Will the Real John Doe Please Stand Up?: Tax Identity Theft Developments

By Sharyn M. Fisk and Cory Stigile

Sharyn Fisk and Cory Stigile describe identity theft as used to commit tax fraud, the actions taken by the IRS to combat this fraud and steps that individuals and practitioners may take to keep at-risk information private

The IRS is grappling with a recent surge in identity theft-based tax fraud. Identity theft topped the IRS's 2012 annual "Dirty Dozen" list of tax scams.[1] In 2011, the IRS stopped approximately 262,000 fake returns based on identity theft from being processed, preventing nearly $1.3 billion in tax refunds from going to criminals.[2] That is more than a fivefold increase from 2008, when the IRS stopped approximately 50,000 fake returns claiming approximately $247 million in fraudulent refunds.[3]

I. Identity Theft

Identity theft occurs when someone uses another individual's personally identifying information (*e.g.,* name, Social Security number (SSN), credit card number, *etc.*), without that person's permission, to commit fraud or other crimes. The Federal Trade Commission (FTC), the lead government agency for information relating to identity theft, estimates that as many as nine million Americans have their identities stolen each year. Identity thieves typically use personal data to deplete financial accounts; place charges on the victim's credit cards; apply for new loans, credit cards, services or benefits in the victim's name; and even file tax returns under a victim's name.

Sharyn M. Fisk and **Cory Stigile** are attorneys with Hochman, Salkin, Rettig, Toscher & Perez, P.C., in Beverly Hills, California.

Identity theft poses a serious problem for individuals. While some identity theft victims can resolve their problems quickly, others can spend months or years repairing damage to their good name and credit. Victims can be left with lingering credit and other financial problems. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or vehicles because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

A. Internet-Based Sources for Identity Theft

The growth in information technology, networking and electronic storage has made it easier for identity thieves to collect personal information. Too much of what ends up in an individual's inbox are veiled attempts to separate the individual from his or her private information, and ultimately his or her money. Two common data gathering techniques identity thieves use are phishing and malware.

1. Phishing

Phishing is the act of sending an email under the auspices of a legitimate enterprise in an attempt to lure the recipient into surrendering private information. According to the FTC, phishers send emails or pop-up messages that claim to be from a business or organization (*e.g.,* an Internet Service Provider, a bank, a

vendor, an online payment service or a government agency). The message may ask the recipient to update, validate or confirm his or her account information. Such emails may be targeted to the individual's particular business, such as emails related to a purported continuing legal or accounting education program. Often, phishing emails threaten dire consequences if the recipient does not respond. The email may even direct the recipient to a website that looks just like a legitimate organization's site—but it is not.

2. Malware

Malware is a malicious code that can take over a victim's computer hard drive, thus giving someone remote access to the computer, or it could look for passwords and other information and send them to the scammer. The scammers will then use whatever information they gather to commit identity theft and/or financial theft.

B. Non-Internet-Based Sources for Identity Theft

Not all identity theft scams are conducted through the Internet—there is still the old-fashioning theft of wallets, purses, mail, *etc.*, to obtain an individual's personal information. Old discarded laptops may contain residual personal information. In addition, identity theft can occur via the telephone or fax. Identity thieves also use pretexting, which is where the thief, with a limited amount of personal information, uses false pretenses to obtain additional personal information from a financial institution, company or government agency. Identity thieves may go through a person's trash looking for credit card receipts, bills, discarded tax returns, bank records or other documents containing personal and financial information. Identity thieves have submitted *Change of Address* forms to divert an individual's billing statements or mail to another location.

The common theme between the Internet and non-internet based sources of information is that identity thieves know how to take otherwise benign information that people use in their lives to steal their identities.

II. Identity Theft for Tax Fraud

The IRS estimates that between mid 2009 to the end of 2011, 404,000 people were victimized by identity theft tax fraud.[4] According to the IRS, identity theft for tax fraud is most likely to occur by a criminal using stolen identities to file fake returns claiming tax refunds. Additional areas involving identity theft include employment tax cases, abusive return preparer schemes, and narcotics and money laundering investigations. Criminals also use the IRS name to steal identities through phishing, malware and other means. When it comes to identity theft for tax fraud, taxpayers may not be aware they have become victims until they receive a letter from the IRS stating more than one tax return was filed with their information or that IRS records show wages from an employer the taxpayer has not worked for.

A. False Refund Claims

On average, the IRS processes more than 100 million income tax refunds each year. Over the past few years, the IRS has seen a significant increase in refund fraud schemes involving identity thefts. Criminals are now using laptops and electronic mailboxes to steal hundreds of millions of dollars by filing fraudulent tax returns with stolen SSNs. The popularity of refund fraud using stolen identities has become so widespread that some criminals are offering classes in how to commit the crime.[5]

To commit identity theft tax fraud, an identity thief uses a legitimate taxpayer's name and SSN to file a fake tax return claiming a large refund. The thief will file the fake tax return early in the filing season before the legitimate taxpayer files his or her return and before the IRS matches up W-2 information with taxpayer SSNs. The IRS, after confirming that the filer's name and SSN match, issues the refund. The thief requests that the refund be paid out to a debit card or direct deposit to a checking account, which is then promptly emptied, rather than by paper checks.

B. Using the IRS Name to Steal Identities

Communications—whether an email, letter or phone call—from institutions of the federal government, especially the IRS, catch a person's attention. Thus, they make good bait for phishing schemes and other scams. Although the FTC has reported that the IRS has a low number of identity theft crimes, phishing schemes using the IRS name have been escalating in number and sophistication. A recent check on the website Snopes.com shows that within the first two months of 2012, there had been three mass phish emailings spamming millions of Internet users with phony notices from the IRS: 1) a January 2012 phony notice from the IRS that the recipient was eligible to

receive a tax refund and inviting the taxpayer to click on a link to a form by which the taxpayer could claim the refund; 2) a February 2012 phony notice from the IRS indicating the recipient is being penalized $10,000 for failure to file an income tax return; and 3) a February 2012 phony notice supposedly sent by Intuit on behalf of the IRS, advising recipients that there were discrepancies in their Employer Identification Numbers. Phishing schemes involving the IRS name attempt to convince the recipient that he or she is receiving an email from the IRS by using the IRS' official seal or logo, attaching a fake form made to look like an official IRS form, and/or directing the recipient to a webpage made to look like the IRS' legitimate website.

Unlike other phishing schemes that emulate mailings from various private financial institutions (*e.g.,* Wells Fargo), which can be easily recognized as false by many recipients (because they do not conduct business with that institution), a forged IRS notice has the potential to take in a much larger pool of victims as most adult U.S. residents have had dealings with the IRS. Many people find the federal income tax filing process complicated and confusing, so it can seem plausible that a return may have gone astray, a necessary form was not filed in time, they might have underreported income, or have unclaimed refunds or payments. The following are some such phishing schemes that take advantage of these factors and use the IRS' name:

- Phony e-mail from the IRS offering $80 to recipients who complete satisfaction surveys is a phishing scheme used to steal personal information;
- Fake notice from Intuit on behalf of the IRS advising recipients that there are discrepancies in their Employer Identification Numbers;
- Bogus notice from the IRS indicating the recipient is being penalized $10,000 for failure to file an income tax return;
- Fake notice from the IRS notifying the recipient of the filing of complaints in regards to business services;
- Fake notice from the IRS indicating that recipient has unreported or underreported income;
- Phony notice from the IRS informing the recipient that his or her electronic tax return or payment has been rejected;
- Bogus notice from the IRS indicating that the recipient has a refund coming;
- Phony notice from the IRS informing the recipient that there have been a number of fraudulent attempts to access the taxpayer's bank account;
- Fake e-mail from the IRS stating that there is a refundable credit available to workers, consumers and retirees that can be paid into the recipient's bank account if the recipient registers his or her account information with the IRS;
- Fake notice related to the repatriation of funds from foreign bank accounts or filing informational returns for foreign entities.

Both the IRS and the Government Accountability Office, which has reviewed identity theft-related tax fraud, agreed that there is *no* evidence that the recent increase in tax-related identity theft is a result of breaches in the IRS' physical or online security.[6]

C. Employment Tax Fraudulent

Identity theft in the employment tax context occurs when an identity thief uses a taxpayer's name and SSN to obtain a job. The IRS subsequently receives income information from the identity thief's employer. When the legitimate taxpayer files his or her income tax return, the IRS matches income reported by the victim's employer, as well as the thief's employer, to the victim's tax return. The IRS subsequently notifies the legitimate taxpayer of unreported income, because it appears that the taxpayer has earned more income than was reported on the tax return. Employment tax fraud causes tax administration problems as the IRS has to sort out what income the legitimate taxpayer earned and what income the identity thief earned.

III. IRS Action

In 2004, the IRS developed a strategy to address the problem of identity theft-related tax administration issues. This strategy has evolved but continues to serve as the basis for all of the IRS' efforts to reduce the effects of identity theft on tax administration and to provide services to victims of identity theft. Currently, the IRS is implementing a two-pronged strategy that focuses on fraud prevention and victim assistance.

A. Fraud Prevention

The IRS is taking multiple steps to detect, prevent and resolve refund and employment fraud conducted through identity theft. Beginning in 2011, the IRS launched the Enhanced Return Processing program. Under this program, it created a cross-functional group made up of various IRS divisions that work to develop enhanced revenue protection processes and policies beginning with the 2012-filing season. The efforts being done by this group are as follows.

1. Filters to Screen for Potential Identity Theft Tax Fraud

The IRS is designing new identity theft screening filters that should improve its ability to spot false returns before they are processed and before a refund is issued. For example, new filters are being designed to flag returns if certain changes in taxpayer circumstances are detected. One way for the IRS to check for identity theft is to look for significant differences between current year and prior year tax returns. However, changes in taxpayer circumstances do not necessarily indicate identity theft. In 2009 there were ten million address changes, 46 million changes in employer, and millions of deaths and births.[7] Normal events like these can result in a large number of false positives. Because a return that is caught by the filter requires manual review, checking all returns that reflect these changes for possible identity theft would overwhelm the IRS' capacity to issue refunds to legitimate taxpayers in a timely manner. Given the number of changes that many taxpayers experience in a year, it is a challenge for the IRS to develop effective filters. Thus, until optimal filters are in place, these new filters mean that refund claims for more taxpayers will get extra screening prior to the issuance of the refund, which may delay the issuance of refunds.

> Identity theft poses a serious problem for individuals. While some identity theft victims can resolve their problems quickly, others can spend months or years repairing damage to their good name and credit.

2. Identity Protection Personal Identification Numbers

Recently, the IRS began issuing special identification numbers (Identity Protection Personal Identification Numbers or IP PINs) to taxpayers whose identities are known to have been stolen to facilitate the filing of their returns and prevent others from utilizing their identities on future returns. The use of IP PINs is more fully described below.

3. Matching Data

Currently, the IRS does not match tax returns to W-2 forms that employers file until months after the filing season ends. The first match is done in June. Consideration regarding accelerating the availability of information returns in order to identify mismatches earlier would enhance the IRS' ability to spot fraudulent tax returns before they are processed.

4. Fraudulent Returns Using Deceased Taxpayers' Identities

The IRS is developing new mechanisms to stop the growing trend of fraudulent tax returns being filed under deceased taxpayers' identities. Identity thieves surf the Internet for the names, addresses and SSNs of recently deceased people. For example, until recently, Ancestry.com website reported the SSNs of deceased individuals. However, after being alerted to the problem of criminals using such information to file fake returns, the company has changed this practice for anyone who had died in the past 10 years.[8] The IRS has now added to its process the re-routing of returns in which it appears that an identity thief has used a decedent's SSN. The IRS is also expanding a successful pilot program in 2010 that marks the accounts of deceased taxpayers to prevent misuse by identity thieves. Currently, the IRS has marked 230,000 accounts of decedents. In addition, the IRS is working with the Social Security Administration (SSA) to more timely utilize the information the SSA makes available to the IRS.

5. Prisoner Identification

The IRS is expanding the use of its list of prisoners to better utilize the list to stop problematic returns. The IRS recently received additional help under the United States-Korea Free Trade Agreement Implementation Act that would require federal and state prisons to provide information on the current prison population. The IRS intends to discuss with prison officials to determine the best way to move forward with this new authority.

These new enhanced revenue protection processes and policies are a double-edged sword for the IRS. The IRS must balance its duty to prevent the public fisc from fraud, while also maintaining its duty to get taxpayers their refunds as quickly as possible. With an ever-evolving criminal element, this trade off will continue to be an issue for the IRS. With more than 100 million income tax refunds to process each year, the IRS acknowledges it will never be able to quell identity theft tax fraud completely. "The IRS cannot stop all identity theft. However, we are committed to continuing to improve our programs."[9]

6. Criminal Investigation Division

The IRS is also using its Criminal Investigation (CI) division to detect, investigate and prevent identity theft tax fraud. CI's investigation of identity theft tax fraud has increased significantly in response to the rise in identity theft cases. In FY 2011, CI initiated 276 investigations, recommended 218 cases for prosecution, resulting in 165 indictments in identity-theft related cases (the decision to prosecute identity thieves does not rest with the IRS, but rather with the Department of Justice (DOJ)), with 80 individuals sentenced to an average time served of 44 months.[10] In late January 2012, the IRS and DOJ announced a nationwide sweep of arrests, indictments and other actions against 105 suspected perpetrators of identity theft tax fraud in 23 states.[11] In conjunction with this sweep, IRS auditors and investigators conducted extensive compliance visits to approximately 150 money service businesses in nine locations across the country to help ensure these check-cashing facilities were not facilitating refund fraud and identity theft.

Currently, CI has four Scheme Development Centers (SACs) across the United States whose primary mission is detecting refund fraud. These SACs have uncovered numerous identity theft-related schemes. These schemes are forwarded to one of CI's 26 field offices for criminal investigation and/or its civil counterparts to resolve victim accounts. After CI conducts its investigation, it recommends prosecution, when appropriate, to the DOJ. Specifically, it may recommend prosecution pursuant to 18 USC §1028 (aka the *Identity Fraud Statute*) where the evidence supports it. Per IRS policy, the Identity Fraud Statute is not intended to be a stand-alone violation, but rather used as a companion charge when it enhances the overall substantive tax, money laundering and/or conspiracy charges.[12] As a result, CI generally pairs 18 USC §1028 with other substantive tax or tax-related charges.

In addition to detecting and investigating identity theft-related refund fraud, CI also works with other IRS divisions to assist in preventing other types of identity theft involving the tax administration. For example, CI provides regular updates to the IRS' Wage and Investment (W&I) division regarding emerging scheme trends so that processes and filters can be modified to prevent fraud. CI also works with other federal, state and local law enforcement agencies on joint investigative efforts involving identity theft tax fraud (*e.g.,* CI participates in the DOJ's *Identity Theft Interagency Working Group*).

Ironically, some of the IRS' initiatives to combat identity theft are limited because tax returns and other information submitted to the IRS—and, in some cases, generated by the IRS—are confidential and protected from disclosure by the IRS unless specifically authorized by statute.[13] The IRS can disclose identity theft-related events that occur on a taxpayer's account to the taxpayer (*e.g.,* the fact that an unauthorized return was filed using the taxpayer's information or that the taxpayer's SSN was used on another return). The IRS cannot, however, disclose to the taxpayer any other information pertaining to employment or refund fraud (*e.g.,* the thief's identity or any information about the thief's employer). Moreover, under the existing rules on disclosure, the IRS has limited authority to share identity theft information with other federal agencies. When performing a criminal investigation, CI can only make investigative disclosures (*i.e.,* the sharing of specific, limited information necessary for receiving information from other federal agencies that might support or further IRS' investigation). Disclosure of taxpayer information to state and local law enforcement agencies is even more limited. Congress is considering amending the disclosure rules so that the IRS can share information with state and local law enforcement in order to combat identity theft tax fraud.

B. Taxpayer Assistance

In 2008 and 2009, the IRS implemented several initiatives to detect and resolve identity theft cases.

1. Account Indicators

The IRS has implemented the use of "indicators"to detect and resolve identity theft.[14] These account flags, which are visible to all IRS personnel with account access, speeds resolution of identity theft issues by making a taxpayer's identity theft problems visible to all IRS personnel accessing the account. The IRS uses different indicators depending on the circumstances in which the IRS receives an indication of an identity theft–related problem. For example, the IRS has a temporary indicator to alert all IRS units that an identity theft incident has been reported but not yet resolved.[15] Once the IRS substantiates any taxpayer-reported information, either through IRS processes or the taxpayer providing documentation of the identity theft, it places the appropriate indicator on the taxpayer's account and notifies the taxpayer. Once an indicator is on a taxpayer's account, the taxpayer is relieved of having to repeatedly explain his or her identity theft issues or prove his or her identity to multiple IRS units (*e.g.,* Examination Division, Collection

Division, *etc.*). The indicators also alert IRS personnel that a future account problem may be related to identity theft and help speed the resolution of any such problems. After three consecutive years of no identity-theft incidents on a taxpayer's account, the IRS will remove an indicator. In addition, the taxpayer can request that an indicator be removed sooner.

2. Identity Protection Personal Information Numbers (IP PIN)

In January 2011, the IRS began piloting an Identity Protection PIN Program, which is aimed at cutting repeat fraud for taxpayers who have been victims of identity theft. Taxpayers who have been victims of identity theft will receive a secret Personal Identification Number (PIN) so that they can verify their identities at the time they file their return. The IRS will process a return that includes the PIN, while a return without it will be rejected. The IRS plans to send a new PIN to the taxpayer every year. The IRS has issued IP PINs to over 50,000 taxpayers who have been victims of identity theft, and it intends to issue IP PINs to more than 200,000 taxpayers for the 2012 filing season.[16]

3. Employee Training

The IRS recently conducted a thorough review of the training it provides to its employees to ensure that they have the tools and sensitivity they need to respond to a taxpayer who has become a victim of identity theft.[17] Typically a taxpayer discovers that he or she has become the victim of identity theft when her or she receives a letter or notice from the IRS. In response, the first thing that taxpayer does is call the number identified on the letter or notice. Thus, the IRS has updated its training course for its telephone representatives to ensure that its operators maintain the proper level of sensitivity when dealing with identity theft victims and understand the serious financial problems that identity theft poses for these taxpayers. The IRS has also broadened the scope of training to cover those IRS employees who are not telephone assistors but who nonetheless interact with taxpayers or work identity theft cases.

4. Taxpayer Outreach and Education

The IRS has recently created a new section dedicated to identity theft matters on its webpage: www.IRS.gov/identitytheft. This section provides taxpayers with resource materials, guides, news and FAQ regarding identity theft. The IRS also provides tips for taxpayers to protect against phishing schemes and identifying the latest schemes on its webpage. The IRS' identity theft section provides links to other agencies that address identity theft (*e.g.,* the FTC, *etc.*). This section includes contact information for the IRS' Identity Protection Specialized Unit at 800-908-4490 where taxpayers can receive assistance in resolving identity theft issues with the IRS. The IRS has also posted on this section YouTube videos and podcasts entitled: *ID Theft: Protect Yourself from Identity Theft* and *ID Theft: Are You a Victim of Identity Theft?*

IV. Taxpayer and Tax Professional Action

There are numerous precautions a taxpayer can take to avoid becoming the victim of identity theft. In addition, if an individual's identity has been stolen, prompt and thorough actions can be taken to minimize the damage and speed the recovery of the theft.

A. Minimize the Chance of Becoming an Identity Theft Victim

1. Do Not Fall for Phishing Schemes

Victims of phishing can become victims of identity theft. First and foremost, the IRS does not send unsolicited, tax-related emails to taxpayers, nor does the IRS request personal or financial information over the Internet.[18] This includes any type of electronic communication, such as text messages and social media channels.[19] The IRS also does not send emails stating a taxpayer is being electronically audited or is getting a refund. When the IRS contacts a taxpayer, it generally sends a letter or notice via U.S. mail, and every such communication includes a telephone number that the recipient can call for confirmation. Additionally, the IRS does not use PIN numbers, passwords or other confidential access information relating to a taxpayer's credit card, bank or financial accounts.

People should promptly report suspicious emails they receive claiming to be from the IRS or an organization closely linked to the IRS (*e.g.,* the Electronic Federal Tax Payment System (EFTPS)), by *forwarding the original email* to: phishing@irs.gov and to the FTC at spam@uce.gov. The IRS can use the information, URLs and links in suspicious emails forwarded to it to trace the hosting website and alert authorities to shut down the fraudulent sites. By the end of 2011, the IRS had received approximately 33,000 forwarded scam emails, re-

flecting more than a thousand different incidents. The Treasury Inspector General for Tax Administration (TIGTA) has reported that it has identified host sites in 19 different countries, including Argentina, Aruba, Australia, Austria, Canada, Chile, China, England, Germany, Indonesia, Italy, Japan, Korea, Malaysia, Mexico, Poland, Singapore and Slovakia, as well as the United States. Individuals can report the fraudulent misuse of the IRS name, logo, forms or other IRS properties by contacting TIGTA at 1-800-366-4484.

> Identity theft does not apply only to individuals. There have been reported instances where company and benefit plan identities have been stolen.

2. Avoid Links or Attachments in Questionable Emails

Do not click on or cut and paste links contained in unsolicited or questionable emails. Instead, if an individual needs to visit an organization's website, he or she should go there directly by typing the organization's URL into the web browser. If an individual does not know the entity's website, he or she should search for it using a web browser rather than following links in email messages. If a person discovers a website that claims to be the IRS but does not begin with www.irs.gov, he or she should forward that link to the IRS at: phishing@irs.gov. Also, email recipients should not open attachments in unsolicited or questionable emails, which may contain malware or viruses that could infect their computer. If a recipient is unsure about a communication from an organization, he or she should check the organization's website. Many organizations post scam alerts when their name is used improperly.

3. Protect Personal Information

Individuals can minimize the risk of having their identity stolen by placing passwords on their credit cards, bank and phone accounts. Individuals should avoid using easily available information like a mother's maiden name, birth date, the last four digits of their SSN or phone number, a series of consecutive numbers, or for the men out there "0007" (one zero better than James Bond).

Identity thieves continue to evolve and often pose as representatives of banks, Internet Service Providers and government agencies to get people to reveal their social security numbers, mother's maiden name, account numbers and other identifying information. Individuals should not give personal information over the phone, through the mail or on the Internet unless they have initiated the contact or they are sure they know who they are dealing with. For instance, if a person receives a call from his or her car leasing company regarding a missed payment, instead of giving them his or her SSN for verification, the individual should politely tell the caller that he or she will call back at the company's 1-800 number.

When sending mail, individuals should not use an unsecured mailbox. Instead, they should deposit directly in a post office collection box or at the local post office. Individuals should promptly remove mail from their personal mailbox when it is received. If a person is planning to be away from home and cannot pick up his or her mail, the individual should call the U.S. Postal Service to request a vacation hold until he or she can pick the mail up or return home to receive it.

Individuals should be cautious when responding to mail, phone or Internet promotions. Identity thieves often create phony promotional offers to get individuals to provide personal information.

When ordering new checks, individuals should pick them up from the bank instead of having them mailed to their home mailbox.

Individuals should protect their computers by using anti-spam/virus software, updating security patches, firewalls, and changing passwords for Internet accounts. If someone works remotely from home, that person should make sure his or her computer has the same protections as his or her work computer. A person's virus protection software should be set to automatically update each week. Individuals should not open files, click on hyperlinks or download programs from strangers, and they should also be careful about using file-sharing programs. If a person is using a high-speed Internet connection like cable that leaves the computer constantly connected to the Internet, he or she should use a firewall program to stop uninvited access to the computer. Without it, hackers can access personal information stored on the computer or use it to commit other crimes. Before disposing of

an old computer, a person should delete all personal information using a "wipe" utility program to overwrite the entire hard drive. Individuals should also treat their Smartphone's like a computer and protect it with a sufficiently complicated password.[20]

Individuals need to show their Social Security card to their employer when they start a job or to a financial institution for tax reporting purposes. However, they should not routinely carry their Social Security card or other documents that display their SSN. Moreover, they should not give a business their SSN just because it is asked for. A SSN should only be given when it is legally required to do so (*e.g.,* for tax reporting purposes, *etc.*)

While preparing a tax return for electronic filing, a person should make sure to use a strong password to protect the data file. Once the return has been e-filed, an individual should save it on a password-protected CD or flash drive and remove the personal information from their hard drive. The CD or flash drive should be stored in a safe place, such as a lock box or safe. If an individual is working with a return preparer, he or she should ask the return preparer what measures they take to protect their client's information.

4. Social Networking Sites

Individuals should be conscientious of how they use social networking sites. Be aware of privacy settings and consider using separate accounts for personal, versus business use. Social networking users with public profiles can be careless with their personal information: 45 percent share their birth date and year; 63 percent shared their high school; 18 percent shared their phone number; and 12 percent shared their pet's name.[21] It has been asserted that there may be a connection between active use of social networks and susceptibility to identity theft. According to one study, slightly more than 10 percent of LinkedIn users say they were hit by identity theft, while 7 percent of Google+ users and 6.3 percent of Twitter users reported being victims—all three above the national average of 4.9 percent. Facebook users were at 5.7 percent.[22]

5. Annually Request a Copy of Your Credit Report

An individual may catch an identity theft incident early by annually ordering a free copy of their credit report.[23] To order a free annual report, the individual should visit www.annualcreditreport.com or complete the annual credit report request form available at www.FTC.gov/credit.[24]

B. Steps an Identity Victim Should Take

A victim of identity theft should take the following five steps as soon as possible upon discovery that his or her identity has been stolen. Victims should keep a record with the details of their conversations and copies of all correspondence with enclosures.

First, a victim should contact his or her local police or sheriff's department and tell them that they want to file a report about identity theft. The department may be reluctant to file such a report, but it is critical to document the theft at an early stage in order to obtain greater legal protection. If the police are reluctant to take a report, the victim should ask to file a "Miscellaneous Incident" report or try another jurisdiction (*e.g.,* the state police). Victims can check with the state Attorney General's office to find out if state law requires the police to take reports for identity theft.

If the victim files a theft report in person, he or she should bring supporting documentation of the identity theft *and* a copy of the FTC's *ID Theft Complaint* form (completed) with the FTC's Law Enforcement Cover Letter, which explains the necessity of a police report and an ID Theft Complaint.[25] The victim should ask the officer to attach or incorporate the ID Theft Complaint into the police report as the victim will need a copy of the "Identity Theft Report" (*i.e.,* the police report with the ID Theft Complaint attached or incorporated) to dispute fraudulent accounts and debts. A victim receives greater legal protection by filing a police report and obtaining an Identity Theft Report (*e.g.,* the Identity Theft Report can be used to: (1) permanently block fraudulent information from appearing on a victim's credit report; (2) ensure that debts do not reappear on the credit report; (3) prevent a company from continuing to collect debts that result from identity theft; and (4) place an extended fraud alert on the victim's credit report).

Second, the victim should contact the fraud department for any one of the three nationwide consumer-reporting companies—Equifax, Experian or TransUnion—to place a fraud alert[26] on his or her credit report.[27] Fraud alerts can help prevent an identity thief from opening any more accounts in the victim's name. Further, a fraud alert on a credit report will cause creditors to contact the individual prior to the opening of any new accounts or making

any changes to the individual's existing accounts. The contacted consumer-reporting company is required to contact the other two consumer-reporting companies, which should also place a fraud alert on the victim's credit report. However, if an identity theft victim does not receive a confirmation from a company, the victim should contact that company directly to place a fraud alert.

Once a fraud alert is placed on an individual's file, the individual is entitled to order one free copy of his or her credit report from each of the three consumer-reporting companies. The victim can ask that only the last four digits of his or her SSN appear on the credit report. Upon receiving the credit reports, the victim should review them carefully for fraudulent activity (*e.g.,* inquiries from companies they have not contacted, accounts they did not open, debts on their accounts they cannot explain, *etc*.). The victim should also check that information, like SSN, address(es), name or initials and employers are correct. If fraudulent or inaccurate information is found, the victim should request that the consumer-reporting companies remove it. When seeking to correct a credit report, to get the fastest and more complete results, a victim should provide a copy of his or her Identity Theft Report with a cover letter explaining the request. The victim should continue to check his or her credit reports periodically, especially for the first year after discovering the identity theft, to ensure no new fraudulent activity has occurred.

Third, an identity theft victim should close accounts that he or she knows or believes have been tampered with or opened fraudulently. The victim should call and speak with someone in the security or fraud department of each company. The victim should follow-up in writing and include copies of supporting documents. It is important to notify credit card companies and banks in writing. The letters should be sent by certified mail, return receipt requested, so the victim can document what the company received and when. If the identity thief has made charges or debits on the individual's accounts, or has fraudulently opened accounts, the victim should ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, a victim should request the company for its fraud dispute forms. If the company does not have special forms, the victim should write a letter disputing the fraudulent charges or debits and send it to the company at the address given for "billing inquiries," ***not*** the address for payments. The FTC website provides a sample dispute letter for existing accounts.[28]
- For new unauthorized accounts, a victim can either file a dispute directly with the company or provide a copy of their Identity Theft Report. The FTC website also provides a sample dispute letter for new accounts.[29]

Once an account has been closed, the victim should request a letter from the company confirming that the disputed account is closed and the fraudulent debts have been discharged. This letter is the victim's best proof if errors relating to this account reappear on his or her credit report or he or she are subsequently contacted about the fraudulent debt.

Fourth, an identity theft victim should file a complaint with the FTC using the online complaint form located at: www.ftc.gov/idtheft; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338). The FTC maintains a database of identity theft cases used by law enforcement agencies across the nation to track down identity thieves. In addition, the FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces. A victim should also call the FTC's Hotline to update the complaint if he or she has any additional information or problems.

Fifth, if a victim's tax records are not currently affected by identity theft, he or she should provide the IRS with proof of his or her identity by submitting a copy of a valid government-issued identification (*e.g.,* a Social Security card, driver's license or passport) along with a copy of a police report and/or a completed IRS Form 14039, *Identity Theft Affidavit*, which should be faxed to the IRS at 978-684-4542. A taxpayer can also contact the IRS Identity Protection Specialized Unit at 800-908-4490. If a taxpayer believes that his or her personal information has been stolen *and* used for tax purposes, he or she should immediately contact the IRS Identity Protection Specialized Unit. A taxpayer's identity may have been stolen if the IRS sends a letter or notice indicating that: more than one tax return was filed for the taxpayer; the taxpayer has a balance due, refund offset or collection action is being taken against the taxpayer for a year he or she did not file a return; or the taxpayer received wages from an employer he or she has not worked for. If a taxpayer receives communication from the IRS indicating identity theft, he or she should respond immediately to the name, address or phone number on the IRS letter and follow the instructions in the letter or notice.

C. Organizations and Tax Professionals Also Need to Take Protective Measures to Protect Their Clients' Personal Information

Identity theft does not apply only to individuals. There have been reported instances where company and benefit plan identities have been stolen. Tax professionals should keep in mind that they have taxpayer information that would be very useful to thieves. Make sure you have appropriate security protocols built into your electronic systems and administration process to avoid being a source of information that thieves can use to steal taxpayer's identities.

Statutory rules, as well as accounting and attorney legal and ethical guidelines, govern the handling of taxpayer information. For instance, the knowing or reckless disclosure or use by a tax return preparer of information obtained in preparing a return is a misdemeanor pursuant to Code Sec. 7216.[30] For purposes of Code Sec. 7216, return preparers include not just persons in the business of preparing returns, but also those who provide auxiliary services in connection with the preparation of tax returns. Tax return preparers may also be subject to the privacy provisions of the Gramm-Leach-Bliley Act (P.L. 106-02), which imposes requirements on financial institutions to protect personal information. The American Institute of Certified Public Accountants (AICPA) provides additional background and useful information about the Gramm-Leach Bliley Act. [31] The AICPA has recently published an alert on its website that it too was a target of a fraudulent email phishing scam that was sent to numerous individuals, CPAs, non-CPAs and members of the general public.[32]

Professionals such as attorneys and accountants have ethical and legal guidelines that keep them from using or disclosing information to their own advantage or their clients' disadvantage. For instance, Rule 1.6 of the Model Rules of Professional Conduct addresses the confidentiality of client information and states that a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent. Similarly, disclosure of confidential client information without the permission of a client is prohibited by the California Rules of Professional Conduct, Section 54.1.[33] Additionally, the AICPA provides useful information for firms implementing policies to safeguard taxpayer data.[34] Other than highlighting these examples of duties and obligations of tax professionals with respect to confidential information, this article focuses on the consequences that can occur when private information arrives in the hands of identity thieves.

In IRS Publication 4557, *Safeguarding Taxpayer Data*, the IRS sets forth some best practices for handling taxpayer information. A starting point to implement some of these best practices is to assess the risks that are present in your office or offices. This includes evaluating your operations, physical environment, computer systems and employees. Assess where you keep information, whether it is files on site, files stored remotely in storage, computers, laptops or any other forum. Some simple securities controls, such as locking doors, creating more complicated passwords, encrypting data and shredding certain records, can reduce opportunities for client information to be stolen.

Another best practice is to write a plan for safeguarding taxpayer information, placing appropriate safeguards in place and then assigning responsibility to these safeguards to an individual or individuals in the firm or business. Of course, these safeguards need to be monitored, evaluated and adjusted as your business grows or changes. Additionally, use only other service providers who have policies in place to also maintain an adequate level of information protection.

While some of these safeguards are common sense, or mirror the suggestions above for individuals protecting their own data, a disciplined policy for safeguarding taxpayer data can reduce privacy-related risks[35] in your practice and protect your clients at the same time.

Endnotes

1 IRS News Release, IR-2012-23, Feb. 16, 2012.

2 *Id.*

3 *IRS faces surge in identity theft tax fraud,* MSNBC.com (2/17/12), http://lifeinc.today.msnbc.msn.com/_news/2012/02/17/10428874-irs-faces-surge-in-identity-theft-tax-fraud?chromedomain=usnews???

4 Written Testimony of Steven T. Miller, Deputy Commissioner for IRS Services and Enforcement before the House Committee on Oversight and Government Reform Subcommittee on Government Organization, Efficiency and Financial Management On Identity Theft, Nov. 4, 2011, at 3.

5 *Id.*

6 GAO, *Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers,* GAO-11-721T, at 4 (Washington, D.C.: Jun. 2, 2011).

7 *Id.* at 10.

Endnotes

[8] *IRS faces surge in identity theft tax fraud,* MSNBC.com (2/17/12), http://lifeinc.today.msnbc.msn.com/_news/2012/02/17/10428874-irs-faces-surge-in-identity-theft-tax-fraud?chromedomain=usnews???

[9] Written Testimony of Steven T. Miller, Deputy Commissioner for IRS Services and Enforcement before the House Committee on Oversight and Government Reform Subcommittee on Government Organization, Efficiency and Financial Management On Identity Theft, Nov. 4, 2011, at 1.

[10] *Id.,* at 5.

[11] IRS News Release, IR-2012-13, Jan. 31, 2012.

[12] *See* Internal Revenue Manual section 9.5.3.3.11.1.

[13] *See* Code Sec. 6103.

[14] GAO, *Tax Administration: IRS Has Implemented Initiatives to Prevent, Detect, and Resolve Identity Theft-Related Problems, but Needs to Assess Their Effectiveness,* GAO-09-882, Appendix II (Washington, D.C.: Sep. 2009).

[15] GAO, *Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers,* GAO-11-721T, at 6 (Washington, D.C.: Jun. 2, 2011).

[16] Written Testimony of Steven T. Miller, Deputy Commissioner for IRS Services and Enforcement before the House Committee on Oversight and Government Reform Subcommittee on Government Organization, Efficiency and Financial Management On Identity Theft, Nov. 4, 2011, at 7.

[17] *Id.*

[18] The IRS does, however, conduct customer satisfaction surveys by telephone, by mail and online to capture taxpayer and tax practitioner opinions. IRS surveys you receive in the mail will provide an Office of Management and Budget (OMB) number. IRS surveys conducted by telephone and online will provide an IRS contact person if you wish to verify the authenticity of the survey. Also, an IRS survey will never ask you for personal identifying information such as your social security number or financial information. http://redtape.msnbc.msn.com/_news/2012/02/22/10471719-survey-id-theft-on-the-rise-again-card-victims-jump-by-2-million-annually.

[19] The IRS participates on the following social media platforms:
- YouTube: The IRS has video channels that provide short, informative videos on various tax related topics in English, American Sign Language (ASL) and a variety of foreign languages;
- Twitter: IRS tweets include various tax-related announcements, news for tax professionals and hiring initiatives; and
- Facebook: IRS has Facebook pages that post valuable tax information for tax professionals and those needing help in resolving long-standing issues with the IRS.

[20] Smartphone users are approximately 30 percent more likely to report being hit by ID fraud. 62 percent say they do not use a screen password to protect their devices. http://redtape.msnbc.msn.com/_news/2012/02/22/10471719-survey-id-theft-on-the-rise-again-card-victims-jump-by-2-million-annually.

[21] *Id.*

[22] *Id.*

[23] The Federal Fair Credit Reporting Act requires each of three nationwide consumer-reporting agencies to provide individuals with a free copy of their credit reports, at their request, once every 12 months. In addition, under federal law, individuals are entitled to a free report if a company takes adverse action, such as denying an individual's application for credit, insurance or employment, and they request the report within 60 days of receiving notice of the action. The notice will provide the name, address and phone number of the consumer-reporting agency that supplied the information.

[24] Roughly 15 percent of adults in the United States say they received a data breach notification in 2011 from a company indicating it had lost their personal information. Those who say they received such a notice were more than nine times as likely to also report being fraud victims. Despite these statistics, many consumers do not sign up for free credit-monitoring services when companies that have leaked data offer them. http://redtape.msnbc.msn.com/_news/2012/02/22/10471719-survey-id-theft-on-the-rise-again-card-victims-jump-by-2-million-annually.

[25] The FTC ID Theft Complaint for and the Law Enforcement Cover Letter can be obtained from the FTC's website at: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html.

[26] There are two types of fraud alerts: an initial alert and an extended alert. An initial alert stays on an individual's credit report for at least 90 days. An initial alert is appropriate where an individual's wallet has been stolen or he or she has responded to a phishing scam. An extended alert stays on a credit report for seven years. An extended alert is placed on a credit report if an individual is the victim of identity theft and provides the consumer-reporting company with an Identity Theft Report. If an extended alert has been placed on a credit report, the individual is entitled to two free credit reports within 12 months from each of the three consumer-reporting companies. In addition, the companies will remove the individual's name from marketing lists for pre-screened credit offers for five years unless the individual requests to be placed back on the list.

[27] Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241. Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9554, Allen, TX 75013. TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

[28] The link to the "SAMPLE DISPUTE LETTER FOR EXISTING ACCOUNTS" can be found at: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html.

[29] The link to the "SAMPLE DISPUTE LETTER FOR NEW ACCOUNTS" can be found at: http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html.

[30] 16 Cal. Cod. Reg. 54.11.

[31] http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/FederalStateandOtherProfessionalRegulations/GrammLeachBlileyAct/Pages/default.aspx.

[32] http://www.aicpa.org/News/FeaturedNews/Pages/alert-fraudulent-email.aspx.

[33] Code Sec. 7216(a); Reg. §301.7216-1(a).

[34] http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/FederalStateandOtherProfessionalRegulations/Pages/SafeguardingTaxpayerData.aspx.

[35] See Frequently Asked Questions about Privacy Services published by the AICPA http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/privacyservices/pages/frequently%20asked%20questions%20about%20privacy%20services.aspx.