Income Tax Return Scams and Identity Theft

Richard G. Brody[1], Christine M. Haynes[2] & Hector Mejia[3]

[1] Department of Accounting, University of New Mexico, Albuquerque, New Mexico, USA

[2] Department of Accounting and Finance, University of West Georgia, Carrollton, Georgia, USA

[3] Graduate of the MBA Program, University of New Mexico, Albuquerque, New Mexico, USA

Correspondence: Dr. Richard G. Brody, Douglas Minge Brown Professor of Accounting, Anderson School of Management, University of New Mexico, Albuquerque, NM 87131, USA. Tel: 1-505-277-7258. E-mail: brody@unm.edu

Received: January 27, 2014 Accepted: February 13, 2014 Online Published: February 17, 2014

doi:10.5430/afr.v3n1p90 URL: http://dx.doi.org/10.5430/afr.v3n1p90

Abstract

This paper explores why income tax return scams are increasing at an alarming rate. Tax identity theft, unscrupulous tax preparers, and the rise in online financial activity all contribute to the problem. We examine ways income tax fraud is perpetrated. E-filing provides the basis for most fraudulent tax schemes. The IRS currently has several measures in place to counteract income tax fraud including: screening filters that flag multiple returns using the same address or the same bank account number for receiving funds, federal legislation that provides albeit weak financial privacy protection for customers, and raising public awareness. Many believe the IRS could do more. We suggest additional steps they might take to further curtail income tax fraud such as verifying tax return information before releasing refunds to taxpayers and creating an audit trail when distributing funds. Finally, we suggest how individuals can protect themselves to reduce the chance of becoming a victim of income tax return fraud.

Keywords: Income tax return fraud, Identity fraud, E-filing

1. Introduction

It does not have to be "tax season" in order to be a victim of income tax fraud. Take the case of Lea 'Tice Phillips:

> Phillips, an Alabama State employee, had access to private records and databases. From October 2009 to April 2012, she stole individuals' identification and sent this information to Antoinette Djonret. Djonret conspired with others to file false tax returns. Over the three-year period, they filed over 1,000 false returns and claimed a total of over $1.7 million in fraudulent refunds (United States. Internal Revenue Service [US IRS], 2013).

Income tax fraud represents the third largest theft of federal funds, following Medicare and Federal Unemployment fraud. In recent years, tax return scams have dramatically increased. From 2008 to 2012, scams have more than doubled each year, skyrocketing from 51,700 cases to 1.8 million cases (USA Today, 2013). Treasury Department investigators have estimated that the Internal Revenue Service paid more than $5 billion in refunds to identity thieves who filed returns in 2011 alone. Projection estimates show that another $21 billion could be refunded to identity thieves between 2012 and 2016 (Lederman, 2012).

Fraudulent tax filings are not limited to federal returns. Many states fall victim to income tax fraud as well. In Oregon, a twenty-five-year-old woman filed a fraudulent 2011 state return claiming $3 million in wages. The tax agency issued a tax refund of $2.1 million. The agency said that human error led to the excessive refund (Kim, 2012). Georgia estimates that "4% of its returns are fraudulent" (Starkman, 2013, para. 12). During the 2012 tax season, over 900 fraudulent filings totaling more than $1.77 million were spotted and stopped by the New Mexico Taxation and Revenue Department (New Mexico Taxation and Revenue Department, 2012). Between March and October 2013, a joint initiative between the Louisiana Department of Revenue and the Attorney General's Office resulted in the recovery of $1.8 million in fraudulent refunds (State investigators crack down on fraudulent tax refunds, 2013).

2. Common Tax Scams

2.1 E-Filing

Since its inception in 1990, taxpayers have e-filed over 1 billion Form 1040 tax returns (Filing Your Taxes, n.d.). E-filing provides a means for perpetrators to submit fraudulent returns using stolen identities and bogus income information. Much of our financial business is carried out digitally, making it easy for someone to intercept financial and personal information. The huge rise in tax identity theft correlates to the increase in the number of electronically filed tax returns. In 2008, 58% of individual taxpayers filed returns electronically; in 2012, the number rose to 81% (Starkman, 2013).

The IRS is pushing Americans to e-file their taxes, claiming it is a safe, fast and easy way to file (US IRS, 2013, September 3). E-filing certainly is fast and easy, and those two characteristics are what make committing tax identity fraud so simple. E-filing allows returns to be processed and refunds to be sent out within 10-21 days from the day the IRS receives them (Kirchheimer, 2012). However, often the IRS doesn't receive withholding or income information from financial institutions and employers until at least four to six weeks later (Lederman, 2012). This means that most returns are processed weeks, even months, before the source documents are available for verification. In addition, evidence of fraud is difficult to detect because there are no signatures on the forms, no envelopes or physical paperwork involved, and no fingerprints left behind. The promise of a quick return with the lack of physical evidence attracts fraudsters. The ease of electronic filing allows individual perpetrators to file multiple returns, having all of the refunds deposited into one account. In one case, an individual claimed 590 refunds in excess of $900,000; all were deposited into a single account (Lederman, 2012).

2.2 Tax Preparer Fraud

In 2011, the IRS began regulating tax return preparers in an attempt to protect taxpayers. Unenrolled preparers were required to obtain a preparer tax identification number (PTIN) by passing a qualifying exam, paying an annual fee, and taking CPE courses. However, in 2014 the D.C. Circuit Court of Appeals upheld the U.S. District Court for the District of Columbia's decision to enjoin the IRS from enforcing the regulation. The court claimed that, among other things, the regulation was beyond the scope of the IRS's statutory authority (Schreiber, 2014). Thus, oversight of preparer credentials has been left up to the states. Currently only three states – California, Oregon, and New York – have regulatory requirements (Smoker, 2013). As a result, preparer fraud is a common occurrence.

For example, tax preparers may claim "inflated personal or business expenses, false deductions, unallowable credits or excessive exemptions on returns" (US IRS, 2007, para. 1) for their clients. Leslie Brewster of Durham, North Carolina, falsified hundreds of tax returns for her clients by claiming nonexistent dependents, fictitious businesses, and false education credits. As a result, Ms. Brewster's clients received almost $100,000 in undeserved tax refunds (US IRS, 2013).

Tax preparers may also form fictitious tax preparation companies and use stolen identities as their "clients." In Florida, "organized crime has learned that stealing from the federal government can be easier and more lucrative than dealing drugs" (Wolman, 2014, para. 4). For example, an unmarked Miami patrol car pulled over a Cadillac carrying two known members of a West Side gang. The officers confiscated a handful of prepaid debit cards marked with the name "Tax Professors." The ensuing investigation revealed that Tax Professors was the gang's fake income tax preparation company that stole identities and used them to file bogus tax returns. By the time the enquiry was complete, investigators determined that the gang had stolen $1.9 million in fraudulent refunds (Wolman, 2014).

Tax preparers may also deceptively claim to be a member of the Free File Alliance, a coalition of tax software companies that partner with the IRS to complete free e-returns for low to middle income taxpayers (Free File, n.d.). In one twist of this scam, taxpayers hire a tax preparer through a website that falsely claims to be a Free File site. The fraudster completes and files the taxpayer's return but changes the bank routing numbers to the fraudster's own bank routing numbers (Coombes, 2007; US IRS 2012).

Others fraudsters have established fake tax preparation services at physical and virtual locations using well-known business names. They use the reputation of well-known companies to gain trust of unknowing victims. In California, a state with tough oversight regulations, the California Tax Education Council estimates there are over "5,000 tax preparers practicing illegally, possibly hundreds in the Bay Area alone" (Somerville, 2013, para. 5).

Overall, tax preparer fraud is increasing annually, as is the number of arrests and convictions. It is listed third on the IRS records of types of tax fraud (Lawrence, 2013).

3. How Tax Fraud Is Perpetrated

Most tax fraud is perpetrated through tax identity theft. Tax identity theft is easy to accomplish. Equipped with only a person's name and social security number, criminals can re-route a refund to their own account. The rest of the information related to income, withholdings, and deductions is generally fabricated. The refund can be electronically deposited to an anonymous prepaid Visa card that can be purchased at drugstores; these cards have routing and account numbers, which allows funds to be directly deposited without having any identifying information tied to the fraudster (Starkman, 2013).

Identity thieves steal information in several different ways. In some cases, tax preparers use information given to them by former clients to file false returns in subsequent years. Additionally, some fraudsters steal supposedly secure tax information from the Internet. In one case, a hacker stole 3.8 million unencrypted tax records from the South Carolina Department of Revenue (Starkman, 2013). Others use information readily available on the Internet. A fraudster in Florida submitted the names and social security numbers of over 5,000 deceased descendants listed on sites such as Ancestry.com and geneaologybank.com (Novack, 2011).

Finally, employees often steal the names and social security numbers of fellow employees or customers (Sullivan, 2004). For example, Charlton Escarmant and Arthy Icart of Miami, FL were charged with submitting false claims to the IRS, accessing device fraud, and aggravated identity theft after stealing at least 3,200 individuals' information from the Tallahassee Community College where Escarmant had worked. The pair submitted 400 false tax returns seeking more than $3.3 million in refunds.

4. Victim Recourse

Many argue that the IRS is not doing enough to protect people from becoming victims of tax identity theft. In 2012, a tax preparer in Atlanta had her computer stolen. She realized all of her clients would be vulnerable to identity theft and called the IRS seeking help to flag her clients' accounts. The IRS told the woman that her clients would have to file their own affidavits. When one of the clients tried to file an Identity Theft Affidavit, the IRS told her she would have to wait until there was a false return submitted under her identity. As a result, the client became an identity theft victim (Tucker, 2013).

Most of the time people will not know they are victims of identity fraud until they attempt to file their own tax return. The IRS will then send them a letter informing them that a return has been filed already. The letter may include information such as income from a fictitious employer, erroneous income information, unrecognizable expenses or deductions, and other falsified data. The victim is then required to file a police report and contact the IRS at the Identity Protection Specialized Unit by filing Form 14039, "Identity Theft Affidavit" (see http://www.irs.gov/pub/irs-pdf/f14039.pdf). Often, the IRS requires additional supporting documentation. It takes the IRS an average of six months to a year to resolve identity theft cases.

5. Tax Fraud Prevention Strategies

5.1 IRS Prevention Strategies

5.1.1 Proactive Strategies

While tax identity fraud is simple to commit, the sheer number of fraud cases makes it difficult for the Internal Revenue Service to catch and investigate all of them. However, the IRS has some controls in place to detect fraud and prevent it prior to refunds being released.

In 2013, new screening filters were implemented to help identify false returns prior to processing them. Once these filters flag a return, the IRS contacts the sender before any further processing is done. The screening filters also identify multiple returns that use the same address or account number for receiving refunds. Last tax season, the filters increased the number of identified fraudulent returns by 2 million (Tucker, 2013). As a result, the IRS blocked more than $20 billion in fraudulent refunds, up from $14 billion the year before.

In 2012, the IRS also devoted significant resources to battling tax identity theft. They spent $328 million implementing new systems and filters to block identity theft tax returns and assigned 3,000 employees to fight income tax fraud. That's double the number of employees assigned the previous year (US IRS, 2013, September 4). In addition, the number of criminal investigations tripled for the 2012 tax year (US IRS, 2012). The IRS conducted identity theft enforcement sweeps, resulting in 734 enforcement actions and "298 indictments, informations, complaints and arrests" (US IRS, 2013, September 4, para. 9). Moreover, the IRS Criminal Investigation Unit devoted 500,000 man hours battling tax identity theft.

In addition to the overarching approaches being taken by the IRS to prevent tax fraud in general, they now also assign special pin numbers known as Identity Protection Identification numbers (IP PIN) to individual victims of identity theft tax fraud (Tucker, 2013). An IP PIN is a unique identifier that proves to the IRS that the individual filing the return is the authentic filer of the return. If an individual is a victim of identity theft, a notification is placed on his/her account, so the IRS requires an IP PIN number to process a return. This eliminates repeat offenses against the same individual (US IRS, 2012).

5.1.2 Legislation Protecting Individuals' Identities

The federal government has also attempted to help consumers avoid tax identity theft by passing various acts. Of significance is the Gramm-Leach-Bliley Act (GLB) that attempts to provide financial privacy protection for the consumer. Under the GLB Act, financial institutions are prohibited from disclosing any personal consumer financial information to nonaffiliated third parties unless the consumer approves it. Moreover, if a financial institution becomes aware that an incident has occurred and determines that unauthorized access of customer information has happened, it must notify all customers that were affected. Under the GLB Act, financial institutions must give customers the alternative to "opt out" if they do not want their information shared with third parties. However, the GLB Act does provide exceptions for some institutions. Under these exceptions, the financial institution may share information with specific third parties without consumer consent (Gramm-Leach-Bliley Act, 1999).

Unfortunately, the GLB fails in several respects. First, it places the burden of privacy on the consumer by having to opt-out instead of making opt-out the default for sharing information. Additionally, because the opt-out forms contain legal jargon, they can be confusing. Finally, companies do not need their customers' permission to share information with affiliates or exempted partnerships such as a non-affiliated marketing partner.

The GLB Act also seeks to ensure that companies implement security protocols to keep consumer information private. Complying with the GLB Act has reduced the number of breaches, but has far from eliminated the problem as evidenced by the number of high profile breaches in 2013 alone. Breaches have occurred at places such as Evernote and the Federal Reserve, where "hacking…breached one of its internal websites, accessing the personal data of 4,000 bank executives" (Top five data breaches in 2013…so far, 2013).

5.1.3 Raising Public Awareness

Another proactive measure the IRS has taken is community education. Through pages on the irs.gov website and YouTube videos, the IRS informs individuals to watch for signs of tax scams. One such web page published by the IRS on an annual basis is the "Dirty Dozen Tax Scams" (US IRS, 2013, September 4). Identify theft topped the list for 2013. Phishing scams (unsolicited emails or fake websites aimed at stealing personal identification) took second place.

In addition to the top two tax scams that directly involve identity theft, the IRS mentioned several others including tax preparer scams, advertisements for "free money from the IRS," and charitable organizations scams – especially in the wake of a natural disaster (US IRS, 2013, September 4). The IRS hopes people will access irs.gov, read about these scams and what to do if victimized.

5.2 Self-Protection Strategies

Individuals can take several measures to protect their identity. One action is as simple as leaving social security cards at home in a safe and secure place. People should memorize their social security number and be cautious about offering it to any institutions other than banks and governmental agencies. Most businesses have no reason for collecting this type of personal information. Other identity protection measures include securing financial information and checking credit reports semi-annually. Monitoring bank accounts often, at least several times a week, will reveal any unusual account activity. Shredding correspondence with identifying information keeps it out of the hands of dumpster divers.

Individuals must also protect themselves from computer breaches. The accessibility of the internet to shop, bank, and pay bills has resulted in an ever increasing number of people entering personal information online. However, an unsecured computer is an easy target. Making sure that anti-virus software is installed and updated on a computer is only the first step to securing it. Setting up a firewall and securing home wireless networks are more important in many cases. If shopping or banking online, one should ensure the sites are secured by looking for two things: a yellow lock in the lower right corner and a website address starting with https://.

Many people share personal information on social media sites, thereby inadvertently sharing it with a wider set of individuals than intended. Learning all security features of a social media site and then implementing privacy is one

way to make sure personal information does not fall into the wrong hands. However, the best way to secure personal information on social sites is to never share personal data.

6. Recommendations

Many argue that the IRS is not doing enough to protect people from becoming victims of tax fraud. The IRS can take several cost effective steps to reduce the number of fraudulent tax returns and protect taxpayers. One of the reasons fraudsters are so successful is the time lapse between individuals filing their returns and employers verifying the return's information. In their eagerness to please taxpayers, the IRS pays refunds as soon as possible, sometime within two weeks. However, the IRS cannot verify the information with employers (and others required to file tax data) until at least a month after the individual's return is filed. Postponing tax refund payments until employers have filed their returns and/or requiring employers to file their returns earlier would help solve this problem.

Another action the IRS can take to reduce tax fraud is to stop allowing refunds to be paid to debit cards. The IRS can limit refunds to actual bank accounts that can be traced to an individual or mail checks to a valid address. Although this limits the number of ways a refund can be received, it also sends a message to fraudsters that they can be traced and prosecuted much easier than using anonymous debit cards. Finally, tax preparer fraud can be reduced by requiring all preparers to be licensed at the state level. States have the regulatory authority to exert the control necessary to enforce licensure requirements. This would allow fraudsters to be tracked, caught, and prosecuted more easily.

7. Conclusions

Fraudulent tax filing is an overwhelming problem for the Internal Revenue Service. The problem is due to several factors. The simplicity of electronic filing makes it easy for an individual with little or no accounting or tax experience to submit a tax return. The increase in digital activities and social media makes it easy for perpetrators to steal identities. Armed with stolen identities, a fraudster can submit hundreds of tax returns and have the refunds sent to a debit card. The IRS has taken proactive measures to stop fraudulent tax returns. These include identification numbers for victims of identity theft and tax fraud, law enforcement sweeps targeting tax fraud perpetrators, and public awareness programs. The government has also attempted to protect individuals' information by enacting laws requiring financial institutions to protect customer information. Individuals can also take measures to prevent their identity from being stolen. As with many other types of frauds, awareness is the key and taxpayers must be proactive in helping to prevent these scams from continuing.

References

Coombes, A. (2007, April 13). *Tax scammers snag refunds*. [Online] Available: http://www.marketwatch.com/story/scam-free-file-web-sites-are-snagging-tax-refunds-irs-warns

Filing Your Taxes. (n.d.) [Online] Available: http://www.rs.gov/Filing

Free File. (n.d.). [Online] Available: http://www.freefilealliance.org/

Gramm-Leach Bliley Act of 1999, Pub. L. No. 106-102, §§ 501-502, 113 Stat. 1437.

IRS (updated 2012, August 25). *Late tax scam discovered; free file users reminded to use IRS.gov.* [Online] Available: http://www.irs.gov/uac/Late-Tax-Scam-Discovered;-Free-File-Users-Reminded-to-Use-IRS.gov

IRS losing identity theft fight: our view. (2013, April 11). *USA Today*. [Online] Available: http://www.usatoday.com/story/opinion/2013/04/11/tax-returns-identity-theft-editorials-debates/2076077/

Kim, S. (2012, June 12). Oregon Woman Gets $2.1M Fraudulent Tax Refund on Debit Card. *ABC News.* [Online] Available: http://abcnews.go.com/Business/oregon-woman-files-million-fake-wages-fraudulent-tax/story?id=16548378

Kirchheimer, S. (2012, February 6). Protect your tax return and refund from identity thieves. *AARP.* [Online] Available: http://www.aarp.org/money/scams-fraud/info-02-2012/tax-refund-scam-alert.html.

Lawrence, C. (2013, April 12). Tax-preparer fraud rises, exploiting lower-income people and Latinos. *Scripps Howard News Service*. [Online] Available: http://www.abcactionnews.com/dpp/money/tax-preparer-fraud-rises-exploiting-lower-income-people-ixzz2jWfi7HlQ

Lederman, J. (2012, August 2). IRS may have lost billions to identity theft, Treasury says. *Huffington Post.* [Online] Available: http://www.huffingtonpost.com/2012/08/02/irs-identity-theft_n_1733905.html

New Mexico Taxation and Revenue Department (2012, February 21). *Tax fraud investigators stop fraudulent personal income tax returns worth nearly $1.8 million [press release]*. [Online] Available: http://www.tax.newmexico.gov/Press Release Document Library/Tax-Fraud-Investigators-Stop-Fraudulent-Personal-Income-Tax.pdf

Novack, J. (2011, May 6). *IRS pays refunds to 5,000 dead people in post-mortem identity theft scam.* [Online] Available: http://www.forbes.com/sites/janetnovack/2011/05/06/irs-pays-refunds-to-5000-dead-people-in-post-mortem-identity-theft-scam/

Schreiber, S.P. (2014, February 11). *D.C. Circuit affirms decision striking down tax return preparer regs*. [Online] Available: http://www.journalofaccountancy.com/News/20149583.htm

Smoker, K.A. (2013, December). Is state regulation of tax preparers the solution? *The CPA Journal* 83 (12): 68-71.

Somerville, H. (2013, March 19). *Tax preparer fraud creates big refunds, big problems for taxpayers.* [Online] Available: http://www.mercurynews.com/ci_22827278/tax-preparer-fraud-creates-big-refunds-big-problems

Starkman, J. (2013, January 13). E-Filing and the explosion in tax-return fraud*. The Wall Street Journal*. [Online] Available: http://online.wsj.com/news/articles/SB10001424127887323374504578222130665022160

State investigators crack down on fraudulent tax refunds (2013, October 21). *FOX 8 WVUE.* [Online] Available: http://www.fox8live.com/story/23688781/state-investigators-crack-down-on-fraudulent-tax-refunds

Sullivan B. (2004, May 21). Study: ID theft usually an inside job. *NBC News*. [Online] Available: http://www.nbcnews.com/id/5015565/ns/technology_and_science-security/t/study-id-theft-usually-inside-job/#.UlgzUpgpL5k.

Top five data breaches in 2013...so far. (2013, October 1). *SC Magazine.* [Online] Available: http://www.scmagazine.com/top-five-data-breaches-in-2013so-far/slideshow/1387/

Tucker, B. (2013, April 11). IRS making progress against fraud: opposing view. *USA Today*. [Online] Available: http://www.usatoday.com/story/opinion/2013/04/11/identity-theft-irs-editorials-debates/2076035/.

United States. Internal Revenue Service. (2013). *Examples of identity theft schemes-fiscal year 2013.* [Online] Available: http://www.irs.gov/uac/Examples-of-Identity-Theft-Schemes-Fiscal-Year-2013

United States. Internal Revenue Service. (2013, September 4). *IRS releases the dirty dozen tax scams for 2013.* [Online] Available: http://www.irs.gov/uac/Newsroom/IRS-Releases-the-Dirty-Dozen-Tax-Scams-for-2013

United States. Internal Revenue Service. (2013, September 3). *Return preparation and filing options.* [Online] Available: http://www.irs.gov/Filing

United States. Internal Revenue Service. (2013, April 22). *Understanding your LTR4868CS letter.* [Online] Available: http://www.irs.gov/Individuals/Understanding-Your-LTR4868CS-Letter

United States. Internal Revenue Service. (2012, November 29). *The IRS is taking action to protect taxpayers from identity theft and helping victims of tax-related identity theft.* [Online] Available: http://www.irs.gov/uac/The-IRS-is-taking-action-to-protect-taxpayers-from

United States. Internal Revenue Service. (2007, January). *Tax return preparer fraud.* [Online] Available: http://www.irs.gov/uac/Tax-Return-Preparer-Fraud-1

Wolman, D. (2014, January 9). Beware of Gangsters Filing Tax Returns. *Business Week.* [Online] Available: http://www.businessweek.com/articles/2014-01-09/tax-refund-fraud-fake-returns-net-gangsters-millions