Stonnington Group

PROTECT YOUR ON-LINE SAFETY

We at Stonnington Group want to take this opportunity to remind our customers of the importance of protecting their personal information, particularly online and keeping their financial accounts secure.

The Problem:

Over the last two years alone, financial regulators have seen a fivefold increase in email related "cyber fraud". It's no longer the "emails from Nigeria" scams. The biggest increase in cyber fraud cases involve instances where hackers illegally gain access to a customer's email account. They then send an urgent email to the financial advisor using that client's email address, requesting that the advisor wire funds from their account to another account. The other account is controlled by the perpetrator and to better avoid detection, sometimes the account may even have the same last name as the client's. Another problem is related to clients storing signed pieces of paper as attachments in their email account which allows fraudsters to forge their signatures once they've compromised the client's email account.

Stonnington's Safeguard:

As part of increased security, we have adopted new procedures to respond to customer requests for the transfer/withdrawal of cash and securities.

If you send an email request to Stonnington to transfer/withdraw cash or securities to a "new" or previously unknown account, payee or address, Stonnington may contact you by phone to verify the instructions prior to entering the order. The clearing firm will also continue to require your Letter of Authorization. Signatures may also be compared against legitimately signed client documents to try and detect any instances of forgery.

Additional Safety Steps You Can Take:

- Notify Stonnington immediately if your email account has been compromised.
- Be sure Stonnington has your current contact information, including your mailing address and email address.

Member FINRA/SIPC
21031 Ventura Boulevard, Suite 1201
Woodland Hills, CA 91364
T: (818) 444-0600 F: (213) 955-4983
www.stonningtongroup.com

Stonnington Group

- Do not use your email address as your login for access to your online banking or investment account websites; consider creating a user ID instead to login to a financial institution's websites.
- Read your statements promptly to make sure all transactions shown are ones that you actually made.
- Think twice before you respond to emails requesting personal information.
- Use extra caution with wireless connections.
- Monitor your credit report. Free annual copies are available at www.annualcreditreport.com.

For More Information & Additional Resources:

- Identity Theft – http://www.finra.org/Investors/ProtectYourself/P037885
- Phishing Scams – http://onguardonline.gov; www.sec.gov/investor/pubs/phishing.htm

Questions:

If you have any concerns or questions you would like to discuss with us, please give us a call at (818) 444-0600.