Tips to Help Protect Yourself From Identity Theft
Stephen Younger

While it’s certainly not a new problem, identity theft is a growing concern in the financial services community. The steadily increasing frequency of alerts from regulators is only one indication of just how widespread this problem has become. We take every reasonable effort to secure and protect personal and financial information, and I would encourage you to proactively do the same.

Recent data breaches at large, national retailers have made it pretty clear that sometimes, no matter how carefully you guard it personally, your financial information can be compromised. These security breaches – in addition to the ever increasing number of email scams, website hacks and incidents of wire fraud – mean a growing number ways for an identity thief to obtain your financial information.

My intent is not to alarm you. Rather, it’s to make you aware of how prevalent identity theft is, and the steps you can take to protect yourself.

PART I: Understanding Identity Theft – The Statistics

Each year, the Bureau of Justice Statistics (BJS) compiles data gathered from the victims of identity theft and publishes a report detailing their findings. In their most recent annual report, the agency found that “an estimated 16.6 million people, representing 7 percent of all persons age 16 or older in the United States, experienced at least one incident of identity theft in 2012.” Whether or not that statistic shocks you, the simple truth is that anyone can be affected. The odds are very good that if you haven’t been the victim of identity theft, you know someone who has.

Unfortunately, most victims are unaware that their identity has been stolen until long after the damage has been done. Contrary to their portrayal in movies and on television, thieves don’t often use stolen identities to adopt a normal daily existence while living long-term under an assumed name in some far-away country. Most stolen information is used to access established financial accounts, drain the victim’s saving and checking accounts, and run up the balances on their credit cards. Sadly, the BJS report indicates that, where the theft involved an existing account or credit card, the majority of victims (60.5 percent) were notified by their financial institution or some other company, often through a bill collector or an adverse credit event, versus discovering the theft on their own (39.3 percent).

One thing the entertainment industry often gets right, however, is the relative “facelessness” of identity thieves. Among victims surveyed, 32 percent believed they knew how their personal information was obtained, although 91 percent did not know anything about the identity of the offender.
Data Source: Bureau of Justice Statistics (BJS) “National Crime Victimization Survey, Identity Theft Supplement, 2012” Appendix Table 3. Sorted by notification source and percentage. Notification by “another way” includes: “Victim noticed suspicious phishing activity, hacked computer, account information missing or stolen, or discovered the theft by accident.”

The impact of identity-theft related fraud varies widely. Victims have reported numerous corollary financial repercussions, including: higher interest rates, adverse credit actions, loss of basic utilities and even criminal proceedings. The direct financial impact is substantial as well, with 66 percent of victims experiencing direct financial losses as a result of the theft and 14 percent of victims experiencing out-of-pocket (not reimbursed) losses. In 2012, losses attributed to identity theft were nearly $24.7 billion, more than $10 billion greater than the combined total for burglary, motor vehicle theft and household theft.

Victims are often surprised at how little of their personal information may be required for a thief to get away with their savings. Many wire frauds, for example, are perpetrated by individuals who gain access to a victim’s email account and search through old correspondence for a banking or investment contact. This contact’s desire to provide speedy service can be exploited by a thief who may not know, at the start of the exchange, whether or not an account even exists. In an effort to combat this common form of theft, your advisor or custodian will likely have implemented recent changes to their procedures, which require additional steps to verify your identity before sending funds on your behalf.

Identity theft also has a non-financial impact, which is much harder to measure. While the severity of emotional distress reported by identity theft victims overall was much lower than that reported by victims of violent crime, victims of personal information fraud in particular described the crime as “severely distressing” more frequently than any other type of crime victim surveyed.
PART II: Protecting Personal Information

As startling as the statistics are, they don’t change the simple fact that we live in a world where nearly every modern convenience comes at the cost of a certain amount of privacy. From the rewards card at the local grocery store – which tracks our purchases – to the typical social media profile – which contains the names and birthdates of our closest friends and relatives – our personal information is a commodity that many people freely share without considering the potential risk. So, without going to the opposite extreme and retreating to a cave, how do you protect your personal information? Some of my suggestions are below:

**Suggestion 1: Buy a safe and a shredder.**

This seems pretty basic in this high-tech era, and most of us know better than to leave our extra checkbook in the glove box of the car or to throw credit card statements in the trash. But we’re all busy and fraudsters know it. Ensuring that your financial information is safe and secure takes a little extra time, but it’s well worth it. The average identity theft is perpetrated by an individual taking advantage of a victim who overlooks basic precautions.

**Suggestion 2: Secure your digital information.**

During the last few months, I have received several calls from friends who were contacted by a rather persistent “technology consultant” informing them that “their computer had an error.” This “technology consultant” said that he could fix the error for a “small fee” and a few minutes of direct access to their hard drive. Most knew better than to allow the scammer access, but some didn’t. A few minutes are all that’s required to compromise your computer and all the data stored there. In the technology community, Scott Culp’s 2000 essay, “The 10 Immutable Laws of Security,” has long been considered a standard for best practices to keep digital information secure. His advice includes:

- If a bad guy can persuade you to run his program on your computer, it’s not your computer any more.
- Weak passwords trump strong security.
- An out-of-date virus scanner is only marginally better than no virus scanner at all.
- Technology is not a panacea.

Computers have changed a lot since Culp’s piece was originally written, but I still strongly recommend that you read his essay and consider his advice.

**Suggestion 3: Be your own advocate.**

When it was announced several years ago that the three nationwide credit reporting agencies (CRAs) would provide free credit reports on an annual basis, people flocked to annualcreditreport.com, a federally authorized website, to obtain their copies. Since then, many haven’t been back. According to statistics provided by the Federal Trade Commission (FTC) in their 2013 report to Congress:
One in four consumers identified errors on their credit reports that might affect their credit scores.
One in five consumers had an error that was corrected by a CRA, after it was disputed, on at least one of their three credit reports.
Four out of five consumers who filed disputes experienced some modification to their credit report.
Slightly more than one in 10 consumers saw a change in their credit score after the CRAs modified errors on their credit report.

As these figures illustrate, regularly checking your reports and working with these agencies to correct discrepancies can be extremely beneficial to your financial health. I would suggest placing a reminder on your calendar to check one report every four months. This allows you to monitor throughout the year.

**Suggestion 4: Hang up or hit delete.**

When’s the last time you received a call or email from someone with an urgent request for your financial information? What did you do? A quick query to my email client informs me that I have received several hundred requests of this type already this year. Thanks to aggressive filtering, most never made it to my inbox, but some still did. Some important things to keep in mind:

- Reputable banks, financial advisors and especially the IRS will not email or call you and solicit personal information as a means of verifying your identity.
- Never share your banking, credit card account or Social Security numbers with anyone unless you are certain that their request is legitimate.
- If the offer sounds too good to be true, it probably is.
- Be wary of online surveys or forms which request personal or financial information.

While the possibility does exist that the email supposedly from your old college roommate, where he laments his lost passport and requests that you wire him funds so he can get home, is indeed legitimate, ask yourself if it’s probable (or even likely) before heading to the bank.

**PART III: Respond Quickly.**

As the old saying goes, an ounce of prevention is worth a pound of cure. But what if, despite your best efforts, you find yourself the victim of identity theft or consumer fraud? The best advice I could offer at a time like that is: “Don’t panic.” Keep a level head and follow the advice given you by those in the banking and law enforcement communities. I recommend the following steps to deter the thieves and begin repairing any damage they may have caused:

1. File a report of the theft with your local police department and a complaint with the Federal Trade Commission (877-438-4338).
2. Notify your credit card companies and banks.
3. Contact the three major credit bureaus (Equifax: 800-525-6285, Experian: 888-397-3742, Transunion: 800-680-7289) to report the theft. Request your credit report and an “extended fraud alert.”
4. Contact the IRS at 800-908-4490. They have their own Identity Theft Affidavit and will assist you with applying for an Identity Protection Personal Identification Number if they determine that your tax files need additional protection.

5. If you have information about the identity thief, you can also file an online complaint with the Internet Crime Complaint Center (IC3). Analysts at IC3 review all complaints and forward them to one or more of the law enforcement or regulatory agencies that have jurisdiction over the matter.

The FTC publication “Taking Charge” has a great amount of detailed information and helpful checklists to assist you in this process.

In my opinion, there’s nothing to be gained by living in fear. Taking reasonable efforts to protect your personal information is often enough. Identity thieves are, by and large, opportunistic in nature and will often simply move on if you make yourself a difficult target.

About  L. Stephen Younger, Director of Operations and Chief Compliance Officer for Green Wealth Management

L. Stephen Younger is Director of Operations and Chief Compliance Officer for Green Wealth Management, an independent member of the BAM ALLIANCE.

Prior to joining Green Wealth Management, Stephen worked in Alaska as Institutional Services Manager for a nationwide trust company and as the fraud, forgery, and account control officer for one of the largest federally-chartered credit unions in the United States.

By clicking on any of the links above, you acknowledge that they are solely for your convenience, and do not necessarily imply any affiliations, sponsorships, endorsements or representations whatsoever by us regarding third-party Web sites. We are not responsible for the content, availability or privacy policies of these sites, and shall not be responsible or liable for any information, opinions, advice, products or services available on or through them.

The opinions expressed by featured authors are their own and may not accurately reflect those of the BAM ALLIANCE. This article is for general information only and is not intended to serve as specific financial, accounting or tax advice.

© 2014, The BAM ALLIANCE