

AMERICA'S LEADING IDENTITY RESOLUTION AND EDUCATION SERVICE

THIS MONTH'S TOPIC...

Tax Fraud:

When the IRS Sees Double

This tax season, taxpayers expecting handsome refund checks aren't the only ones who become more diligent and focused. Between January and April, opportunity is ripe for tax-specific identity fraud. These schemes involve con artists and thieves who cash in on a person's tax-filing obligation, or phishers who try to pass themselves off as IRS representatives or legitimate tax preparers. In this month's newsletter, "[Tax Time Perfect For Identity Scammers to Strike](#)," Identity Theft 911 fraud specialists talk about these risks, and what consumers can do to mitigate them.

Unfortunately, it isn't just the money-hungry scammers who cause confusion with the IRS. In some cases, an individual will use someone else's Social Security number to secure employment, leaving victims and tax officials with the onerous task of trying to separate the fraudulent from the legitimate. As the April 15 tax deadline approaches, it's a good time to consider [tips](#) that will help consumers avoid future headaches.

For a complete newsletter archive, visit: www.identitytheft911.org/newsletters
To learn about the latest scams on identity theft, visit: www.identitytheft911.org
Comments, questions? Contact us: newsletter@identitytheft911.com





TAX TIME PERFECT FOR IDENTITY SCAMMERS TO STRIKE

FRAUD EXPERTS CAUTION TAXPAYERS
ON IDENTITY THEFT SCHEMES

In 2007, Bill and Sue, a married couple from the Midwest, were anxiously anticipating their federal tax refund. They had filed jointly and, between their combined incomes and deductions, were expecting a sum in excess of \$25,000. Soon, though, thoughts on how to best invest or spend the money gave way to concern over where it actually was. The check never showed up.

They contacted the IRS and discovered why: fraud. Someone had already filed a return in Sue's name, and their paperwork had been forwarded to an IRS department responsible for handling possible identity-theft situations. Eight months later and still waiting, Bill and Sue got in touch with Identity Theft 911 fraud specialist Mark Fullbright through their financial institution. "They really didn't know when it was going to come in," Fullbright says. "They just kept getting letters telling them it was going to be another 45 days." ▶

Fullbright has seen this scam before, in which one person files a tax return using someone else's name and Social Security number. In Bill and Sue's case, Fullbright suspects the perpetrator may have done so online—a method offering convenience to law-abiding tax-payers and lawbreakers alike.

"My belief is that the people who do this aren't just those who find a Social Security number in the trash," Fullbright says. "They are those who have knowledge of the business of the IRS and who know the ins and outs of what kinds of returns are going to be stopped."

Direct deposit of tax refunds also makes it easy for scammers to make a "quick hit" on the IRS, Fullbright says. "By the time the victim finds out, five or six days may have passed. That money is gone."

Although it's less common than fraud committed with fake credit-card accounts, tax-related identity theft remains a persistent problem—for both the government and consumers. A U.S. General Accountability Office (GAO) report released last year identified more than 23,000 incidents in which fraudulent tax returns were filed through Dec. 31, 2008. The perpetrator

"Direct deposit of tax refunds also makes it easy for scammers to make a "quick hit" on the IRS. By the time the victim finds out, five or six days may have passed. That money is gone."

Mark Fullbright, fraud expert, Identity Theft 911

typically strikes early in the tax season, prompting the IRS to freeze the refund of the second (typically legitimate) person who attempts to file using that same Social Security number. Data from the 2008 tax year shows that the agency stopped 90 percent of fraudulent refund claims related to identity theft—amounting to a total of nearly \$164 million—but the remaining 10 percent made their way into thieves' pockets, accounting for \$15 million in losses. According to data quoted by the GAO, the median amount of suspected identity theft-related refunds identified during the 2009 filing season was about \$3,400. At the time of the GAO report, it wasn't known how much of the IRS's losses the agency had recovered, but recovery of funds is contingent upon successful prosecution of an identity thief in court. Likewise, this process "may take a long time," the GAO notes, "and it is rarely possible to associate any restitution paid with a specific refund fraud incident because these prosecutions generally involve more than fraudulent refund schemes."

Employment Fraud

A separate but related phenomenon, in which individuals steal identities in order to gain employment, accounted for a comparable number of incidents catalogued as of the end of 2008: nearly 25,000. This form of identity theft can also hold up tax returns, as it results in discrepancies in the amount of income claimed on a particular Social Security number.

Tax-related fraud is bound to eat up some of the victim's time and energy, but knowing some basics can help a person better navigate through the unwelcome situation.

With Bill and Sue, Fullbright began his investigation of the matter by asking himself the same questions he does in other fraud cases. "You have to look at a few different things," Fullbright says. "Did someone steal her Social Security number? Was somebody living as her? Were they using her Social Security number for other things?" The key is to start with the worst case scenario and then begin ruling things out."

Before they'd contacted Fullbright, the couple had already placed fraud alerts on their credit reports. Federal law allows consumers to check their credit reports with each of the three major credit-reporting agencies once a year. Fraud alerts allow more frequent checks, every 90 days. This is key, the fraud resolution specialist says. A fraud alert not only signals creditors to be more judicious in checking the credentials of a credit applicant, it also allows victims a chance to review their credit files to see whether new accounts have been opened in their name using their Social Security number and other personal identifying information.

It's the domino effect evident in the worst identity theft cases—a criminal's movement from one creditor or government agency (or Web site) to another—that worries Fullbright and his fraud resolution colleagues. "One of the first things victims say: What about my taxes? Actually quite a few of my cases involved a person's car being broken into and having tax documents stolen. A person may not realize how bad that is." Indeed, a stolen Social Security number could be used in tandem with other information to set up credit with retailers, to acquire fake identification that could be shown to law enforcement, set up utility accounts and more.

For Bill and Sue, the IRS's process of detecting fraud, validating theft, and substantiating identity amounted to a year and a half of logistical work before they were able to see their refund

money. "One of the frustrating things for my client was that they had to keep sending documents, which they had done several times already," Fullbright says.

IRS addresses vulnerabilities

The IRS has taken steps toward combating identity theft. In 2008 and 2009, the agency added identity theft "indicators" on tax files where the IRS has determined current or potential identity theft issues, and it has implemented screening procedures to handle such cases. The agency also decentralized the resolution of tax fraud and established an Identity Protection Specialized Unit to assist taxpayers.

And yet vulnerabilities remain. The GAO report points out that the timing of tax return filing is such that some employment fraud may go undetected for a year or more. Some cases are never detected at all. "Because of the large volume of mismatches between what is reported on a Form W-2 or a Form 1099 information return and what is reported on an income tax return, and also because of IRS's limited resources, IRS does not pursue some mismatches," the GAO report notes. In cases where the personal identifying information of a person with no tax filing obligation (like a child) is used by someone trying to work under false pretenses, the IRS "may have no way of detecting identity theft," it states. "From IRS's point of view, a tax return has been filed with a name and SSN that match and the income on the tax return matches income reported by an employer."

In employment-related identity theft cases, the IRS will typically notify employers of a Social Security number discrepancy involving one of their employees. Employers are asked to submit an updated W-2 in such cases, and can receive a penalty if they do not. But the GAO notes that "in prior work, we have reported that because of limited requirements for employers to verify and report accurate employee names and SSNs, few, if any, employers are likely to be penalized. In situations where

employers establish "a reasonable cause for the incorrect Form W-2 information by showing they solicited an SSN from each employee one to three times, depending on the circumstances, and that they used this information to complete the wage statements, IRS will waive the penalties on the employers."

A niche market

In the Internet age, tax time poses other problems for consumers, like phishing schemes in which scammers create e-mails or Web sites designed to look as though they've come from the IRS and are designed to trick people into handing over personal data. "Get our refund" e-mails, likewise, capitalize on potential victims' eagerness to obtain refunds, according to the GAO. Reports have also surfaced of surveys having been sent out under the guise of collecting data on taxpayers' satisfaction with the IRS. In reality, these surveys are intended to plant data-harvesting malware on victims' computers.

Identity Theft 911 fraud specialist Raul Vargas says that scammers have also designed Web sites to look like those of legitimate tax preparers—the difference being that these "preparers" route filed returns to themselves rather than the taxpayers to which they are owed. Vargas, too, sees tax cases every year. In one case, a small business owner was worried when he discovered that employee W2's he'd been provided in the mail were missing some of the attached duplicates. They had been torn off. "We were thinking someone might try to use those in order to go online and file a return quickly," Vargas says.

Given the opportunity for fraud—the IRS expects about 140 million paper and electronic returns to be filed this year—Fullbright understands why scammers might try to move into this niche market. "It's not that easy to do but when it happens they are successful," he says. "They can make a lot of money in a short period of time." ■

5 TIPS FROM THE EXPERTS

1. Store sensitive documents, including tax documents, in a secure place like a safe deposit box.
2. Don't ignore your Social Security statements. Review them and if you notice something that doesn't look right, notify the IRS immediately.
3. If you suspect you're a victim of tax-related identity theft, place an initial fraud alert with one of the major credit reporting agencies.
4. Check your credit reports for signs of fraud (www.annualcreditreport.com). If you're a victim of tax-related fraud, there's a chance perpetrators may have hit other areas as well. Also check addresses, employers and other information.
5. Consider a credit monitoring service that will alert you to changes on your credit report.



PROACTIVE TIPS TO WARD OFF TAX FRAUD



E-FILERS

Avoid Solicitations

1. The IRS never communicates via e-mail.
2. If you receive an e-mail claiming to be from the IRS, forward it to phishing@irs.gov.
3. Avoid following links in e-mail and banner ads.

Know Your Tax Preparer

Beware of imposter eFile Web sites. They are rapidly increasing, appear to be legitimate, and can cause serious complications. Be sure to go directly to your tax preparer's Web site.

Protect Your Computer

1. Use strong user names and passwords whenever conducting financial business online.
2. Keep hackers from stealing your information.
3. Do not store your tax information on your computer. Store sensitive information on a safe external drive or disk and keep it secured.
4. Avoid disposing of or donating computers that contain your past tax information.



PAPER FILERS

Carefully Choose Your Tax Preparer

1. Many fraud rings front as tax preparation companies who may steal personal information, redirect your return, or offer to fraudulently review your returns for inaccuracies.
2. Research your preparer with the Better Business Bureau and IRS Office of Professional Responsibility to verify the status of their license.

Review Your Returns

1. Paid preparers are required to sign your return and complete all preparer sections requesting their ID number.
2. Never sign a blank or incomplete return.

Watch For Your Statement Of Earnings

Your annual statement of earnings from the Social Security Administration will identify all individuals working in the United States under your Social Security number. You should receive it approximately three months before your birthday.

Protect Your Tax Documents

1. Mail your returns from a USPS office via certified mail.
2. Opt for direct deposit of refunds to avoid lost/stolen checks.
3. Safely store all tax-related documents including your paystubs, W-2s and tax returns in a secured location such as a safe deposit box or immobile safe.

Review Your Credit Report

Examine your credit report and monitor your accounts to ensure they are not being used to purchase goods or services in your name.

Don't Wait Until The Last Minute To File Your Return

For more information, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490 or visit <http://www.irs.gov/privacy/article/0,,id=186436,00.html>.

For more information on how to safeguard your identity, visit www.identitytheft911.org.