Preventing Wire Fraud

Cases of wire fraud -- fraudulent transfers of money using phone, fax, or computer -- have **risen more than tenfold** over the past decade. Most fraud attempts reported by advisors involve client email takeovers. It is important to us that you not be the victim of wire fraud.

To protect your privacy and security, **we do these things**:

1) If we receive an emailed or faxed request to transfer funds from your account, we call to confirm that the request came from you. We call you as soon as possible after receiving the request. If we cannot reach you, the transfer will be delayed until we speak with you.
2) We always call you at the phone number of record for your account. We cannot determine which other phone numbers are yours, so we only accept confirmation at that number.

What can you do to protect yourself?

1) Guard your personal information. If you suspect that your identity might have been compromised, contact your advisor immediately.
2) Check your financial accounts each month. If you see activity you do not recognize, speak immediately with the advisor, bank, or custodian.

What about email fraud?

1) Be wary of emails that ask for personal information, passwords, or account numbers. Fraudulent emails often appear to be legitimate. Check the sender's address.
2) Fraudulent emails often contain incorrect spelling, bad grammar, or phrasing that is not typical of your advisor or bank. In this case, verify its source with the sender over the phone.
3) **If your email account has been "hacked"** and the hacker is able to send email from the account:
    a. Change your account password and consider changing your email address. Your email and financial account passwords should not be used for any other account; if you use the hacked account's password elsewhere, change those passwords.
    b. Contact all financial institutions with which you do business (including credit issuers) and inform them of the hacking. Change those passwords as well.
    c. Run a scan on all of your computers for malware and viruses.
    d. Notify your email contacts that your account has been compromised and that they should not click on links coming from that email address until further notice.

    If you have experienced fraudulent attempts (successful or not, in addition to the above):

    e. Restrict outbound money movement until the situation is completely resolved.
    f. Place a fraud alert on your social security number, bank and credit card accounts, and credit bureau accounts.
    g. Contact your advisory team for additional information on dealing with identity fraud.