role.

Sean Fitzgerald Mescall, of Denver, NC, was arrested by law enforcement agents of the Securities Division on September 9, 2009, on charges of securities fraud, obtaining property by false pretense and conducting an unlawful telephone room. He is alleged to have defrauded approximately 69 victims of approximately $1.3 million in a Ponzi scheme involving foreign currency trading since at least September 2006. In a separate action, the CFTC has filed a civil action against Mescall and Capital Street Financial. On May 25, 2010, US District Court Judge Robert Conrad, Jr., ruled Mescall to be in contempt of the Court's Sept. 2009 Preliminary Injunction. On May 4, 2011, he was sentenced to 27 months in federal prison for criminal contempt relating to the CFTC action.

Walter Ray Reinhardt, of Durham, NC, was served with 62 felony arrest warrants for securities violations on November 17, 2010. He is alleged to have defrauded 16 victims in Durham County out of more than $1 million. Reinhardt had his first appearance in Durham County District Court on November 18, 2010 on 38 felony counts of securities fraud, 12 felony counts of common law forgery, and 12 felony counts of common law uttering. He is currently being held in the Durham County Jail under a $4 million bond. No trial date has been set.

Darren Joseph Capote, of Patterson, NY, was indicted on July 11, 2011, in Ashe County Superior Court on three Class C felony counts of securities fraud. He is alleged to have defrauded an elderly victim in Ashe County. He was released from custody on a $100,000 secured bond. His next court appearance in Ashe County is expected in March 2012.

.

Recent Enforcement Actions

(For prior administrative and criminal actions, click on the badge to the right.)

News from the Regulators

(The following are selected public notices issued by one or more securities regulator. Click the links to view the full notices. These are offered for informational purposes only.)

SEC Seeks Public Comment for Financial Literacy Study Mandated By Dodd-Frank Act

Jan. 18, 2012 **–** The Securities and Exchange Commission has published on its website a request for public comment on financial literacy and investor disclosure issues that it is studying as part of a review mandated by the Dodd-Frank Wall Street Reform and Consumer Protection Act. Section 917 of the Dodd-Frank Act directs the SEC to conduct a study of retail investors' financial literacy and submit its findings to Congress by July 21, 2012. The SEC is using qualitative and quantitative research, including investor testing, to help inform the study. To supplement its research, the SEC also is seeking public comment on financial literacy and investor disclosure issues. The public comment period will remain open for 60 days, following publication of the request in the Federal Register.

CFTC Chairman Names Vincente Martinez as Director of Recently Opened Whistleblower Office

Jan. 6, 2012 -- Commodity Futures Trading Commission (CFTC) Chairman Gary Gensler announced that Vincente Martinez has been hired as the first director of the CFTC's recently opened Whistleblower Office. Additional information about the Whistleblower Office can be found here.

All investors are strongly encouraged to contact the Securities Division at (919) 733-3924 or toll-free at (800) 688-4507 to check that their investment professional is properly registered ***before*** transferring any assets to that person's control. One five-minute telephone call to the Securities Division could protect your entire life's savings from being stolen from you. For a wealth of investor education information, please visit our Web site, www.sosnc.com. Click on the yellow box entitled "Investment Securities".

This newsletter is produced by the Investor Education Program of the Securities Division of the North Carolina Department of the Secretary of State. If you have questions or comments about this publication, or would like to schedule an investor education presentation with your group or organization, please email John Maron, Director of the Investor Education Program, or call (919) 807-2106.

Please help us publicize the educational information in this mailing by forwarding it to your contacts around the state. If you no longer wish to receive mailings from the Securities Division, please send an email to: jmaron@sosnc.com with "Remove from mailing list" in the subject line.

Remember that if an investment sounds too good to be true, it *probably* is!