The Growing Issue of Tax Return Fraud:

What Are the Causes and What Can Be Done

Sara Fritz

May 04, 2016

Abstract

The aim of this thesis is to detail the current tax return fraud problem and provide proposed solutions.

The paper begins by describing the tax filing process. This process includes ways in which the taxpayer can file a tax return, current security measures of this process, and the percentages of individuals who file their return in the different ways. I then describe how a taxpayer receives a refund, the options the taxpayer has for methods of receiving a refund, and the percentage of people who receive a refund through direct deposit. This discussion also includes when forms are due and what the government agencies do when they receive the forms.

Next, I detail the problems associated with fraudulent federal tax returns. This relates primarily to the problem of identity theft and how it pertains to tax return fraud. I list several ways identity theft is a factor in this issue, including stolen identity information and the previously hacked IRS "Get Transcript" site. I also list and describe several ways taxpayers can deal with their identity being stolen after the fact.

I then propose five solutions to the proposed problem. The first is the authentication of information required by the IRS to file a tax return. The current authentication standards have proven to be weak, so I suggest less accessible security questions and alternate forms of identification such as a driver's license or state issued ID number.

Another proposed solution is increased controls at the IRS. This includes a more advanced computer system that can readily red-flag suspicious items. Additionally, I propose that the IRS should have access to the W-2 and 1099 forms at the same date they are sent to the individuals. Upon receipt of the W-2 and 1099 forms, the IRS should implement an automated system where the forms are scanned in and compared to the individuals' tax returns before a refund is remitted.

I then discuss the PINs currently implemented by the IRS available to the taxpayers, current issues with those PINs, and potential ways to resolve the issues relating to them. Problems discussed include accessibility and solutions include increased security and other ways to access these PINs.

Finally, I discuss what precautionary measures individuals can take and ways new companies are emerging to offer remedies. Individuals can aid in the solution to this problem by filing their tax return as soon as possible, being aware of any fraudulent activity, and notifying government agencies as soon as they are alerted of any fraudulent activity. Identity theft protection service companies are now developing to help individuals to be aware of fraudulent activity and to help remedy the problem after the crime has occurred.

The paper is concluded with a discussion of the monetary aspect of the tax return fraud problem, and how it compares to overall tax deficits. I also summarize the proposed problems and solutions, and suggest that a combination of evolving solutions be implemented to address the issue.

The Growing Issue of Tax Return Fraud: What Are the Causes and What Can Be Done

Thesis

This paper discusses the increasing problems and proposed solutions associated with fraudulent individual federal income tax returns.

My paper begins by describing the tax filing process for individuals in the United States. I then detail the problems that are associated with increases in the amount of tax return fraud. I follow with a discussion of possible solutions, including authentication of information, increased controls, PINs, precautions that can be taken by individual taxpayers, and what industries are emerging to help.

The Tax Filing Process

There are a variety of methods available to individuals for filing their individual federal income tax returns with the Internal Revenue Service. To file a return with the IRS, an individual has the option of e-filing an electronic copy of the return or mailing a paper version of the return. If the individual is owed a refund for overpayment of taxes during the preceding year, the taxpayer has the option to receive the refund through direct deposit into their bank account, issuance of a pre-paid debit card, or a check.

According to the IRS, for 2014, individuals chose e-filing as the primary method for filing their federal tax returns, which represented 93% of all tax returns filed (IRS 2014). Of the individuals who chose to e-file, 56% had a tax professional prepare their tax return, and the remaining 44% prepared the return themselves (IRS 2014). The e-filing approach provides several methods for

filing the return depending on the taxpayer's income. If the taxpayer's adjusted gross income falls below $62,000, the IRS provides Free File Software to the taxpayer. If their income is above $62,000, the taxpayer may use the free file fillable forms, commercial software (such as TurboTax, Taxhawk, or TaxSlayer), or have a tax professional complete and file a return on their behalf (IRS 2016). After entering the required information in the e-filing process, the taxpayer must electronically sign the tax return with a PIN (personal identification numbers). There are three primary types of PINs that taxpayers can use to file their electronic returns: Self-Select PIN, Electronic Filing PIN, or the Practitioner PIN (IRS 2015). Additionally, the IRS provides an Identity Protection (IP) PIN for individuals that have been previously subject to identity theft.

Unlike the electronic filers, individuals choosing to file their federal income tax returns using the paper-based approach (7% in 2014) complete the paper-based forms and then mail them to the IRS (IRS 2014). When filing a paper tax return, the taxpayer may fill in the forms by hand or use the free fillable forms online and print them when completed. If the taxpayer has been previously given an IP PIN, they must include it at the bottom of the tax return. When it is time to mail the tax return, the taxpayer must use the IRS website to determine where to send their return. The IRS mailing address is based on the taxpayer's state of residence and whether an additional tax amount is owed or a refund required.

Once the IRS receives the tax return (electronic or paper-based), it is processed and a refund is sent, if necessary. Based on the taxpayer's request, the IRS will either deposit the refund directly into a checking account, mail a paper check, or mail a pre-paid debit card for the amount. According to the IRS, the most common way to receive a federal income tax refund in 2014 was

through direct deposit, with this method comprising 87% of the number of returns receiving a refund and 88% of the total dollar amount refunded (IRS 2014). Direct deposit is the most common refund method used, but the IRS also maintains the other two refund options. Although the Department of the Treasury suggests that direct deposit is the safest option for taxpayers to use, taxpayers may prefer a check or debit card because they do not have a bank account or do not want to be charged for cashing a check at a bank (U.S. Department of Treasury).

The deadline for submitting a federal income tax return to the IRS is April 15 of the following year. However, before many taxpayers can submit a tax return, they must wait to receive a W2 or 1099 from their employer. Form W2 provides information regarding the employee's prior year wages, earnings, and income taxes withheld. The employer must submit a copy of the W2 to the employee by January 31st, and to the Social Security Administration by March 31st (SSA). Form 1099 is used when an individual is an independent contractor rather than an employee. This form is due to the recipient by February 1st and due to the IRS by March 31st (West 2016). Table A details the deadlines for each of these forms.

Table A

Form	Due to Employee	Due to IRS	Due to SSA
Tax Return	n/a	April 15	n/a
W-2	January 31	n/a	March 31
1099	February 1	March 31	n/a

Increasing Problems Associated with Fraudulent Federal Tax Returns

The IRS has historically reviewed and audited individual tax filings for incorrect or fraudulent tax information. However, more recently, the agency is faced with a growing problem associated with fraudulent income tax refunds. As shown in Table B below, the number of complaints of identity theft filed with the Federal Trade Commission in 2015 is more than 15 times the number of complaints filed in the year 2000 (Peterson 2016). Although identity theft is used by criminals for a variety of crimes, tax return fraud is one of the major ones. According to the United States Government Accountability Office, the IRS estimates it paid out $5.8 billion in fraudulent refunds in the 2013 tax year due to identity theft (U.S. Government Accountability Office). Other sources state the IRS has suggested that this number could reach $21 billion by tax year 2016 (Hunter 2015).

Table B
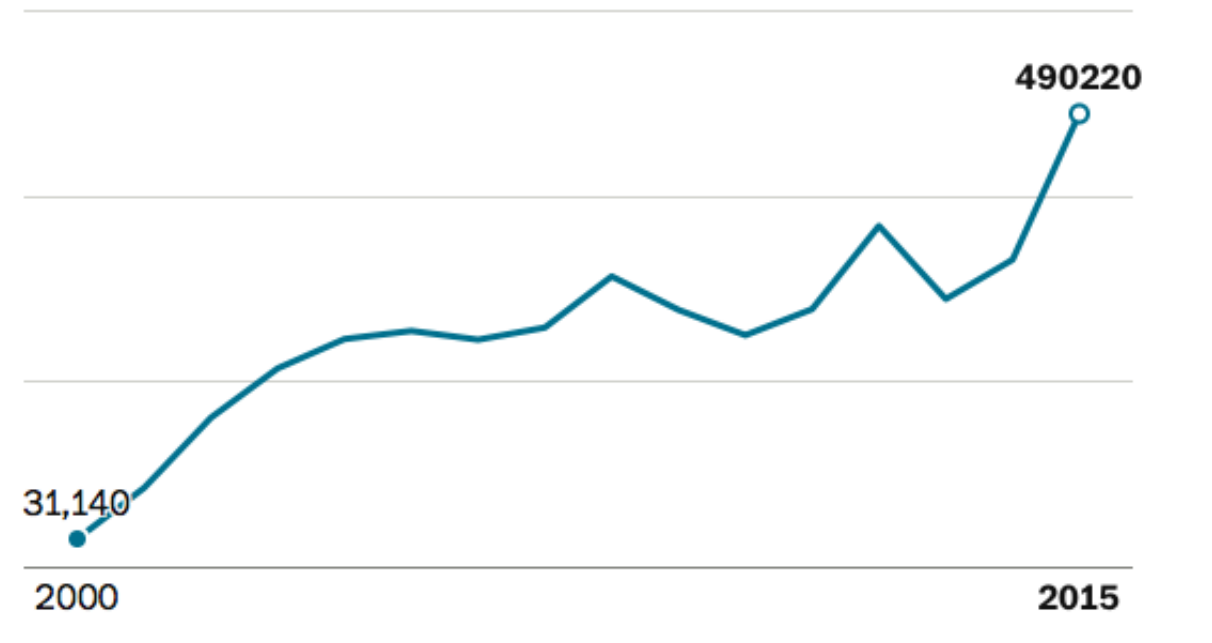
There are a variety of problems contributing to this rapid increase. One is that when an identity is stolen, a person may not know, and by the time they do know it is often too late to take preventative measures. When an identity is stolen, it may not be used immediately, or it may be used long before anyone knows. This is a problem on tax returns because the information received by the criminal can give them the information needed file both e-file tax returns and paper tax returns, for a potentially infinite number of years.

In January 2014 the IRS launched a tool called "Get Transcript" which allowed taxpayers to have online access to their previously filed tax returns after answering a series of questions known as "Knowledge Based Authentication" (KBA) (Mart). KBA includes questions about information that is readily accessible through other online sources such as social media or credit reports. In May 2014, five months after its launch, the KBA system was hacked and the data of over 700,000 taxpayers was stolen (Mart 2016). This information can be used on future tax returns because it gives criminals the detailed personal information needed to fraudulently file a tax return.

A study by the Department of Treasury determined that in 2013 the average amount of time it took the IRS to resolve a tax-related identity theft case was 312 days (U.S. Department of Treasury 2013). This left taxpayers without their refund for 312 days, and even after the issue was resolved, the IRS was still having to pay both the criminal and the taxpayer refund amounts.

Steps Victims Can Take

If an individual's identity is stolen, it often remains unknown to the victim for a period of time. Once the victim becomes aware of this crime against them, there are several steps to take

according to the website www.identitytheft.gov. Screen-prints of the steps presented and

discussed on this website are presented in Table C.

Table C

What To Do Right Away

Print Checklist

Are you dealing with tax, medical, or child identity theft? See: Special forms of identity theft

➕ Step 1: Call the companies where you know fraud occurred.

➕ Step 2: Place a fraud alert and get your credit reports.

➕ Step 3: Report identity theft to the FTC.

➕ Step 4: File a report with your local police department.

What To Do Next

Print Checklist

Take a deep breath and begin to repair the damage.

➕ Close new accounts opened in your name.

➕ Remove bogus charges from your accounts.

➕ Correct your credit report.

➕ Consider adding an extended fraud alert or credit freeze.

The first step an identity theft victim should take is to call all companies where the fraudulent

activities occurred and freeze all accounts. The passwords and PIN numbers for these accounts

should be changed as well. Next, the individual should contact all three credit bureaus and place

a fraud alert on their account. A fraud alert is a free precautionary measure that makes it difficult

for someone to open new accounts in your name. Also, the individual should obtain their credit report from these bureaus and make note of all unrecognized transactions.

The third step is to report the identity theft to the Federal Trade Commission. The FTC provides an interactive form where individuals can detail the fraudulent acts committed. After completing the form, the FTC will then provide a recovery plan based on the given information. As a preventative measure, Form 14039 (Identity Theft Affidavit) should be filed with the IRS (Intuit 2015). This form notifies the IRS of the identity theft and is a red-flag in the system for tax return fraud.

Proposed Solutions

Authentication of information

Currently the information required to submit a tax return includes the name, birthdate, and social security number of an individual. However, due to advancements in technology and the rise of social networking websites, full names and birthdates are easily obtainable by criminals. Additionally, if a password or username is "forgotten," a series of security questions can be asked for the individual to regain access to the password or username. These questions typically include information such as mother's maiden name, pet's name, elementary school name, etc. With the lack of protection and use of social media it is easier than ever to discover the answers to these questions. For example, women often change their middle name to reflect their maiden name, so that information can be found by looking at an individual's Facebook page.

To begin addressing this issue, a variety of information should be required to file a tax return, and security questions should be based on less accessible answers. An option as an alternative to, or in addition to, the Social Security number to file a tax return, is to request either a copy of or the number of the taxpayer's driver's license or state issued ID. Although this could have the same vulnerabilities as a social security number in the long run, it offers a temporary solution until the IRS implements controls that can successfully identify fraudulent tax returns.

Increased controls

The IRS currently maintains an unspoken "pay now, ask questions later" policy which has made it difficult to control the increasing tax return fraud problem. A potential solution to this problem is to increase controls so the IRS return processing system can raise questions and identify fraudulent returns before refund payments go out. This would include delaying payments when multiple checks or debit cards are sent to one location, or when a taxpayer's address is different from the previous year's tax return. While it is possible that several taxpayers file separately under one roof or that the taxpayer has moved, these factors could also indicate fraud and should be red-flagged automatically by the IRS tax return processing system.

Additionally, the W-2 and 1099 forms should be entered and automated into the system as soon as they are received and verified and matched with the information reported on the tax return before a payment can go out. Although this could delay refunds for some taxpayers, it is arguable that it would take less time than if their tax return was fraudulently filed and they had to wait for the IRS to resolve the issue. Currently when an employer files a W-2 for an employee, it is sent to the Social Security Administration, and when the SSA is done with the forms, they are

forwarded on to the IRS. In order to synchronize and better automate the system, the 1099 and W-2 forms should be sent directly to both the IRS and SSA at the same time as they are sent to the employee.

PIN

There are three primary types of PINs currently available to all taxpayers for increased security when filing a tax return: Self-Select PIN (SSP), Electronic Filing PIN (EFP) and the Practitioner PIN. The SSP uses either your birthdate, prior year adjusted gross income, or prior year SSP to authenticate your identity. This was a problem through 2015, as prior year tax returns were available to taxpayers via an IRS "Get Transcript" tool that became an object of vulnerability prone to hacking. Currently, if a taxpayer forgets their SSP, they are issued a temporary EEP. This PIN is issued through the IRS website upon entering a social security number, full name, date of birth, filing status, and address. This PIN changes each year. The Practitioner PIN serves as the signature of a taxpayer when a tax professional is completing the form. This PIN is comprised of a series of five numbers that the taxpayer can create himself, and then must provide along with Form 8879 to the tax professional completing the return (IRS 2015).

In addition to the PINs described above, the IRS recently has added an Identity Protection (IP) PIN. This PIN is a series of six digits generated by the IRS that is changed on an annual basis. An IP PIN is automatically assigned to taxpayers that have previously dealt with a fraudulent federal income tax return. Additionally, individuals who have been subject to identity theft, as well as residents of Florida, Georgia, and the District of Columbia can "opt-in" to the IP PIN

program. Currently, taxpayers can access their IP PIN at any time, just like the other PINs. To access their IP PIN, a taxpayer must supply a social security number, date of birth, email address, filing status, and address (IRS 2016).

Although PINs were recently deemed to be the next big step in security, many problems have arisen in recent months pertaining to them. Because IP PINs are regularly accessible to taxpayers at any time, they are also available to criminals attempting to file fraudulent returns. According to an article in The Washington Post, in February 2016, hackers were able to access the IP PINs on the IRS website and hack into the system because it used the same technology as the previously hacked "Get Transcript" site (Peterson 2016). This resulted in many people who had previously been victims of tax return fraud, being a victim in 2015 as well.

A solution to this problem could be to confirm the taxpayer's identity online through a series of questions, confirm the address online, and only allow taxpayers to obtain an IP PIN through mail and within a smaller window than year round. This will prevent criminals from being able to access IP PINs year round and will also leave criminals with a smaller window to file a fraudulent tax return because the IP PIN must be correctly stated on the tax return to be filed.

Individuals

Although the IRS is the primary regulator in the tax return fraud dilemma, there are measures that individuals can take to help protect themselves from being victims. As mentioned previously, individuals should file a complaint with the FTC and file the IRS Form 14039 as soon as they become aware of any fraudulent activity in their accounts. Those steps will raise awareness in the IRS if a fraudulent tax return were to be filed in the future.

As previously stated, companies are not required to submit W-2 forms to employees until the end of January, which makes it difficult for individuals to properly file close to year end. However, individuals should be prepared to file as early as they have the ability to, as this reduces the chances of a criminal fraudulently filing and receiving a refund with that individual's identity.

As a simple precautionary step, individuals should change their e-filing password on an annual basis. Finally, if a fraudulent tax return was previously filed, that individual should request a copy of the false tax return to examine what information was stolen. This will give the victim the opportunity to investigate where the information came from and the ability to protect it better in the future.

ID Theft Identity Protective Services

While the IRS and individuals are doing their parts to combat the tax return fraud issues, an industry is also forming around the issue as they have noticed a need. This industry is identity theft protection services. One example of this type of company is LifeLock, but there are many other similar companies emerging.

Although no company can truly protect an individual from having their identity stolen, these companies offer monitoring services to watch for signs of criminals using the personal information of their customer to commit identity theft. The monitoring services vary among companies, but there are two primary types: credit monitoring and identity monitoring (FTC). Credit monitoring uses the information reported by the major credit monitoring agencies and

notifies the customer of any new transactions noted on their credit report. Identity monitoring

monitors your personal information, information that does not typically show up on a credit

report, such as change of address, loan applications, or other uses of the customer's social

security number or passport.

Also, the companies offer recovery services if the customer's identity is stolen. The recovery

services often include trained professionals and counselors that work with the customer and the

customer's specific situation (FTC). Although there are recovery plans accessible through the

IRS website, the professionals available through the identity theft protection services are trained

in the matters and are more readily accessible to help.

Conclusion

The growing problem of fraudulent tax refunds as it has earned a place on IRS's annual list of

"Dirty Dozen" tax scams for several consecutive years. However, Victor Searcy, Director of

Fraud Operations at IDT911, an identity protection and risk services firm in Scottsdale, Arizona,

describes the IRS as having a "pay first, ask questions later" system, which has resulted in this

problem remaining untamed (Hunter 2015).

A tax refund can be defined as the difference between taxes paid and taxes owed, or a reduction

in government collections, and therefore a refund is paid when the taxpayer has overpaid their

taxes. When a criminal files a fraudulent tax return, they are claiming a refund of taxes that were

never remitted to the government. The government proceeds to pay this criminal a tax "refund"

and is only reducing government collections.

According to the IRS, in fiscal year 2014, federal income was $3.021 trillion and outlays were $3.506 trillion, leaving a deficit of $485 billion (IRS 2016). The $21 billion previously mentioned as the expected 2016 outlay for fraudulent tax returns, makes up over 4% of that 2014 deficit. Although $21 billion sounds small in comparison, when the United States is facing a multi-billion-dollar deficit from federal income taxes alone, the $21 billion is a huge part. Additionally, when the IRS addresses the tax return fraud problem, and updates the controls, it is possible that those control updates will assist in other areas causing the $485 billion deficit.

In conclusion, the IRS needs to make timely adjustments to address the growing tax return fraud problem to benefit the IRS, individual taxpayers, and the United States government as a whole. This will not be a simple task, and will require a combination of solutions, but needs to be done soon before the problem grows out of hand.

Works Cited

Federal Trade Commission (FTC). "Identity Theft Protection Services." Mar. 2016. Web.

Hunter, Matt. CNBC. "Tax-refund fraud to hit $21 billion, and there's little the IRS can do." 11 Feb. 2015. Web.

Intuit. TurboTax. "Guide to IRS Form 14039 Identity Theft Affidavit. 2015. Web.

IRS. "More Taxpayers Filing from Home Computers in 2014, Many Taxpayers Eligible to Use Free File." 13 Mar. 2014. Web

IRS. "Free File: Do Your Federal Taxes for Free." April 2016. Web.

IRS. "Get An Identity Protection PIN (IP PIN)." April 2016. Web.

IRS. "Topic 255 - Signing Your Return Electronically" 30 Dec. 2015. Web.

IRS. *2015 1040 Instructions*. 5 Jan. 2016. Print.

Mart, Jonnelle. The Washington Post. "The IRS says hackers stole data for twice as many taxpayers as initially expected." 26 February 2016. Web.

Peterson, Andrea. The Washington Post. "Why so few identity theft victims turn to the government for help." 28 Jan. 2016. Web.

Peterson, Andrea. The Washington Post. "The IRS suspends hacked tool meant to help identity theft victims." 8 Mar. 2016. Web.

SSA. "Deadline Dates to File W-2s." Web.

U.S. Department of Treasury. "Direct Deposit of IRS Tax Refunds Resource Page." Web.

U.S. Department of Treasury. "TIGTA Report: The IRS Needs to Improve Customer Service for Identity Theft Victims" 7 Nov. 2013. Web.

U.S. Government Accountability Office. "High Risk Series." Feb. 2015. Web.

West, Sharon Lindsey. Tax Act Professional. "1099-MISC Deadlines for 2016 and New State Filing Requirements." 2016.