COMPLIANCE
ADVISOR
PROFESSIONALS, LLC

Phone: (508) 828-1410
Email: info@complianceadv.com

We recommend sending information security reminders to clients at least once a year. Here is a sample:

The Security of your Personal Information is Important to Us

In an ongoing effort to keep our clients informed and aware of identity protection measures and cybersecurity guidelines, we are providing this circular as a helpful reminder of the following information to help you keep your information secure.

We will *NEVER*:

- ✓ Ask for Social Security Number (SSN) or other personally identifiable information via email
- ✓ Ask for login credentials or passwords
- ✓ Send you email from an address other than [INSERT EMAIL]
- ✓ Accept trade instructions or fund transfer requests by email or voicemail – these must be verbally confirmed EVERY TIME
- ✓ Ask for payment or account details via email (unless through encrypted service or eSignature form)
- ✓ Send you an email requesting that you "verify" any personal information (unless through encrypted service or eSignature form)
  - *If a message contains a hyperlink to another website, the purpose for the website will be included in the body of the email and you will **NEVER** be redirected to a site that asks you to verify any personal information*

Use the Tools You Have to Protect Your Identity and Accounts

- ✓ Monitor your accounts online; be aware of your balances and holdings
- ✓ Be alert to "phishing" scams which seek to gain access to your personal information
- ✓ Protect your login IDs and passwords; use a combination of letters, numbers and special characters for your passwords and change them at least every 90 days; do not carry them on you/in your wallet
- ✓ Do not give your SSN or other personal information about yourself to anyone you do not know
- ✓ Order copies of your credit report once a year to ensure accuracy
- ✓ Choose to do business with companies you know are reputable, particularly online
- ✓ When conducting business online, make sure it is a secure transaction (look for **HTTPS** in the address)
- ✓ When using social media sites, NEVER publish personal information including telephone numbers, Social Security number, date of birth, email addresses, physical address, mother's maiden name or other information that may be sensitive information to fraudsters or hints to passwords
- ✓ Do not open email from unknown sources and use virus detection software

What to Do if You Believe You are a Victim of Fraud

- ✓ Contact us immediately if you know or suspect your identity has been stolen or your account has been compromised; the phone number for our office is [(XXX) XXX-XXXX]
- ✓ File a police report and contact the three major credit reporting companies; the fraud unit numbers are:

  Transunion – (800) 680-7289
  Experian – (888) 397-3742
  Equifax – (800) 525-6285

- ✓ Keep records of your communications with authorities, including names, contact numbers and dates and times of the calls

PLEASE SEE THE REVERSE FOR INFORMATION ON "PHISHING" – THE MOST COMMON METHODS BY WHICH FRAUDSTERS SEEK TO GAIN ACCESS TO YOUR PERSONAL INFORMATION

How Not to Get Hooked by a "Phishing" Scam

Phishing is a high-tech scam that uses spam emails or pop-up messages to deceive you into disclosing investment account numbers, bank account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop-up message that claims to be from a business or organization with which you already do business, such as your Internet Service Provider, investment adviser, bank, online payment service, or even a government agency. The message typically states that you must "update" or "validate" your account information, and it may additionally allude to dire consequences in the event you fail to respond (i.e., the closure or suspension of your account). The message then redirects you to a fraudulent website designed to look like a legitimate site for the organization; however, it is not. The purpose of the fraudulent site is to trick you into divulging your personal information so the operators can steal your identity, run up bills or commit crimes in your name.

The FTC, the nation's consumer protection agency, suggests these tips to help you avoid getting hooked by a phishing scam:

- ✓ If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct website address. NEVER cut and paste the link in the message.
- ✓ Do NOT email personal or financial information. Email is NOT a secure method of transmitting personal information. Protect your personal information at all costs and only divulge in person or by phone to an individual known or verified by you.
- ✓ Review credit card and bank account statements routinely to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- ✓ Use anti-virus and anti-malware software and keep your programs up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Antivirus software and a firewall can protect you from inadvertently accepting such unwanted files. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It is especially important to run a firewall if you have a broadband connection. Always install routine updates to ensure your software is current to evolving schemes.
- ✓ Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.
- ✓ Report suspicious activity to the FTC. If you receive an email phishing for information, forward it to www.ftccomplaintassistant.gov. If you believe you have been scammed, file a complaint at www.ftc.gov, and then visit the FTC's Identity Theft website at www.ftc.gov/idtheft to learn how to minimize your risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam. The FTC works on behalf of the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, (877)-FTC-HELP ((877)-382-4357); TTY: (866)-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.