www.taxpreparerconnections.com

20 Steps to Prevent Tax Refund and ID Theft

Protect your clients AND your practice from attacks

By Jon A. Hayes, TaxPreparerConnections.com

A silent epidemic is sweeping the tax system, and it appears the Internal Revenue Service cannot stop its spread.

It's called tax refund theft, and it is a billion-dollar business. For the 2013 tax year, the IRS reported that 2.2 million fraudulent returns were filed, with 940,000 involving identity theft. Thieves literally stole $6.5 billion in fraudulent refunds. According to an internal government report, the IRS missed another 1.5 million bogus returns with fraudulent refunds potentially exceeding $5.2 billion.

That's nearly $12 billion dollars. The IRS estimates the overall loss will grow 5 to 7 percent in each of 2014 and 2015.

The problem intensified early in the 2012 season, forcing the IRS to shut down refunds temporarily as they implemented additional security protocols into their system. The Tampa Bay Tribune reported that thieves were actually giving classes on how to file false returns and estimated total fraud in the Tampa area at $1 billion. News agencies have reported the wholesale identity theft of over 80 percent of residents in a nursing home facility, fraudulent theft of corporate identification numbers leading to massive filing of false W-2s and 1099s, and fraudulent returns filed on behalf of people who applied for credit with several agencies.

Even worse, the IRS has received over 120,000 phone calls reporting identity theft in 2013, with less than 25 percent of the calls answered timely by the Service.

The typical tax refund fraud case involves using a deceased person's name and a stolen social security number from a child or elderly dependent – considered the easiest targets. The thieves typically file fraudulent returns early in the tax-filing season before the IRS has received W-2 or 1099 information. Then, when the legitimate taxpayers file their returns later in the tax season, the IRS notifies them that they are attempting to file a duplicate return. While the duplicate filing issue can be resolved fairly easily by filing an originally signed paper copy with the IRS, there have been delays of as long as four months in legitimate taxpayers receiving their refunds.

For the 2012 filing season, the IRS issued 250,000 Identity Protection Personal Identification Numbers (IP PINs) to taxpayers whose identities are known to have been stolen.

The IRS continues to work on the problem by addressing areas of weakness in the tax-reporting process that are exploited. IRS Notice 2011-38 now allows anyone filing a W-2 or 1099 to truncate Social Security numbers on information returns to make it much more difficult for thieves to obtain SSNs. The IRS has also stopped placing

full Social Security numbers on some taxpayer notices and is testing a barcoding system as the means of identifying taxpayers in correspondence.

Unfortunately, there are still many taxpayers who fall for email phishing scams and bogus websites, which are designed to steal their information. Tax preparers can use this helpful IRS resource page to educate their clients on how to avoid identity theft, and if victimized by it, how to resolve it:

http://www.irs.gov/privacy/article/0,,id=249929,00.html

Immediate Steps to Take When You Discover Client Identity Theft

If you suspect or uncover identity theft or tax refund theft with a client, you must move swiftly to minimize the damage. Be sure to bookmark these pages on identity theft so you can provide your clients with the information needed to report and stop the crime with the IRS (we've included Michigan information for our IAAM members):

IRS - Identity Theft Information for Tax Preparers

IRS - Identity Theft Prevention Detection and Assistance

Michigan - I believe I am a Victim of Identity Theft
Email: **Treasury-ReportIDTheft@michigan.gov**
Telephone: **517-636-4486**

10 General Things Your Clients Should be Aware of to Avoid Identity Theft

1. Do not click on any links, open or respond to any email that claims to be from the IRS. The IRS **never** initiates correspondence via email.

2. Install and maintain a powerful anti-virus and firewall software system. Good anti-virus and firewall programs are Panda Cloud Antivirus (free) or Webroot Antivirus with SpySweeper (about $39), and Comodo Firewall Pro 3.0 (free).

3. Review your credit report annually and block it from new credit requests if acceptable. It is available annually for free at www.annualcreditreport.com or 877-322-8228.

4. Do not give anyone your social security number under almost any circumstances.

5. Destroy (shred) any old checks reflecting your social security number.

6. Buy and use a home shredder to shred all personally identifiable documents at all times.

7. Never, ever give personally identifiable information over the telephone unless you are absolutely certain of the identity and need of the other party. If you have ANY doubt, don't provide the information.

8. Secure all electronic files and paper files from intruders, children and outsiders.

9. Carefully guard against filling out any online forms and do not open accounts with anyone who requires social security numbers online.

10. Because the National Master Death list is public information (with Social Security numbers), file returns as soon as possible for decedents.

Additional Steps to Take if You Suspect Identity Theft

If you or your client suspects identity theft, contact the fraud departments at any of these major credit bureaus to begin the process of stopping the theft:

1. Equifax – www.equifax.com 1-800-525-6285
2. Experian – www.experian.com 1-888-397-3742
3. TransUnion – www.transunion.com 1-800-680-7289

What Tax Professionals Can Do to Prevent Identity Theft

Many firms are sitting on a powder keg of liability due to current practices. Prevention starts at the firm level. Be sure to review **IRS Circular 230** for guidance on how to avoid any issues and to better understand required confidentiality rules and preparer penalties for failure to comply with them.

Follow these 10 steps to protect your office and clients against identity theft:

1. Develop, discuss and immediately implement a written firm confidentiality policy. Here's a good website to guide you: **http://www.wbsonline.com/resources/your-confidentiality-policy/**

2. Immediately implement a policy of cleaning off desks and putting client information away in a secure area every night, and consistently enforce the policy.

3. Require that all client information be secured out of sight of anyone.

4. Install heavy duty shredders at several locations in the office.

5. Never e-mail a client any confidential tax information without password protection. This is a direct violation of Circular 230.

6. Hard drive data must be encrypted.

7. Computers should be re-booted at lunch and never ever left on at night or around cleaning crews or outsiders.

8. Passwords must be required to login to idle computers.

9. Physical security of client data should be required behind locked doors, cabinets and file rooms at night or when the office is closed.

10. A firm wide internet and computer usage policy must be in place and enforced. Here's a link to a sample policy you can customize: **http://www.twc.state.tx.us/news/efte/internetpolicy.html**

How to Service Clients in Identity Theft Cases

Implement this easy-to-follow system:

Step 1: Confirm the identity theft.

For a refund identity theft, the cause is simple to confirm because a return was filed under your client's SSN. If your client received a notice or a refund offset in a following year, you will have to investigate further.

You can call the **IRS Practitioner Priority Service line at (866) 860-4259** with a **Power of Attorney (Form 2848)** or **Tax Information Authorization (Form 8821)** to get your client's account information. Request return transcripts, account transcripts, and wage and income transcripts for the past three years and verify the information against your client's filed return. You will be able to quickly identify information statements that were not your client's, and identify whether someone has filed under your client's SSN.

It is important that you report any identity theft to the IRS if the theft compromised your client's tax information. For example, if your client's Form W-2 was sent, but your client did not receive it, you may want to consider whether it ended up in the hands of an identity thief. The thief could file a return, claim deductions and try to obtain a fraudulent refund. The conservative approach: Any time a client's identifying information is compromised, consider reporting it the IRS.

Step 2: Report the identity theft.

Contact the IRS IPSU at **(800) 908-4490** to report identity theft. Keep in mind that the IPSU only monitors victims' accounts; it does not resolve identity theft cases. If your client's situation involves a post-filing issue, the IRS compliance function that issued the notice is responsible for clearing up the identity theft. If there is a hardship or any confusion about how the IRS is handling your client's situation, contact the IRS Taxpayer Advocate Office. Download **Form 14039, *IRS Identity Theft Affidavit***, and be prepared to present that information to the IRS on the phone. The IRS will put an identity theft indicator on your client's account.

Remember, if you are going to call on behalf of your client, you will need a Power of Attorney, Form 2848.

Step 3: Document the theft to the IRS.

You will need to prove your client's identity to the IRS. If your client's return was rejected, file a paper return with **Form 14039** and attach proof of your client's identity (such as a copy of your client's driver's license, Social Security card or passport). The IRS will take several months to sort out the correct return and issue any refund. Keep your client's documentation handy. The IRS does not assign one person to your client's account, and it's often necessary to resend information.

If the identity theft is a post-filing issue (for example, a CP2000 underreporter inquiry, refund offset, audit, or collection letter resulting from a return filed by an identity thief), fax **Form 14039** and attachments to the compliance unit assigned to your client's case.

Again, if there is a hardship or impending adverse action, contact your client's local Taxpayer Advocate Office.

When the identity theft is confirmed, the IRS will put an identity theft indicator on your client's account. Later in the year, the IRS will also send your client an Identity Protection Personal Identification Number (IP PIN) to use to file his or her return. For the next three years, the IRS will reissue a new IP PIN in December. The IP PIN and identity theft indicator will automatically expire in three years if no threat to identity security exists.

Step 4: Resolve resulting issues.

The IRS requires the IP PIN to process future returns. If the identity theft was detected after your client filed the return, you may have to help your client with resulting problems.

Many post-filing problems are found in automated underreporter notices (CP2000). These notices propose additional taxes from unreported information statements. Other common notices involving identity theft are refund offsets and collection notices. In dealing with these identity theft cases, you may need the IRS to halt the automated notice stream to avoid premature assessments or collection actions. Request these extensions early,

and be prepared to follow up often to request additional extensions as needed. Remember, clearing up identity theft at the IRS may take some time. IRS systems generally cannot give collection extensions past four months. Follow up is essential to avoid systematic, premature IRS actions.

Additional Tips

- When in doubt, if your client is a victim of any form of identity theft, file **Form 14039** with the IRS by faxing it to (978) 684-4542.

- Consider going straight to the **Taxpayer Advocate Office**, which can cut through red tape concerning identity theft issues. When doing so, visit a local office to get the most expedited consideration.

- Prepare your client for a process that could take several months and incur substantial fees from your services. If your client has credit repair insurance from a credit monitoring company, ask your client to request that the insurance pay for the costs of repair.

Implement a Simplified ID Theft Information Service

IF You Don't Want to Use a comprehensive protection, you can implement an informational service on your own in the following possible ways:

1. Create an Identity Theft Helpline AND charge for the service, whether it's a nominal hourly rate or a onetime charge to do "x" things only. Post it to your website and include it in your rate sheet and other marketing materials. We've given you the four step process to help a client stop identity theft. All you have to do is decide what you will do and how much you will charge to do it.

   HINT: If you choose NOT to charge directly for the service, you could "tie" it into a tax preparation agreement and related services agreement with new clients by requiring the agreement in exchange for providing the service and then choosing to build the cost into the preparation rate schedule.

2. Copy and paste the "10 things a client can do to prevent ID theft" to your website. We suggest you create an identity theft section on your website and copy and paste any or all of the information in this white paper to it.

   HINT: You could develop a "Do-it-yourself" checklist for clients if they balk at paying you for your services. For example, don't provide any of the service checklist you can follow but simply provide general information. If you're smart in developing a DIY service, you'll paint a bleak picture for success without your help, especially when the theft has been financially painful and threatens to continue.

   ANOTHER HINT: The "10 Things a Practitioner Can Do to Prevent Identity Theft" can be easily tweaked to say "10 Things a SMALL BUSINESS Can Do to Prevent Identity Theft." You could post this to your website and/or include it in a special correspondence to your small business clients (along with your new ID Theft Service information of course).

Above all, remember that tax refund theft and identity theft are the fastest growing crimes in the world today. ANYTHING you can do to help clients minimize their potential exposure or deal with a theft is a BONUS for them . . . and your tax practice.