The Navigator

A Financial Planning Resource from Appleseed Capital

Winter 2015 | Issue 2

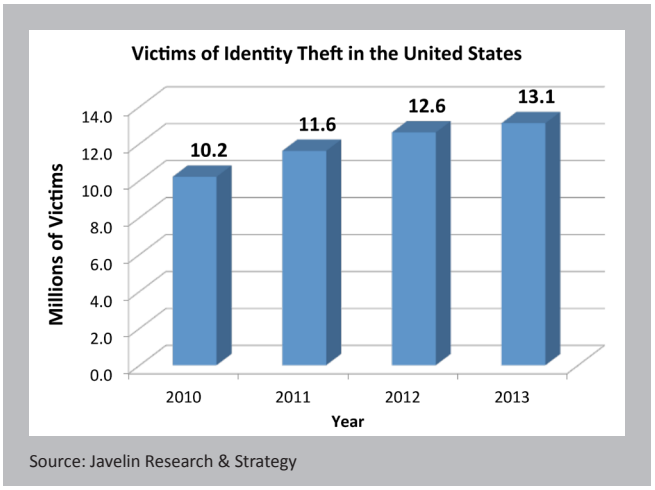
The Growing Threat of Identity Theft

The risk of becoming a victim of identity theft or fraud has risen to an alarming level for most Americans, yet both the frequency and severity of these crimes continue to accelerate. Investors must be especially wary of this risk, given the potential consequences that could occur if their confidential personal information were to fall into the wrong hands. In this article, we discuss some of the specific risks that investors face with regard to identity theft, as well as some of the measures that they can take to reduce their risk of becoming a victim and to minimize the damage that could be caused if they do, in fact, fall victim to identity theft.

The Growing Threat of Identity Theft: Protecting Yourself and Your Assets

by Matthew Blume, CFA

Identity theft or identity fraud has become increasingly prevalent over the last few years. Based upon statistics alone, there is a nearly 7% chance that you have experienced such an incident.[1] According to an annual study conducted by Javelin Strategy & Research, approximately 13.1 million Americans were victims of identity theft or fraud in 2013. In total, identity theft crimes caused approximately $24.7 billion in direct and indirect damages in 2012, according to the Bureau of Justice Statistics. This figure dwarfs the $14 billion in damages caused by all other types of theft (burglary, auto theft, etc.) combined in the United States over the same time period, and the numbers are deteriorating at an alarming rate. Experts predict that the frequency and severity of identity theft/fraud will continue to increase for the foreseeable future, as Americans put more of their personal information online and identity thieves grow in their level of sophistication. This concerning trend can be seen in the chart below, which shows the number of victims of identity theft in the United States for each year from 2010 to 2013.



Source: Javelin Research & Strategy

Unquestionably, identity theft has become a very real financial risk for practically all Americans. With that in mind, in this letter, we will first explain exactly what identity theft/fraud is and how it can occur. Then, we will discuss the specific risks that we and our clients face with regard to these crimes and the ways in which we and our clients' primary custodians (Pershing and Schwab) are working to mitigate those risks. Lastly, we provide actionable steps that you can take to reduce your risk of becoming a victim or to reduce the amount of damage that these crimes can cause should you fall prey to an identity thief.

According to the Department of Justice, identity theft or identity fraud victims are defined as persons age 16 or older

1 http://www.bjs.gov/content/pub/pdf/vit12.pdf

Appleseed Capital

161 North Clark Street, Suite 2200, Chicago, IL 60601
1.800.611.2187 | contact@appleseedcapital.com | www.appleseedcapital.com

who have suffered one or more of the following incidents:

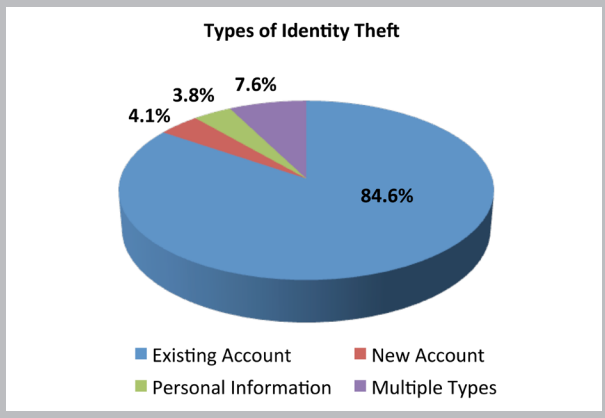
- Unauthorized use or attempted use of an existing financial account (e.g., checking, savings, investment, credit or debit card, telephone, online, or insurance account);
- Unauthorized use or attempted use of personal information to open a new financial account;
- Unauthorized use or attempted use of personal information for a fraudulent purpose (e.g., obtaining medical care, renting an apartment, or providing false information to a law enforcement officer);
- Unauthorized claims of IRS tax refunds and/or Social Security payments.

Identity theft can result from any of a number of different root causes, but, in essentially every case, sensitive personal information is obtained by an identity thief and used to commit fraud or property theft. Interestingly, the Internet is not the primary source of this divulgence of information – at least not yet. Stolen physical property remains the largest source of sensitive information for identity thieves. Stolen wallets, purses, mail, cell phones, laptops, and even garbage can provide identity thieves with a wealth of personal information that can be used to wreak havoc on a victim's life. Thieves can also steal credit and debit card information by using skimming devices that can read and store credit or debit card information. These devices can be used by dishonest employees who quickly swipe a distracted customer's card, storing the information for later use, or they can be placed inside of a retailer's credit card readers, storing the card data of each card that is used on the machine and retrieved later by the identity thief.

While the Internet is not the primary source, it has become a significant and fast-growing source of confidential personal information for identity thieves. Fraudsters can hack email accounts to obtain account information and passwords. In addition, they can skim credit and debit card information from poorly secured websites that process retail transactions, and they can take advantage of unsecured public wireless networks to intercept sensitive data transmissions. Identity thieves also engage in "phishing," in which the fraudster creates a fake website that is designed to look just like the website of a legitimate financial institution. The fraudster then contacts the victim through email, posing as the institution, and asks the victim to provide his or her account information on the fake website in order to "verify" the account for security reasons.

Security breaches of third-party data providers are yet another source of confidential personal information for identity thieves, in which the data of thousands or even millions of people can be compromised at one time. There have unfortunately been several well-publicized cases of such breaches in recent years, in which customers of Target, Home Depot, JPMorgan Chase, and Staples (among others) had their personal data stolen by identity thieves, causing major headaches for both customers and businesses alike.

The vast majority of identity theft incidents involve the fraudulent use of an existing account. In 2012, 85% of all identity theft crimes fell into this category.[2] Given the nature of our business as an investment advisor, we play an important role in monitoring the flow of client assets, as we often facilitate the exchange of wire and transfer instructions between our clients and their custodians. In recent years, our industry has been besieged by fraudsters who have zeroed in on a particular type of transaction called a "third-party wire transfer," in hopes of exploiting these transactions at the expense of investors. In a typical wire transfer, a client instructs his or her custodian to send funds electronically to the client's bank account or another financial account owned by the client. A third-party wire transfer, however, differs from a typical wire transfer in that the client's instructions are for the custodian to send funds electronically to a financial account owned by someone other than the client. Legitimate third-party wire transactions might include things such as paying a bill, donating to a charity, gifting assets to a family member, or paying a tax bill.



Source: Bureau of Justice Statistics

Until somewhat recently, the process for initiating a third-party wire transfer consisted of the client submitting a signed Letter of Authorization (LOA) indicating the party to whom the transfer was to be sent and the amount to be wired. We then passed these instructions on to the custodian, who would execute the actual transfer of assets. That system existed for years, but identity thieves and fraudsters eventually found a way to exploit this process. As more and more business correspondence has transitioned to online

2 http://www.bjs.gov/content/pub/pdf/vit12.pdf

media (primarily email), thieves have discovered that they can intercept client communications and create fraudulent third-party wire transfer requests.

Often times what happens is that a client will request a legitimate third party wire transfer and will provide the necessary signed LOA as an email attachment. Fraudsters who hack into a client's email account can then reuse this signed LOA, simply changing the recipient, amount, and date, so that the funds are set to be transferred to an account to which the thief has access. The thief will send this LOA from the client's email account, often including some friendly conversation or personally identifying information (such as the use of a nickname) in the email to make it seem as though it really is the client who is sending it.

Fortunately, while the crooks are creative and devious, the industry has been quick to react to third-party wire fraud and put into place a number of technical and procedural safeguards that are significantly reducing the frequency and severity of these incidents. We and our clients' primary custodians have enacted new practices that are aimed specifically at minimizing the risk of fraudulent third-party wire transfers. The primary safeguard that has been put in place is very simple but highly effective. It consists merely of a phone call between us and the client to provide assurances that the client did indeed request a wire transfer to the third party listed on the LOA. While a thief may be able to imitate a client very effectively via email, it is a much taller order to imitate a client over the phone, especially given that the thief would have to have physical access to the client's telephone. For this reason, the practice of calling the client and signing a form verifying that we have, in fact, verbally spoken to the client to confirm the request, has been one of the most effective tools against third-party wire fraud. In addition to the all-important phone call, we have procedures in place that spell out exactly how to respond to any red flags that are discovered in communications with clients, including changing account numbers, monitoring accounts, and notifying law enforcement when appropriate.

While the procedural changes described above have created quite an impediment to fraudsters with regard to third-party wire transfers, there is no doubt that danger still lurks. Identity thieves are constantly looking for new ways to obtain and exploit client information for illicit gain. These thieves are technologically savvy and always seem to be a half step ahead of regulators and financial institutions. This means that while we and our clients' custodians remain vigilant in employing methods to prevent these types of incidents, our clients must also do everything that is within their power to protect themselves from identity theft and fraud.

There are many things that clients can do to minimize their vulnerability to identity theft. The primary focus should be on protecting personal information, whether physical or electronic. Below we have listed important actions that you can take to protect your personal information and therefore reduce your risk of becoming a victim of identity theft.

Protecting Physical Data

- Lock sensitive documents in a safe place, both at home and at work.
- Limit what you carry with regards to personal identification information (identification, credit cards, Social Security card, etc.)
- Shred receipts, credit applications, bank and brokerage account statements, checks, etc. Anything that contains account numbers or other personally identifying information should be shredded.

Protecting Electronic Data

- Encrypt sensitive emails.
- Use a reputable email provider that puts a strong emphasis on security. Google's Gmail is generally regarded as one of the best free email providers with regard to security, whereas certain other providers have a reputation for having weaker security. Use strong, complicated passwords, and always keep passwords private.
- Avoid using the same password for multiple log-ins.
- Activate two-step verification or other enhanced security features as part of your log-in process.
- Periodically change your passwords.
- Consider a password vault program to store and maintain your log-in information.
- Don't overshare on social networking websites. For example, do not share pictures of you on vacation, as that could be a signal for burglars that your house is vacant.
- Use security software on your computer to protect against viruses that can skim information from your computer.
- Avoid opening suspicious emails.
- Be wary of public Wi-Fi networks, as they do not use encryption to protect transmissions.
- Password-protect your mobile phone and computer and enable timed lock functionality after periods of inactivity.

- If you are replacing your mobile phone, use a memory wiping application to clear the memory before discarding the phone.
- If available, enable a remote wipe or kill button functionality in the event of a lost device.
- Be aware of your surroundings when accessing personal data in a public place, as identity thieves may observe your actions and gain access to your online accounts (this may be especially important when traveling abroad).

While this list of recommendations is by no means exhaustive, putting the aforementioned items into practice will go a long way toward reducing your risk of becoming a victim of identity theft. However, no matter how careful you are in protecting your personal data, there is no guarantee that you will not have to deal with the fallout of identity theft at some point. There are simply too many ways for thieves to steal and exploit personal information to know with any certainty that identity theft will not happen to you. With that in mind, below are some guidelines for what you should do if you do in fact find yourself the target of an identity thief.

- As soon as you become aware of the issue, immediately contact one of the three credit reporting agencies (TransUnion, Experian, or Equifax) and report a fraud alert. You do not need to contact all three agencies, as you can ask the one agency that you do contact to then pass along the alert to the other two agencies.
- After you report a fraud alert, order your credit report from all three credit agencies to see what, if any, damage has been done. Check for unauthorized uses of and applications for credit. If you are able to determine that a specific account has been tampered with, contact the fraud department of the associated business to inform them of the fraud. Follow up in writing and keep detailed records of all of your communications. Sign up for fraud monitoring with one of the credit reporting agencies and be sure to dispute unauthorized charges on a timely basis.
- Go to www.ftc.gov/complaint to file an Identity Theft Affidavit. Print the affidavit, and take it to your local police department. File a police report about the theft. The police report combined with the Identity Theft Affidavit makes up what is called an Identity Theft Report. This report will be very important when disputing unauthorized charges and repairing any damage that has been done to your credit.

These steps should help stop the immediate damage caused by identity theft, though more serious cases of fraud could require significantly more work to fully repair the damage caused by an identity thief. Visit the FTC's website at http://www.consumer.ftc.gov/topics/privacy-identity to learn more about ways to protect yourself from identity theft and also what to do if you find yourself a victim.

Given the prevalence of identity theft crimes in the United States, the magnitude of the potential losses that can occur, and the variety of ways in which thieves can obtain the data needed to commit these crimes, it is clear that identity theft has become a significant risk for practically all Americans. As financial institutions that have been entrusted with protecting our clients' assets, Appleseed Capital and our clients' custodians must constantly be vigilant for any indication that the identity of a client has been compromised. Similarly, you should do everything that you can to reduce your vulnerability to identity theft, as doing so could save you countless hours spent cleaning up the damage (let alone the monetary consequences) caused by fraud. If you have a suspicion that your identity has been jeopardized, please contact us immediately so that we can work with you to protect your financial assets from theft. We take our responsibility as your advisor very seriously, so you can rest assured knowing that, as has always been the case, we place the protection of our clients' capital above all else.
