

## Protecting Your Financial Identity

*"Just because you're paranoid, it doesn't mean they're NOT out to get you!"*

### Three Attempts in Three Weeks

We do not tend to be alarmist in our outlook on the markets, the economy or world events in general. However, in just the past few weeks, three of our clients have had their personal e-mail accounts hacked by scammers who then sought to misappropriate funds from their accounts. Fortunately we were able to thwart those attempts, but financial institutions report that such scams have become quite common, and that's a scary prospect!

This past October we hosted an Educational Workshop entitled **"Protecting Yourself Against Identity Theft"** at the Mountaineers' facility at Seattle's Magnusson Park. We outlined ways our clients could minimize the chances of being victimized by identity theft or fraud. Many attendees brought paper documents to be shredded by a truck we had onsite, and we discussed how long various types of investment, bank, and tax records should be retained.

Our IT consultant, Grant Eckstrom of BEIT Consulting, gave a detailed presentation on a variety of related threats we all should be mindful of. We also shared information about LifeLock Solutions, an insurance program and identity theft prevention service that can be accessed by our clients at a discounted rate.

Of course we had no idea how quickly these kinds of concerns would play out with our own clients!

### Access: Hacking Personal Email

Here's what we can tell you about the fraud attempts mentioned above. First, the would-be thieves hacked into the personal email accounts of each client to gain access to the string of personal emails. These were 'Gmail' or 'AOL' accounts, so it's clear that these widely used services are not impervious to such efforts. The weak link may be an overly simple or obvious password. Or, as Grant Eckstrom noted last October, hackers may be attacking smartphones to get access to email accounts, because the security protocols are not as robust as internet and computer networks where people are more likely to have firewalls, spam, and malware protections in place.

With access to your e-mail account, a hacker can review your messages for information on the financial institutions and service providers you deal with – including your advisory relationship with our office and the individuals who assist you. It's easy then to craft a message that would appear to be from you, requesting more detailed information on your accounts or funds to be wired to a third party to "settle" an investment opportunity, usually with some story as to why the need is urgent.

We believe these attempts originate from non-U.S. locations due to somewhat awkward wording, misspellings, etc. We also got a consistent negative response from each when we asked them to call in to confirm this request and to discuss the reasons for such urgency.

These attempts may strike you as relatively amateurish, but we take them very seriously. And both our broker/dealer (KMS Financial Services, Inc.) and custodian (Pershing) have long maintained special verification procedures around any "third-party" wire requests.



## Advisors are Good Targets

It is actually rather clever to target the clients of financial advisors given our desire to be as responsive as possible to an apparent special request from a client. That desire makes us a potential weak link in the eyes of those who would exploit any vulnerability. As noted above, this type of activity has been increasingly common across our industry the past couple of years.

On the other hand, we haven't received any requests from Nigerian princes or princesses to rescue them from a fate worse than death.

## How We Respond

Of course, we reached out to our clients to let them know their email accounts had been hacked and to take this attempt to defraud VERY seriously! We urged them to contact any other financial institutions they deal with to alert them to this threat and make sure no funds would be transferred without proper documentation and a confirmation call. And we warned them to immediately change their e-mail passwords and set up a system to rotate them regularly. Beefing up your password security – i.e., more complex passwords changed with some regularity – is probably the single most critical measure you can take.

## Additional Steps to Protect Yourself

Here are some steps you can take to further reduce the chance of becoming a victim of identity fraud – steps our staff already takes to protect your information.

- Beef up the security of email passwords (make them longer, more complex) and change them periodically
- Delete old emails and limit the number of contacts in your Outlook or other email programs

- Avoid revealing in emails where accounts are held, account numbers, social security numbers, etc.
- Place a CALL, or request a CALL, to direct any actual transaction
- If someone calls or emails SEEKING information, be circumspect about providing it without verification of who they are.
- Expect increasingly tighter security and verification procedures in ordering out funds.

## Consider Hiring a Service like LifeLock Identity Theft Protection Solutions

According to a Javelin Strategy & Research study, one in twenty consumers learned they were the victims of identity fraud in 2012. Have you received replacement credit cards recently because there was a breach of security at a bank?

Large companies (Barnes & Noble, Zappos, livingsocial, Sony PlayStation Network, LinkedIn, and Yahoo, to name a few) have been hacked, exposing millions of records of their customers information including names, email addresses, dates of birth, billing and shipping addresses, phone numbers and last four digits of credit cards.

LifeLock Solutions will proactively scan and monitor for threats to your financial identity, respond to identity thefts when they occur, and provide you with assistance in unwinding any instances of identity theft or fraud.

Many victims of identity theft are staggered by the sheer amount of time it takes to follow up and resolve disputes that arise from identity fraud. LifeLock Solutions provides you with up to \$1 Million to hire experts to help your recovery after an event. Coverage starts for as little as \$9/month, which is a discounted rate for Opus 111 Group clients. If you are interested in this program, you can enroll at: <http://opus111group.excelsiorenroll.com>

