Tax-Related Identity Theft

By Sharyn M. Fisk and Cory Stigile

THE INTERNAL REVENUE SERVICES IS combating a huge increase in incidents of tax-related identity theft. During the first nine months of 2012, the IRS identified approximately 642,000 instances of tax-related identity theft—more than double the number for all of 2011.[1] Identity theft is at the top of the IRS's annual "Dirty Dozen" list of tax scams.[2]

There are three major forms of tax identity theft: the filing of false refund claims using a legitimate taxpayer's name and Social Security number (SSN); employment tax fraud; and using the IRS name to steal identities through phishing[3], malware[4] and other means. The most common type of tax-related identity theft, and the focus of this article, is the filing of fake returns claiming refunds.

To file a fake return, an identity thief uses a legitimate taxpayer's name and SSN on a tax return seeking a refund early in the filing season before the legitimate taxpayer files his or her actual return and before the IRS conducts its first matching of W-2 information with taxpayer SSNs. If the IRS determines the name and SSN on the tax return are valid (the IRS checks all returns to see if filers' names and SSNs match before issuing refunds) and it passes through the IRS' other filters, the IRS will issue the refund to the thief. The thief requests that the refund be paid out to a debit card or direct deposit to a checking account that is then promptly emptied. The legitimate taxpayer may not be aware he or she has become a victim until filing his or her own return and receiving a letter from the IRS stating that more than one tax return was filed with their information.

In 2004, the IRS developed a strategy to address the problem of identity theft-related tax administration issues. This strategy, while still evolving, 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.

Fraud Prevention

Beginning in 2011, the IRS launched the Enhanced Return Processing Program. Under this program, a cross-functional group was formed made up of various IRS divisions that work to develop enhanced revenue protection processes and policies beginning with the 2012 filing season. The IRS has committed more than 3,000 employees to identify and address theft issues through the use of filters to screen for potential identity theft tax fraud; the use of Identity Protection Personal Identification Numbers (IP PINs); updated registries of deceased taxpayers and prisoners; and increased focused by the IRS Criminal Investigation Division.

On average, the IRS processes more than 100 million income tax refunds each year. It has implemented screening filters to improve its ability to spot false returns before they are processed and before refunds are issued. During the 2012 fiscal year, the IRS prevented $20 million in tax refunds from going to criminals—up from $14 million in 2011.[5] Given the number of changes that many taxpayers experience in a year, it is a challenge for the IRS to develop effective filters. Until optimal filters are in place, the current filters may cause delays as refund claims for more taxpayers get extra screening prior to the issuance of the refund.

The IRS has also recently begun issuing special IP PINs to taxpayers whose identities are suspected of or known to have been stolen, to facilitate the filing of their returns and to prevent others from utilizing their identities on future returns. Taxpayer use of IP PINs is more fully described below.

The agency is currently 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 individuals. Until recently, Ancestry.com reported the SSNs of deceased individuals. But after being alerted to the problem of identity theft, the company changed this practice with respect to individuals who have died in the past 10 years.[6]

The IRS is expanding its successful 2010 pilot program of marking the accounts of deceased taxpayers to prevent misuse by identity thieves. Currently, the IRS has marked 230,000 accounts of decedents. In addition, the agency is working with the Social Security Administration (SSA) to improve the utilization of the information the SSA makes available to the IRS. It is also expanding the use of its list of prisoners to stop problematic returns. In 2011, the IRS received additional help under the United States-Korea Free Trade Agreement Implementation Act which included language requiring federal and state prisons to provide information on the current prison population.

The IRS' Criminal Investigation (CI) Division has increased its efforts as a fraud prevention measure. Within the last year, in conjunction with the Department of Justice (DOJ) and the U.S. Attorney's offices, the CI Division has conducted 734 enforcement actions against 389 suspects in 32 states and Puerto Rico. Currently, the CI Division has four Scheme Development Centers (SDCs) across the United States whose primary mission is to detect refund fraud.

These SDCs have uncovered numerous identity theft-related schemes. These schemes are forwarded to one of CI Division's 26 field offices for criminal investigation

and/or its civil counterparts to resolve victim accounts. After the CI Division conducts its investigation, it recommends prosecution, when appropriate, to the DOJ.

The CI Divisions also work with other federal, state and local law enforcement agencies on joint investigative efforts involving identity theft tax fraud (e.g., the CI Division 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.[7]

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 from fraud, while also maintaining its duty to issue refunds to taxpayers 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.[8]

Taxpayer Assistance

The IRS has implemented several initiatives to detect and assist the taxpayer in resolving tax-related identity theft, including account indicators, IP PINs, employee training and taxpayer outreach and education.

The IRS has implemented the use of "indicators" to detect and resolve identity theft.[9] Different indicators are used depending on the circumstances by which the IRS receives an indication of an identity theft–related problem.[10] Once the IRS substantiates any taxpayer-reported information, it places the appropriate indicator on the taxpayer's account and notifies the taxpayer. 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 with account access. Thus, the taxpayer is relieved of having to repeatedly explain their identity theft issues or prove their 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. After three consecutive years of no identity-theft incidents on a taxpayer's account, the IRS will remove an indicator or the taxpayer can request that it be removed sooner.

In January 2011, the IRS began piloting an IP PIN program aimed at cutting repeat fraud for taxpayers who have been victims of identity theft. Taxpayers who have been victims of identity theft will receive an IP PIN to verify their identities at the time they file their return. The IRS will only process a return containing the IP PIN and reject any return filed without it. The agency intends to send a new IP PIN annually to the affected taxpayer. It has issued IP PINs to over 50,000 taxpayers who have been victims of identity theft and anticipates issuing more than 200,000 for the 2012 filing season.[11]

As another measure to improve taxpayer assistance, 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.[12] The agency has specifically updated the training course for its telephone representatives to ensure they maintain the proper level of sensitivity and understand the serious financial problems that identity theft poses for these taxpayers. The agency 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.

In an effort to improve taxpayer outreach and education, the IRS created a new section on its website dedicated to identity theft matters.[13] This section provides guides, videos, podcasts and news regarding identity theft as well as links to other agencies that address identity theft (e.g., the FTC). It also includes contact information for the IRS' Identity Protection Specialized Unit where taxpayers can receive assistance in resolving identity theft issues with the IRS.

What Tax Professionals and Taxpayers Can Do to Prevent Identity Theft

There are numerous precautions both tax professionals and taxpayer can take to avoid having confidential private information from being stolen.

Protective Measures by Tax Professionals

Statutory rules, as well as accounting and attorney legal and ethical guidelines, govern the handling of taxpayer information. For example, the knowing or reckless disclosure or use by a tax return preparer of information obtained in preparing a return is a misdemeanor pursuant to IRC §7216.[14] Per §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, PL 106-02, 11/12/99, 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.[15]

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. 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 §54.1.[16] Additionally, the AICPA provides useful information for firms implementing policies to safeguard taxpayer data.[17] IRS Publication 4557, *Safeguarding Taxpayer Data*, sets forth some best practices for handling taxpayer information.

A starting point is to assess the risks that are present in the attorney or tax professional's office. This includes evaluating the operations, physical environment, computer systems and employees. Assess where you keep information, whether it is physical files onsite or stored remotely in storage or electronic files on networks, computers, laptops or other forums. 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.

If employees can work remotely from home, their home computers should have the same protections as their work computers. Care also should be taken with respect to using file-sharing programs. In addition, simple security controls, such as locking doors, creating more complicated passwords, encrypting data and shredding records, can reduce opportunities for client information to be stolen.

While some of these safeguards are common sense, a disciplined policy for safeguarding taxpayer data can reduce privacy-related risks in your practice and protect your clients at the same time.[18] Write a plan for safeguarding taxpayer information, placing appropriate safeguards in place, then assign responsibility for these safeguards to an individual or individuals in the firm or business. These safeguards need to be monitored, evaluated and adjusted as your business grows or changes. Additionally, use only service providers who have policies in place to also maintain an adequate level of information protection.

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

Proactively Minimizing Taxpayers Risk

There are several ways a taxpayer can minimize the risk of becoming a victim of identity theft. Most importantly, individuals should protect their computers—and their smartphones[19]—by using anti-spam/virus software, updating security patches and firewalls and employing sufficiently complicated passwords. Virus protection software should be set to automatically update each week. An individual should not open files or click on hyperlinks or download programs from questionable emails that may contain malware or viruses that could infect their computer. Individuals should also avoid phishing schemes purporting to be from the IRS[20] or release financial information over the internet.[21]

Care also should be taken with respect to using file-sharing programs. If a person is using a high-speed internet connection that leaves their computer constantly connected to the internet (e.g., cable), they should use a firewall program to stop uninvited access to their computer. Without it, hackers can access personal information stored on the computer or use it to commit other crimes

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

Steps an Identity Theft Victim Should Take

If a taxpayer's identity has been stolen, prompt and thorough actions must be taken to minimize the damage and speed the recovery of the theft.

A victim of identity theft should first complete the FTC's *ID Theft Complaint* form.[22] 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 and can investigate companies for violations of laws the agency enforces. Be sure to follow the directions on the ID Theft Complaint form and be as detailed as possible in completing the form. Once complete, the victim should file the ID Theft Complaint form with the FTC. A victim should also call the FTC's hotline to update their complaint if they have any additional information or problems.

An identity-theft victim should also contact their local police or sheriff's department to file a report of identity theft. It is important to document the theft at an early stage in order to obtain greater legal protection.[23] Bring supporting documentation of the identity theft and a copy of the completed *ID Theft Complaint* form along with the FTC's *Law Enforcement Cover Letter* explaining the necessity of a police report.[24] 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 obtaining an Identity Theft Report.[25]

Of course, a victim should contact the fraud department of one of the three nationwide consumer-reporting companies—Equifax, Experian or TransUnion—and request a fraud alert[26] be placed on their 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 other credit reports. 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. Victims should keep a record with the details of their conversations and copies of all correspondence with enclosures.

The victim should also request a copy of their credit report from each of the three consumer-reporting companies.[28] A victim should review the reports carefully for

fraudulent activity and to verify that all personal information reported is accurate (e.g., SSN, address, name and initials, employers, etc.). 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, a victim should provide a copy of their Identity Theft Report with a cover letter explaining their request. The victim should continue to check their credit reports periodically, especially for the first year after discovering the identity theft, to ensure no new fraudulent activity has occurred.

An identity theft victim should close accounts known or believed to be tampered with or opened fraudulently. He or she should speak with someone in the security or fraud department of each company and follow-up in writing. Letters should be sent by certified mail, return receipt requested, so the victim can document the correspondence. 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 fraudulent charges or debits on existing accounts, a victim should request the company send its fraud dispute forms. If the company does not have special forms, 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.[29] For new unauthorized accounts, the identity theft victim should file a dispute directly with the company or provide a copy of the Identity Theft Report to the company.[30]

Once an account has been closed, a 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 if he or she is subsequently contacted about the fraudulent debt.

If a victim's tax records are not currently affected by identity theft, they can still contact the IRS Identity Protection Specialized Unit[31] and request an IP PIN. The victim will need to provide the IRS with proof of identity (e.g., a Social Security card, driver license or passport) along with a copy of a police report and/or a completed IRS Form 14039, *Identity Theft Affidavit*.[32]

If a taxpayer believes that their personal information has been stolen and used for tax-related fraud, they should immediately contact the IRS Identity Protection Specialized Unit. A taxpayer's identity may have been stolen if the IRS sends them 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 taken against the taxpayer for a year they did not file a return; or wages were reported to the IRS by an employer the taxpayer did not worked for. If a taxpayer receives communication from the IRS indicating identity theft, they should respond immediately to the name, address or phone number on the IRS letter and follow the instructions in the letter or notice.

---

[1] GAO, *Identity Theft: Total Extent of Refund Fraud Using Stolen Identities is Unknown*, GAO-13-132T (Washington, D.C.: Nov. 29, 2012).
[2] IR-2012-23, *IRS Releases the Dirty Dozen Tax Scams for* 2012, Feb. 16, 2012.
[3] "Phishing" is the act of sending an e-mail under the auspices of a legitimate enterprise in an attempt to "lure" the recipient into surrendering private information.
[4] "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.
[5] Comments of acting IRS Commissioner Miller, *Miller Hails Identity Theft Crackdown, But Olson Critiques Victim* Assistance, Tax Notes Today, 2013 TNT 27-4 LEXIS (2/8/13).
[6] *IRS faces surge in identity theft tax fraud*, MSNBC.com (2/17/12), *http://lifeinc.today.com/_news/2012/02/17/10428874-irs-faces-surge-in-identity-theft-tax-fraud?lite*
[7] See I.R.C. §6103.
[8] "The IRS cannot stop all identity theft. However, we are committed to continuing to improve our programs." 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, pg. 1 (Nov. 4, 2011).
[9] 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 (Washington, D.C.: Sep. 2009).
[10] GAO, *Taxes and Identity Theft: Status of IRS Initiatives to Help Victimized Taxpayers*, GAO-11-721T (Washington, D.C.: Jun. 2, 2011).
[11] 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, pg. 7 (Nov. 4, 2011).
[12] 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).
[13] See www.IRS.gov/identitytheft.
[14] 16 Cal. Cod. Reg. 54.11.
[15] http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/FederalStateandOtherProfessionalRegulations/GrammLeachBlileyAct/Pages/default.aspx
[16] IRC §7216(a); Reg §301.7216-1(a).
[17] http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/FederalStateandOtherProfessionalRegulations/Pages/SafeguardingTaxpayerData.aspx
[18] 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
[19] 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.
[20] Promptly report suspicious e-mails 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 e-mail to:* phishing@irs.gov and to the FTC at spam@uce.gov. The IRS can use the information, URLs and links in suspicious e-mails forwarded to them to trace the hosting website and alert authorities to shut down the fraudulent sites.
[21] 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. The IRS does conduct customer satisfaction surveys by telephone, mail and online to obtain taxpayer and tax practitioner opinions. However, IRS surveys received via mail contain an Office of Management and Budget (OMB) number. IRS surveys conducted by telephone and online provide an IRS contact person so the authenticity of the survey can be verified. An IRS survey will never ask for personal identifying information such as a 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
[22] The form is available online at www.ftc.gov/idtheft or via telephone at the FTC's Identity Theft Hotline: 1-877-ID-THEFT (438-4338).
[23] 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). Check with the state Attorney General's office to find out if state law requires the police to take reports for identity theft.
[24] The FTC ID Theft Complaint Form and the Law Enforcement Cover Letter can be obtained from the FTC's website at: http://www.consumer.ftc.gov/articles/0281-sample-letters-and-forms-victims-identity-theft
[25] 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).
[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 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. The companies will also 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 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 (e.g., denying an 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. 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.
[29] FTC provides a sample dispute letter for existing accounts entitled "Ask a Business to Remove Fraudulent Charges From Your Existing Accounts" located at: http://www.consumer.ftc.gov/articles/0282-ask-business-remove-fraudulent-charges-your-existing-accounts
[30] FTC provides a sample dispute letter for existing accounts entitled "Ask a Business to Close a New Account Opened in Your Name" located at http://www.consumer.ftc.gov/articles/0283-ask-business-close-new-account-opened-your-name.
[31] The IRS Identity Protection Specialized Unit can be reached at (800)908-4490.
[32] The completed IRS Form 14039, *Identity Theft Affidavit,* should be faxed to the IRS at (978)684-4542.

Sharyn M. Fisk is a Principal at Hochman, Salkin, Rettig, Toscher & Perez, P.C., a California State Bar Certified Specialist in Taxation Law and a Professor at the College of Business and Economics at CSUN. She can be reached at sf@taxlitigator.com. **Cory Stigile** is a Principal at the firm specializing in tax controversies. Mr. Stigile is also a CPA licensed in California. He can be reached at stigile@taxlitigator.com.