ASPIRIANT

Insight

June 2013

Wealth Management Commentary

Achieve more.

Covering your assets

Protecting yourself from financial fraud ... and that pesky Nigerian prince

John Lund / Sam Diephuis / Blend Images / Getty Images

Identity theft and identity fraud have become one of the fastest growing and most pervasive crimes in the United States. During 2012, approximately 15 million individuals in the US had their identities used fraudulently, resulting in financial losses exceeding $50 billion. And the threat is ever-increasing as the methods thieves use to obtain personal information grow more and more sophisticated.

Traditionally, petty thieves accessed personal information by stealing a wallet or mail or by "dumpster diving." Today, identity theft is increasingly driven by organized crime using sophisticated techniques such as "skimming" (stealing credit card numbers by using illegally installed readers on credit card processing machines), hacking into corporate databases, and "phishing" email scams.

An ounce of prevention

Identity fraud is often narrow in scope. Many readers of this article have probably received "the call" from their credit card company (usually at the most inopportune time) alerting them to a $2,500 purchase at a Wal-Mart 3,000 miles from home. Fortunately, due to federal credit laws, most of these situations result in some hassle but no out-of-pocket cost to the victim. More sophisticated identity theft, however, can result in large financial losses, damage to one's credit rating, and many hours (and lawyers' fees) spent recovering.

While no one can control all of their financial information (e.g., information stored in corporate or government databases), there are many simple steps you can take to limit access to personal information, thus reducing the chance of having sensitive information stolen and misused.

- **Think outside the (mail) box.** Sign up for electronic delivery of utility and credit card bills and statements from financial institutions. Install a mailbox with a lock. Have the post office hold your mail or have a friend or family member pick it up when traveling.
- **Free credit.** Obtain your credit report periodically from the three major credit reporting agencies at www.annualcreditreport.com, and review for unfamiliar accounts. You can obtain one free credit report from each agency every 12 months.
- **No extra credit.** Ask your credit card companies to stop sending credit pre-approval offers, and stop all unrequested credit card solicitations by registering at www.optoutprescreen.com.
- **Just shred it.** Shred statements and receipts that contain your personal information…tearing them up and putting them into the recycling bin isn't good enough!
- **Hire a pro.** Not surprisingly, a cottage industry has sprung up around protecting people's identity. Identity theft protection services will monitor your credit reports, scour data sharing websites for your personal information, and assist with remediating any credit damage. There is some debate about the value of this as a preventative measure, but it's available at a nominal cost to those who want the extra layer of monitoring. LifeLock® is perhaps the most well known service, but there are many similar offerings, including some from the credit bureaus Equifax and Experian.
- **Leave it at home and lock it down.** Leave your Social Security card and unused credit cards at home rather than in your wallet. It's a good idea to lock these up (along with your passport, birth certificate and other sensitive information) because sophisticated thieves (and sometimes housekeepers or contractors) look for these items to sell on the black market.

Get online without putting your money on-the-line

In recent years, the internet has become a fruitful and low-risk place for criminals to obtain personal information by exploiting weaknesses in corporate, government and individual computer security, and through a variety of scams directed at tricking people into revealing personal data. The pervasiveness of social media and mobile computing has opened up many more opportunities than existed even five years ago, and criminals are becoming increasingly sophisticated and effective.

Identity theft and **identity fraud** are terms used to encompass crimes in which someone wrongfully obtains key pieces of another person's personal identifying information, such as Social Security number, driver's license, or bank or credit card account information, and uses the information for their financial gain.

"**Phishing**" is the practice of attempting to fraudulently gather private financial information via email. The criminal creates an email that looks like a legitimate email from a financial institution (e.g., using the company's logo and color scheme) and sends it to millions of email addresses, hoping to snare a few unsuspecting victims.

- **PC security.** The first step to protecting yourself online is to make sure that all of your home computer operating systems are up to date with the latest patches, protected with strong passwords and are running anti-virus and anti-malware software with current update subscriptions. Your computers should be connected to the internet through a firewall router. Increasingly, thieves are hijacking computers or email accounts and sending email to banks and investment advisors requesting wire transfers to third-party accounts. (Yes, we at Aspiriant have received such emails!)
- **Bad phish.** The typical phishing email will prompt the recipient to click on a link and enter personal information (usually account numbers and passwords) on what appears to be a login page. It is a good practice

to hover the cursor over the link (without clicking on the link!) to reveal the actual website address. An unknown address is a clear telltale of a fraudulent email. Legitimate financial services companies (such as Aspiriant, Charles Schwab, Fidelity, TD Ameritrade, and all commercial and private banks) will never send you an email asking you to click on a link to "verify" your account information or install any applications. These emails are always fraudulent and should be deleted immediately without clicking on any links, opening attachments, or responding to the sender.

Phishing emails could also come from "friends" or "family members" whose computers have been hacked. If in doubt, don't click on any attachments or links, as they might install malicious software onto your computer.

- **Buyer beware.** Only submit your personal information to reputable online merchants, who will have secure websites (denoted by https://) for making purchases.
- **Constrained mobility.** With a mobile hotspot on every corner, accessing information has never been easier…the same goes for thieves trying to access *your* information. Moreover, people are increasingly replacing the functions of their home computer (hopefully hidden behind a firewall and private network) with their less-protected phones and tablets. Mobile devices are subject to the same risks as PCs, so it's wise to take the same precautions – use a strong password, install anti-virus software (especially on Android and other open-platform devices), and avoid connecting to unsecured public networks. Don't download mobile apps outside of established app stores and reputable vendors, as they often contain malware designed to hack into your mobile device and obtain access to your email, logins and passwords.
- **Living (a little less) social.** Many people routinely share personal information such as birth dates, addresses, telephone numbers and the innocuous pet name (a favorite for passwords) on Facebook and other social media. While you may limit access to your social media sites to only your friends, thieves who've gained access to your friends' computers can quickly assemble sensitive information about you.

Playing our part

Consumers are not the only ones targeted for financial fraud. Increasingly, criminals are directly targeting financial institutions. Charles Schwab reports a fourfold increase in fraudulent wire requests over the last year! Schwab and other investment custodians have a series of verification processes, including signature matching and verification phone calls, to catch these fraudulent requests.

Beware of the Nigerian Prince!

Many readers have, at one time or another, been offered a share of the fortune of an unfortunate Nigerian prince who has millions of dollars in gold locked away, and who needs a mere $10,000 from you to help him claim it. Contrary to popular belief, this scam didn't arise along with the internet; rather, it's a modern variation on the Spanish Prisoner scam, which dates back to the late 19th century. In that scam, the perpetrator contacted businessmen, claiming to have a wealthy friend in a Spanish jail. He just needed a little money to bribe the guards to release his friend at which time, of course, the grateful friend would repay the businessman's generosity in spades.

Of course, in those days the perpetrator had to write letters and send them via regular mail, so the cost was considerably higher than now. Yet enough people fell for it to make it worthwhile…some things never change!

Aspiriant, too, has received a number of email requests from "clients" (usually overseas and in need of funds right away) whose email accounts were hacked. To combat this, we've recently enhanced our wire verification processes to require verbal verification of any third party wire transfers. Although this can at times be a little cumbersome, it can mean the difference between becoming the victim of financial identify theft and not.

Of course, part of our job requires sharing sensitive information (e.g., investment account data) with tax preparers and attorneys and, of course, with you. We take care to send anything with account numbers or Social Security numbers

via encrypted email. This practice complies with the most restrictive state laws that apply to financial institutions for emailing sensitive data. We encourage clients, and their other advisors, to use Aspiriant's secure email system for sending information securely to us as well.

Despite the best laid plans…

Short of living "off the grid," it's virtually impossible to completely secure your personal information. The steps above will dramatically reduce your risk, in part because the presence of a secure firewall or locked mailbox is enough to cause many thieves to simply move on to the next potential victim. Inevitably, though, virtually everyone will experience some form of financial fraud at some point. When that happens, immediately alert the affected financial institutions and file a police report to limit further damage; after that, call Aspiriant so we can help you think though additional steps to take…depending on the nature of the fraud, this could include possibly placing fraud alerts on your credit reports and opening new credit and brokerage accounts.

Hopefully, with the simple practices outlined here, that will be a call you never need to make.

Alec Manoukian
Director - Information Technology

Ginny King, JD
Director - Wealth Management, Principal