# The "Dirty Dozen" Tax Scams Plus 1

***Betty M. Thorne and***
***Judson P. Stryker***
***Stetson University***
***DeLand, Florida, USA***

**betty.thorne @stetson.edu** **jstryker@stetson.edu**

## Executive Summary

Tax scams, data breaches, and identity fraud impact consumers, financial institutions, large and small businesses, government agencies, and nearly everyone in the twenty-first century. The Internal Revenue Service (IRS) annually issues its top 12 list of tax scams, known as the "dirty dozen tax scams." The number one tax scam on the IRS 2014 list is the serious crime of identity theft. The 2014 list also includes telephone scams, phishing, false promises of "free money," return preparer fraud, hiding income offshore, impersonation of charitable organizations, false income, expenses, or exemptions, frivolous arguments, false wage claims, abusive tax structures, misuse of trusts and identity theft. This paper discusses each of these scams and how taxpayers may be able to protect themselves from becoming a victim of tax fraud and other forms of identity fraud. An actual identity theft nightmare is included in this paper along with suggestions on how to recover from identity theft.

Key Words: identity theft, identity fraud, tax fraud, scams, refund fraud, phishing

## Introduction

Top Ten Lists and Dirty Dozen Lists have circulated for many years on various topics of local, national and international interest or concern. Some lists are for entertainment, such as David Letterman's humorous "top 10 lists" on a variety of jovial subjects. They have given us an opportunity to smile and at times even made us laugh. Other "top ten lists" and "dirty dozen" lists address issues such as health and tax scams. For example, to help the public become more aware of food concerns the Environmental Working Group (EWG) issues various Dirty Dozen guides. The EWG on November 12, 2014 issued a news release about their new first Dirty Dozen Guide to Food Additives (Sciammacco, 2014). This guide "covers food additives associated with serious health concerns, ingredients banned or restricted in other countries, and other substances that shouldn't be in food" (Sciammacco, 2014).

Fraudulent tax returns are a public concern. To help the public become more aware of tax scams, the Internal Revenue Service (IRS) annually issues an updated list of its own top 12 tax scams, known as the "dirty dozen tax scams." Identity theft tops the list of tax scams for 2014 (IRS Releases, 2014). Other tax scams on the 2014 list include telephone scams, phishing, false promises of "free money," return preparer fraud, hiding income offshore, impersonation of

charitable organizations, false income, expenses, or exemptions, frivolous arguments, false wage claims, abusive tax structures, and misuse of trusts (IRS Releases, 2014).

# The Dirty Dozen

## Identity Theft

What is identity theft? According to the IRS, "Identity theft occurs when someone uses the taxpayer's personal information, such as name, Social Security number and other data without the permission of the taxpayer. The intent of the scammer is to commit fraud or other crimes. In many cases, an identity thief uses a legitimate tax payer's identity to fraudulently file a tax return and claim a refund" (IRS Releases, 2014).

J. Russell George, the United States Treasury Inspector General for Tax Administration (TIGTA), stated that "Tax-related identity theft continues to be one of the biggest challenges facing the Federal system of tax administration" (Becker, 2014). George continued "It is incumbent upon the Internal Revenue Service to fully utilize all available tools in the fight against this fraudulent activity" (Becker, 2014). The TIGTA report of July 19, 2012 warned that "Undetected tax refund fraud results in significant unintended Federal outlays and erodes taxpayer confidence in our Nation's tax system" (There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft, 2012). TIGTA warned that an estimated $21 billion could be distributed in fraudulent tax returns by 2016 unless the IRS follows TIGTA's recommendations to help reduce fraudulent tax returns (TIGTA Recommends, 2012).

On September 21, 2014 "The Tax Refund Scam" aired on the CBS program *60 Minutes*. Correspondent Steve Kroft spoke with Wilfredo A. Ferrer, the United States Attorney for the Southern District of Florida. Ferrer commented that for tax refund fraud "all you need is a laptop, someone's Social Security number, date of birth, not even their name. They can do it from their kitchen table. They can do it at a fast-food chain restaurant. Or they can do it on the beach, as long as they have Wi-Fi access" (CBS *60 Minutes*: The Tax Refund Scam, 2014). Debbie Wasserman Schultz, member of the United States House of Representatives (Florida) introduced House of Representatives Bill 744 (H.R.744) on February 15, 2013. This bill, now known as Stop Identity Theft Act of 2014 or sometimes known as Stopping Tax Offenders and Prosecuting Identity Theft Act of 2014, passed the House of Representatives on September 8, 2014 and was received by the United States Senate on September 9, 2014 where it was read twice and placed on the United States Senate Legislative Calendar as Calendar No. 555 (H.R.744 Stop Identity Theft Act of 2014: Major, 2014). This Act proposes a punishment up to 20 years in prison if an individual is convicted of tax return identity theft, includes organizations as possible tax return identity theft victims, and requires the Attorney General to submit a report to the judiciary committees of the House of Representatives and the Senate within 180 days of the enactment of this Act concerning:

> (1) Information readily available to the Department of Justice about trends in the incidence of tax return identity theft. (2) Recommendations on additional statutory tools that would aid in the effective prosecution of tax return identity theft. (3) The status on implementing the recommendations of the Department's March 2010 Audit Report 10-21

> entitled 'The Department of Justice's Efforts to Combat Identity Theft.' (H.R.744 Stop Identity Theft Act of 2014: Text, 2014)

The IRS issues a special number called an IP PIN – identification protection personal identification number – which identity theft victims must use in filing their federal tax returns. In 2012 the number of IP PINS issued was 250,000; this number increased in 2013 to 770,000; and in 2014 the number of IP PINS issued by the IRS increased to 1.2 million. IP PINS are to help identify legitimate taxpayers and to more quickly process their returns. However, according to the United States Treasury Inspector General for Tax Administration 532, 637 identity theft victims did not receive an IP PIN in 2014 since the IRS stated that they could not confirm the addresses of these taxpayers (Becker, 2014).

***Examples.***

Corey Williams had been a legitimate tax return preparer until he became aware of the ease of committing tax return fraud and the millions of dollars that he could steal. Williams stated

> …you don't even need a laptop, you can file phony returns on your cell phone, if you have the right app…. I could wake up in the comfort of my own home, and just get on a laptop, do about 15 returns a day. Fifteen times $3,000 a return, that's $45,000 a day. (CBS 60 *Minutes:* The Tax Refund Scam, 2014)

According to the Federal Bureau of Investigation Miami Division, Corey Williams was sentenced "on May 21, 2014 to 40 months in prison, to be followed by three years of supervised release, and was ordered to pay $2,089,411 in restitution" (Two More Defendants, 2014).

Maximo Amparo-Vazquez pleaded guilty in July 2014 to conspiring to defraud the government with respect to claims.

> According to court documents, from January 2010 to March 2012, Amparo-Vazquez conspired with others to use stolen identities to file income tax returns for the purpose of obtaining fraudulent income tax refunds. The conspirators in the income tax fraud scheme obtained the stolen identities of more than 2,600 individuals, including people's names and social security numbers. (Examples of Identity Theft Schemes – Fiscal Year 2014, 2014)

***Tips.***

Although there is no way to positively guarantee that one does not become a victim of a tax fraud scam, there are some tips that may help reduce one's probability.

- File early. Fraudsters know that the IRS tries to process refunds as quickly as possible, and therefore, they file early hoping to claim a refund before you file. It is recommended that a taxpayer file early "even if you owe money, and then send in your check later, by the April 15th filing deadline" (Weisman, 2015, p. 70).
- Ask your tax preparer (if you use one) if the security software on the preparer's computer is current.
- Be sure you have a very strong password and up-to-date security software on your computer if you file your own return electronically.

- Delete tax return information from your hard drive. This information can be stored on an external hard drive or some other external device such as a flash drive (Weisman, 2015, p. 77).
- Consider filing an IRS form 8821. This form "authorizes any individual, corporation, firm, organization, or partnership you designate to inspect and/or receive your confidential information for the type of tax and the years or periods listed on the form" (Form 8821, Tax Information Authorization, 2014). If you name yourself in Form 8821, you will "receive information about your income tax return so that if there are any issues with the phony income tax return filed by the identity thief, you will be contacted" (Weisman, 2015, pp. 70-71).

It is important to note that identity theft extends beyond tax refund fraud to include credit card fraud, medical fraud, bank account fraud, mortgage fraud, Social Network ID theft and other types of frauds. Javelin Strategy & Research annually conducts various primary research studies including a study of fraud and security. Their findings are available in the month of February for the preceding calendar year. Javelin's 2014 Identity Fraud Report "provides a comprehensive analysis of fraud trends in the context of a changing technological and regulatory environment in order to inform consumers, financial institutions and businesses on the most effective means of fraud prevention, detection and resolution" (2014 Identity Fraud Report, 2014). In 2013 Javelin surveyed a representative sample of 5,634 U.S. adults, including 936 fraud victims. According to this Javelin report, 13.1 million identities were stolen in 2013, the second highest number of victims recorded (2014 Identity Fraud Report, 2014).

The 2014 Javelin report also indicated that in 2013 there was an incident of identity fraud every two seconds, approximately $18.1 billion stolen, and that one out of every three people who receive a data breach letter actually became a victim (Equipping Consumers in the Fight Against Identity Fraud: Fraud Prevention Checklist, 2014, pp. 2-3).

The Consumer Sentinel Network (CSN) is available only to law enforcement. CSN is a secure online data base of consumer complaints. CSN released its findings for calendar year 2013 in February 2014. One finding was that in 2013 (as in several previous years) Florida had the highest per capita reported rate of identity theft complaints in the United States. Georgia was second and California was third (*Consumer Sentinel Network Data Book*, 2014, p. 3). It is important to note that the CSN findings are not based on survey data, but rather on "unverified complaints reported by consumers" (*Consumer Sentinel Network Data Book*, 2014, p. 2).

The Consumer Sentinel Network also reported on various methods (such as email, mail, Internet, or phone) that consumers in 2013 were initially contacted concerning identity theft and fraud. From those complaints that reported an answer to method of initial contact, telephone calls was the most common method (40%) followed by 33% being notified by email, 15% by Internet, 5% by mail, and the remainder by some other method (*Consumer Sentinel Network Data Book*, 2014, p. 9).

Through the media (such as "The Refund Tax Scam" on CBS *60 Minutes*), through government legislation (such as H.R.744 – Stop Identity Theft Act of 2014), and through efforts on the part of the IRS (such as IP PINS), it is hoped that the public becomes more aware of the dangers of identity theft and that the estimated loss from identity fraud can be reduced.

## Pervasive Telephone Scams

Some scammers take on the identity of the IRS in hopes of stealing money or the identities of their victims. Callers may say that victims owe money or are entitled to large refunds (Scam Phone Calls Continue; IRS Identifies, 2014). Other variations threaten arrest and revocation of drivers' licenses. One approach has callers paired with follow-up callers saying they are from the local police department or the state motor vehicle department. Victims are told they owe money to the IRS and must pay promptly through a preloaded debit card or wire transfer (IRS Repeats Warning, 2014). If the victim refuses they are threatened with arrest, deportation or suspension of a business or loss of a driver's license. It is not uncommon for the caller to become hostile in an attempt to instill fear. As of August 2014, the Treasury Inspector General for Tax Administration reported receipt of 90,000 complaints and identified approximately 1,100 victims who have lost an estimated $5 million from these [phone] scams (IRS Repeats Warning, 2014).

The IRS Commissioner, John Koskinen, reminds the public:

> Taxpayers should remember their first contact with the IRS will not be a call from out of the blue, but through official correspondence sent through the mail. A big red flag for these scams are angry, threatening calls from people who say they are from the IRS and urging immediate payment. This is not how we operate. People should hang up immediately and contact TIGTA or the IRS. (IRS Repeats Warning, 2014)

The IRS has processes for taxpayers with tax issues. According to Koskinen, "The IRS respects taxpayer rights, and these angry, shake-down calls are clear warning signs of fraud. This is not how we do business. We urge people to be careful when they get these threatening phone calls" (Scam Phone Calls Continue; IRS Unveils, 2014).

Technology has brought numerous advances to the twenty-first century in many ways attempting to make our lives easier. One such advancement is the use of mobile phones for activities such as mobile banking. However, it is easy to download a bogus banking app opening the doors to tax return fraud. There are steps that can be taken to limit this type of scam. The mobile industry can take actions such as developing specific app clearinghouses. The business sectors such as banking or healthcare could benefit from being knowledgeable and have a way to approve apps with that specific sector. Individuals can take immediate action by contacting their bank or credit union in changing login passwords regularly.

***Examples.***

A Baptist minister, the Rev. Al Cadenhead, from Charlotte, North Carolina received a phone call in October, 2014 from a lady who claimed that his tax return was being audited and that due to "serious miscalculations" that he owed taxes to the IRS, that there was a warrant out for his arrest, and that a lien was being put against his house. This IRS imposter cheated Cadenhead out of $16,500 (Hastings, 2014)

In July 2014 Frank Garcia, a former North Carolina Panthers player and host of radio show on station WFNZ became a victim of a pervasive telephone scam. The caller posing as an IRS

representative told Garcia that he had less than one hour to wire $3,985.69 or he would be arrested. Garcia wired the money, and was told that he still owed an additional sum of $9,000. At this point Garcia realized he had become a scam victim (TWS staff, 2014).

***Tips.***

- A call to the IRS is an appropriate step in shutting down a pervasive telephone scam.
- The IRS will not call taxpayers to request personal or financial information such as PINs, passwords, and other confidential access information for taxpayers' bank accounts, credit cards, or other financial accounts.
- If the mobile application is questionable, have it removed and evaluated by a technical team to ensure appropriateness. It is recommended that individuals wait until applications have been thoroughly proven to be secure before downloading (Holtfreter, 2010). You may also contact the Federal Trade Commission (IRS Releases, 2014).

## Phishing

Phishing is a scam typically carried out through an unsolicited e-mail or a fake website that appears to be legitimate. The scam attempts to lure potential victims and prompt them to provide personal and financial information. With this information the scammers can commit identity theft and financial theft. The IRS points out that they do not initiate contact with taxpayers by e-mail to request personal and financial information (IRS Releases, 2014).

***Example.***

On March 28, 2014 the IRS warned consumers about an email phishing scam claiming to be from the Taxpayer Advocate Service (TAS) which is a "legitimate IRS organization that helps taxpayers resolve federal tax issues that have not been resolved through the normal IRS channels" (The IRS Warns of New Email Phishing Scheme, 2014). According to the IRS warning, the email might contain a message such as,

> Your reported 2013 income is flagged for review due to a document processing error. Your case has been forwarded to the Taxpayer Advocate Service for resolution assistance. To avoid delays processing your 2013 filing contact the Taxpayer Advocate Service for resolution assistance. (The IRS Warns of New Email Phishing Scheme, 2014)

Recipients of this phishing scam were then instructed to click on links that would take them to someone assigned to their case; the links simply took recipients to web pages soliciting personal information allowing the scammers to file false tax returns.

***Tips.***

- If you suspect phishing, it should be reported to the IRS by submitting an e-mail to phishing@irs.gov.
- The Taxpayer Advocate Service and IRS will never contact taxpayers by email, texting, or any social media (The IRS Warns of New Email Phishing Scheme, 2014). Taxpayers

who receive an email claiming to be from the IRS "should not open any attachments or click on any links contained in the message. Instead, forward the email to phishing@irs.gov" (IRS Repeats Warning, 2014).

- Weisman (2015) recommends that one does not "click on the hyperlink in the email that purports to send you directly to the company's website. Rather, type in what you know to be the proper website address for the company with which you are dealing" (p. 9).
- Only download from legitimate websites that you know. Identity thieves attempt to lure people to fake websites on popular topics or current events (such as the Ebola virus or a public election). "But you should always remember that whatever fascinates large numbers of the public, also sparks the interest of identity thieves" (Weisman, 2015, p. 10).

## Free Money

Scammers frequently pose as tax preparers during tax time who are promising large federal tax refunds. A deceitful tax preparer promises large, attractive refunds where his or her commission is based on the refund (Lauridsen, 2014). Flyers, advertisements, and storefronts are used to find victims. Some scammers have used community groups or churches to give credence and trust to the scammers. The focus is generally on low income individuals, elderly and non-English speaking taxpayers. Victims can be misled by offers of fictitious rebates, benefits, and tax credits. It is not uncommon for these unscrupulous scammers to file false returns in a person's name without their knowledge. Victims of this scam frequently are not given a copy of the return that has been filed. Fraudulent refunds are often deposited into the scammer's bank account. Large fees are often deducted before cutting the check to the victim. Unfortunately, the taxpayer has the legal responsibility for the content of the tax return, even if prepared by someone else. The taxpayer can incur penalties for filing a false claim or receiving fraudulent refunds.

***Example.***

- Fraudulent tax preparers increase the number of dependents on the tax form in order to obtain a larger refund. The taxpayer is not aware of this fraud until the taxpayer is notified by the IRS.

***Tips.***

- Carefully choose individuals or firms in preparing your tax returns.
- Remember that professional return preparers will ask for proof of income and eligibility for credits and deductions.
- Remember that professional return preparers will also sign the returns as the preparer, show a preparer's tax identification number, and then give the taxpayer a copy of the return (IRS Releases, 2014).

## Return Preparer Fraud

A closely related topic is return preparer fraud. According to the IRS about 60% of taxpayers use professional preparers to complete their returns. Those few unscrupulous preparers can initiate

identity theft or cause refund fraud. An unscrupulous tax preparer alters a taxpayer's return, requesting a larger refund, after the taxpayer has signed the return. The preparer pockets the inflated portion of the refund, while the unsuspecting taxpayer receives the correct refund. Eventually, the IRS sends a notice requesting repayment for the missed statements on the tax return (Lauridsen, 2014).

***Examples.***

The IRS provides numerous examples of abusive return preparer investigations that "are written from public record documents on file in the courts within the judicial district where the cases were prosecuted" (Examples of Abusive Return Preparer Investigations – Fiscal Year 2014, 2014). Two such examples are Anita R. Ford (a.k.a Anita R. Dixon) and Keller Covington Jr.

According to court records, between 2004 and 2012 Anita R. Ford owned and operated Georgia Peach Financial & Fast Tax Service. In order to obtain fraudulent refunds, Ford filed thousands of Form 1040 returns in which she intentionally misstated her clients' income. On September 26, 2014, Ford was sentence to "51 months in prison, two years of supervised release and ordered to pay $5,732,021 in restitution" (Examples of Abusive Return Preparer Investigations - Fiscal Year 2014, 2014).

According to court records, Keller Covington Jr. owned and operated KCJ Financial Corporation and assisted in the operation of DFC Tax Pros, Inc. Both tax preparation businesses were located in New Jersey. Covington falsified clients' information in order to obtain larger tax refunds. Covington was sentenced on July 8, 2014 in Newark, New Jersey for aiding and assisting in the preparation of false tax returns. His sentence included a prison term of 18 months, a supervised release for one year, and a ten-year suspension of the tax preparation business (Examples of Abusive Return Preparer Investigations - Fiscal Year 2014, 2014).

Charles Corbitt, an IRS employee, was indicted on September 18, 2014 "for wire fraud in connection with a false federal tax return" (IRS Employee Indicted, 2014). Corbitt "prepared and electronically filed, or caused to be filed, a fraudulent tax return for an acquaintance without the individual's knowledge of its false claims" (IRS Employee Indicted, 2014). Corbitt and the individual met through a mutual friend. The individual trusted Corbitt simply because he was employed by the IRS (IRS Employee Indicted, 2014).

***Tips.***

- Check the credentials of your tax preparer.
- Use only preparers who sign returns they prepare and enter their IRS preparer tax identification number (IRS Releases, 2014).

## Hiding Income Offshore

Harbor Financial Services (HFS) assists clients in the development of offshore plans and believes that one legitimate reason for offshore accounts is protection from litigation. "Ex-spouses, ex-business partners, disgruntled employees or predatory attorneys may file suit if they believe a potential defendant is an attractive target. Losing such a lawsuit could cause a lifetime's

worth of savings, investments and real estate holdings to be lost" (Harbor Financial Services, 2015). However, taxpayers must be careful to not initiate a tax scam or fraud by evading taxable income through hiding it in offshore banks, brokerage accounts, or foreign trusts. The IRS will track taxpayers with undeclared accounts and severe penalties can result (IRS Releases, 2014).

In order to prevent people from hiding income offshore and avoid paying taxes on that income, the IRS on June 18, 2014 announced significant changes to its Offshore Voluntary Disclosure Program, or OVDP, "providing new options to help both taxpayers residing overseas and those residing in the United States. The changes are anticipated to provide thousands of people a new avenue to come into compliance with their U.S. tax obligations" (IRS Makes Changes to Offshore Programs, 2014). On July 1, 2014 reporting requirements under the Foreign Account Tax Compliance Act, or FATCA, became effective. FATCA is "intended to encourage tax compliance and reduce U.S. tax evasion. The approach taken by Treasury and the IRS has been to encourage FFIs [foreign financial institutions] to enter into agreements with the United States to provide information on the accounts of U.S. taxpayers. The "encouragement" is in the form of a 30% withholding tax…" (Kelleher, 2013). With FATCA more international banks (including Credit Suisse) will provide the U.S. Department of Justice with information concerning their U.S. customers (IRS Makes Changes to Offshore Programs, 2014).

***Example.***

In May 2014 Viktor Kordash pleaded guilty to hiding income of approximately $1.5 million offshore in a bank account at Wegelin & Co. in Switzerland (McCoy 2014). On October 30, 2014 in *United States v. Kordash*, No. 14-cr-00345 (S.D.N.Y.), a federal judge sentenced Kordash to a three-month prison term, a three-year supervised release, and payment of over $1 million in back taxes and penalties (Lee, 2014).

**Tips.**

- IRS Commissioner, John Koskinen advises that "For anyone who wants to come into compliance but isn't sure what to do, I recommend talking to a tax professional or going to our website, IRS.gov. (Statement by IRS Commissioner John Koskinen, 2014).
- We encourage taxpayers who are concerned about their undisclosed offshore accounts to come in voluntarily before learning that the U.S. is investigating the bank or banks where they hold accounts. By then, it will be too late to avoid the new higher penalties under the OVDP of 50 percent – nearly double the regular 27.5 percent (Statement by IRS Commissioner John Koskinen, 2014).

## Impersonation of Charitable Organizations

A variety of tactics are used in the impersonation of charitable organizations. Some scammers contact individuals by phone or e-mail to solicit money and funding. Another approach is to contact victims and claim to be working on behalf of the IRS to help victims file casualty loss claims and get tax refunds. Once the perpetrators have gained personal financial information or Social Security numbers they use them to steal identities or financial resources. Bogus websites are also used in the scam to solicit funds for disaster victims (IRS Releases, 2014).

When national disasters or threats (like Ebola) occur, scammers may impersonate charities to get money from well-intentioned taxpayers. "Ebola-related fear is spreading far faster than the virus itself – and, sadly, that means Ebola-related fraud can't be far behind" (Fake charities shoot up faster than Ebola, 2014). To guard the public against Ebola-related charity scams, the Federal Trade Commission (FTC) recommends checking out charities before making a donation and to be "alert for charities that seem to have sprung up overnight in connection with current events" (Tressler, 2014). The Better Business Bureau and AARP's Fraud Watch Network also serve as watchdog organizations for impersonation of charitable organizations (Fake charities shoot up faster than Ebola, 2014).

Many charities are required to file IRS Form 990, Return of Organization Exempt from Income Tax (Form 990, Return of Organization Exempt From Income Tax, 2014). Identity Finder (a software designed to locate personally identifiable information such as Social Security numbers and credit card numbers, that is stored on computers) analyzed 3.8 million Form 990 tax returns for the years 2001-2013 and estimate there are 630,000 Social Security numbers exposed on these forms (Tax Returns Expose SSNs to Public: Study, 2014). This information including your Social Security number is available to the public

***Example.***

Neil Thrasher, from West Bloomfield, Michigan, created "two fake charities: The Paralyzed American Veterans and Disabled Veterans of America. The names used were strikingly similar to two longstanding national organizations that have assisted veterans for years: Paralyzed Veterans of America and Disabled American Veterans. In November 2012 Michigan's Attorney General, Bill Schuette, stated that Thrasher "established fake charities and impersonated legitimate veterans groups for his own gain" (Yearout, 2012). Thrasher was sentenced to a prison term of 17 months to 10 years, and restitution of $29,257 to Paralyzed Veterans of America and $45,143 to Disabled American Veterans (Yearout, 2012).

***Tips.***

- Do not give your Social Security number to any charity. They do not need it.
- Do not carry your Social Security card or your Medicare card (if you have one) as it contains your Social Security number. Make a paper copy of your Medicare card with all your Social Security numbers except the last four digits cut out or scratched out. "Medicare has not found a good solution to removing Social Security Numbers on beneficiaries' cards, a government watchdog warned, leaving open the possibility that stolen cards could easily lead to stolen identities" (Swarts, 2013).
- Check if the charity is a legitimate and financially responsible charitable organization as unfortunately scam charities are "designed to take your money with phony claims of helping the needy. Unfortunately, it's not always easy to distinguish between legitimate fundraisers and unscrupulous solicitors who misrepresent themselves and mislead the public in order to line their own pockets" (How to Spot a Bogus Charity, 2014). Top ten lists of charities that fall into different categories, such as most consistently low rated charities or most followed charities, are available online (Charity Navigator: Your Guide to Intelligent Giving**:** Top Ten Lists, 2014).

## False Income, Expenses, or Exemptions

Another scam listed by the IRS is inflating or including income on tax returns that were not earned in an effort to maximize refundable credits. Reporting income not earned or expenses not paid sometimes affects the earned income tax credit. In addition, some excessive claims may be filed for fuel credits that can result in penalties of up to $5,000 (IRS Releases, 2014).

***Examples.***

A self-employed taxpayer may commit this fraud by claiming personal expenses as business expenses. For example, this individual may claim personal dinner expenses as business expenses; or gas mileage for a personal vacation as a business travel expense; or even a personal cell phone as a business expense.

A fraudulent tax preparer or tax service business may commit this scam, and therefore this is similar to a return preparer fraud. For example, in September 2014 the United States Justice Department filed several lawsuits against Loan Buy Sell (LBS) Tax Services which the government claims filed more than 55,000 tax returns in 2013. Complaints against LBS were that it instructed its preparers to "Falsely claim or increase the amount of the Earned Income Tax Credit" or to "Fabricate businesses and related business income and expenses; Fabricate Schedule A deductions, particularly for unreimbursed employee business expenses" (Justice Department, 2014). One example cited by the Justice Department was that LBS allegedly reported that an individual "had a mechanic business through which he earned income, when he did not" (Justice Department, 2014). Another example was that LBS Tax Services allegedly claimed several false deductions for a lottery winner in order to "offset that income, including $30,141 in charitable contributions and $10,279 in unreimbursed employee business expenses. The customer's tax return allegedly claimed a bogus refund in the amount of $8,247 (Justice Department, 2014).

Another example was the case against Pete Rose, a well-known Major League Baseball player and manager who in 1990 pled guilty to charges of filing false income tax returns (Smith, 1990).

***Tips.***

- Carefully investigate any tax preparer or tax preparation filing company.
- Discuss any concerns over income, expenses, or exemptions with a qualified tax preparer.
- Be honest.

## Frivolous Arguments

Some scammers "encourage taxpayers to make unreasonable and outlandish claims to avoid paying the taxes that they owe" (IRS Releases, 2014). The IRS continues to make taxpayers aware of what constitutes an inappropriate position (Cohn, 2014). The 2014 version of "The Truth about Frivolous Tax Arguments" which was released by the IRS on April 11, 2014 contains three sections: Frivolous Tax Arguments in General; Frivolous Tax Arguments in Collection Due Process Cases, and Penalties for Pursuing Frivolous Tax Arguments (The Truth

about Frivolous Arguments, 2014). Some examples of frivolous arguments listed by the IRS include believing that filing a tax return or payment of federal income tax is voluntary; that only foreign source income is taxable; that only employees of the federal government are required to pay the federal income tax; that the First Amendment permits taxpayers to refuse to pay federal income tax based on their religious or moral beliefs (The Truth about Frivolous Arguments, 2014).

Taxpayers have a right to challenge tax liabilities in the courts, but they do not have the right to "disobey the law or disregard their responsibility to pay taxes" (IRS Releases, 2014). Those who adopt the frivolous position risk a variety of penalties such as the accuracy penalty, civil fraud penalty, an erroneous refund claim penalty, or failure to file penalty. Even criminal prosecution can occur if someone is attempting to evade tax payments. A taxpayer can be convicted of a felony for willfully making and signing returns with false information (IRS Releases, 2014).

***Example.***

The Wesley Snipes trial in 2008 brought to the public's attention the tax scam of a frivolous argument. Snipes contended that only income earned in foreign countries, not income earned in the United States, was taxable (Oldenburg, 2013). According to Robert Wood, a San Francisco tax attorney, Snipes was found guilty of a misdemeanor failing to file, not of a felony of falsely filing (Wood, 2012). "The U.S. taxes all income wherever you earn it. So forget arguing that only foreign-source income is taxable, making your domestic income exempt. There is a convoluted argument that foreign income is different, but don't bother making it" (Wood, 2012).

***Tips.***

- Don't argue that filing a tax return and paying federal income tax is voluntary.
- Don't argue that the term "income" does not include wages, tips, or other compensation received for personal services.
- Don't argue that only income earned in foreign countries is taxable.
- Don't attempt to claim the First Amendment gives the right to not pay federal taxes based on taxpayer's religious or moral beliefs.

## Falsely Claiming Zero Wages or Using False Form 1099

Still another scam identified by the IRS is the use of a false W-2 or 1099 form. These approaches attempt to reduce taxable income to zero. In some cases, a taxpayer may submit a statement challenging wages and taxes reported by the payer. Such schemes can result in being held liable for financial penalties or even criminal prosecution (IRS Releases, 2014).

***Examples.***

The IRS provides numerous examples of non-filer investigations including falsely claiming zero wages or using a false form 1099. The IRS examples "are written from public record documents on file in the courts within the judicial district where the cases were prosecuted" (Examples of Non-filer Investigations – Fiscal Year 2014, 2014). Charles Loewen is one such example.

According to court documents, Charles Loewen, a former National Football League player for the San Diego Chargers and owner of Paradise Stone & Tile, created phony 1099-OID forms and falsely claimed tax refunds for $2,353,173. He also attempted to conceal his income from Paradise Stone & Tile by depositing this income into his wife's bank account. In addition, Loewen falsely claimed zero net income for three years. On July 3, 2014, in Honolulu, Hawaii, Loewen was sentenced to a prison term of 37 months, a supervised release of three years, and an order to pay restitution of $235,288 (Example of Non-filer Investigations – Fiscal Year 2014, 2014).

Another example of filing a false form 1099-OID (Original Issue Discount) is the case of Gerald A. Poynter who on March 13, 2014 was sentenced to 13 years in prison without parole and fined $951,930 for leading a $100 million nationwide tax fraud conspiracy. "Poynter acknowledged that conspirators "prepared and filed 284 fraudulent tax returns from July 1, 2008, to Sept. 21, 2011. Each of the returns contained false claims that the taxpayer listed was due a refund due to over-withholding of taxes, based on fictitious forms 1099-OID" (KC Man Sentence to 13 Years, 2014).

***Tip.***

- Use the 1099 – OID forms to pay taxes "on income received from the interest on their bond investments" (KC Man Sentence to 13 Years, 2014).

## Abusive Tax Structures

Abusive tax schemes are scams that violate the Internal Revenue Code and involve multiple flow-through entities to evade taxes. These schemes usually include limited liability companies, limited liability partnerships, international business companies, foreign financial accounts, offshore credit/debit cards and other similar instruments. These are usually complex and are structured for the purpose of concealing the true nature of taxable income (IRS Releases, 2014).

Abusive tax schemes can be simply "taking unreported cash receipts and personally traveling to a tax haven country and depositing the cash into a bank account. Others are more elaborate involving numerous domestic and foreign trusts, partnerships, nominees, etc." (What are some of the Most Common Abusive Tax Schemes?, 2014).

***Examples.***

International Business Corporations (IBCs) are included in the IRS list of most common abusive tax schemes.

> The taxpayer establishes an IBC with the exact name as that of his/her business. The IBC also has a bank account in the foreign country. As the taxpayer receives checks from customers, he sends them to the bank in the foreign country. The foreign bank then uses its correspondent account …to process the checks so that it never would appear to the customer, upon reviewing the canceled check that the payment was sent offshore. Once

> the checks clear, the taxpayer's IBC account is credited for the check payments. Here the taxpayer has, again, transferred the unreported income offshore to a tax haven jurisdiction. (What are some of the Most Common Abusive Tax Schemes?, 2014)

Willie Nelson's tax return problems illustrate an abusive tax scheme. Willie Nelson's long history with the IRS began in 1984 when the agency chose to review his tax returns back to 1972. After several years and an extensive audit, the IRS presented Nelson with a bill for more than $16 million in underpaid taxes and interest and penalties (O'Brian, 2011). Nelson's accounting firm had filed for the singer every year, but it had claimed tax shelters that the IRS disallowed. The IRS seized most of Nelson's assets (including his musical instruments, platinum records, posters and his recording studio) and sold them at auction. Most were purchased by friends and supporters who gave them back to the singer. The settlement was negotiated down further and Nelson ended up paying it off. He later sued Price Waterhouse, now PricewaterhouseCoopers, and settled with the accounting firm for an undisclosed amount (Johnston, 1995).

***Tip.***

- Taxpayers should verify that tax shelters used in filing their returns are shelters allowed by the IRS.

## Misuse of Trusts

Many times unscrupulous promoters continue to urge taxpayers to transfer large amounts of assets, such as cash and investments, into trusts. Though there are legitimate uses for trusts, the IRS sees many questionable transactions. These promise reduced taxable income, inflated deductions and reductions in a variety of taxes. These transactions commonly occur in the transfer of wealth from one generation to another. The trusts seldom provide the tax benefits promised by the unscrupulous promoters (IRS Releases, 2014).

***Example.***

The IRS provides numerous examples of non-filer investigations including misuse of trusts. The IRS examples "are written from public record documents on file in the courts within the judicial district where the cases were prosecuted" (Examples of Non-filer Investigations – Fiscal Year 2013, 2013). Peter Ian Turner is one such example.

> On June 14, 2013, in Springfield, IL, Peter Ian Turner was sentenced to 18 months in prison, three years of supervised release and ordered to pay $170,030 in restitution. Turner pleaded guilty to one count of tax evasion. According to the indictment, in March 2001 and March 2002, Turner filed a Form W-4, Employee's Withholding Allowance Certificate, in which he falsely represented that he was "exempt" form federal income tax withholding. In addition, in March 2004 Turner and a family member established a trust named "Trinity Consultants" and made themselves the trustees. The purpose and effect of the trust was to defraud the United States by attempting to conceal the defendant's

income and assets. In the summer of 2004, Turner and the family member established another trust, Normandy Contractors, again naming themselves trustees. Turner directed payments he received as a relief pharmacist be made to the trust he established. (Examples of Non-filer Investigations – Fiscal Year 2013, 2013)

***Tips.***

- The IRS reminds taxpayers to seek advice from professionals before entering into a trust arrangement (IRS Releases, 2014).
- The IRS "warned that taxpayers may not eliminate their federal income tax liability by attributing income to a trust and claiming expense deductions related to that trust" (The Truth about Frivolous Tax Arguments Section 1: D to E, 2014).

# Plus 1: A Victim's Story

Although the example that follows is not about a tax return scam case, it is a true story of an identity theft case resulting from credit card fraud and bank identity theft.

The telephone rang. The caller identified herself as an employee with the fraud division of a particular credit card company and asked for a specific individual at that telephone number. The receiver identified himself as that person and was promptly asked if he had authorized a $10,000 balance transfer to his credit card with this company. The receiver had not authorized such a transfer, and a long, frustrating identity theft battle began.

The credit card in question was canceled immediately, and the credit card company stated that a new credit card would be mailed overnight to the victim. No new credit card arrived on the following day. The victim called the credit card company only to learn that the new credit card had been mailed to a fraudulent address. Immediately this second credit card was canceled. The perpetrator had requested a change of address from the victim's correct address to the identity thief's fraudulent address. The credit card company now questioned the victim's true identity and was unwilling to send a third card to what the victim stated was the correct address. The following day a conference call took place between the victim, the credit card fraud department employee, and a representative from one of the three major credit bureaus who asked the victim to send copies of various personal identification information (driver's license, birth certificate, etc.) to the credit bureau in order to establish proof of identity. The credit bureau agreed to place a 7-year fraud alert and would notify the other two credit bureaus to do the same.

The victim filed a police report with the local police department and obtained copies of this report for future use. The next couple of days realized the fast development of additional problems. The victim notified his financial institutions and other credit card companies of the problem. The victim also filed a complaint with the Federal Trade Commission, contacted the Social Security Administration as well as the IRS, called the Department of Motor Vehicles, and spoke with his accountant. The victim obtained current credit reports, and identified from these credit reports several fraudulent addresses, fraudulent telephone numbers, fraudulent credit cards and balances, questionable inquiries, and other concerns.

Within days the bank accounts of the victim's son was wiped out. Many years previous the victim had opened a joint bank account with his son when he first left home for college. Neither the victim nor the son remembered that it was a joint account. The bank agreed to return 50% of the loss to the son and would return the remainder of funds when the case was closed. Fortunately the victim's son had checked his bank account online and reported the theft to the bank within hours of the actual theft.

Months of investigation, hours of long telephone calls, visits to branch banks, and countless moments of frustration followed. Visits and talks with additional police departments and sheriff deputies produced no results. Many weeks of continuous phone calls from the bank's collection agency took place. Each call came from a different person, but all calls stated that the victim (or son) must pay back to the bank the 50% refund given by the bank.

Fortunately for the victim and son, the perpetrator was actually caught, calls from the bank's collection agency seized, and all monies were returned. The victim was still left struggling to bring his credit score back up to where it had been prior to this incident.

The authors developed several tips based on conversations with this victim. These tips are contained in Appendix A (Top Ten Tips to Thwart Trouble) and in Appendix B (Top Ten To-Do Tasks if you become a victim of identity theft).

# Conclusion

According to attorney Steve Weisman the "bad news is that you can't do anything to guarantee that you will not become the victim of identity theft" (Weisman, 2014). Although this is true, this paper suggests many ways tax payers may reduce their risk of becoming a victim of the insidious crime of tax identity theft/ fraud. The authors discussed the "Dirty Dozen" tax scams which are issued annually by the Internal Revenue, provided examples of each scam, offered several recommendations or tips to reduce tax fraud victimization.

One tip the authors suggested is to carefully select a tax preparer, if you use one. A preparer tax identification number is required of all paid tax preparers. But CPA Valrie Chambers warns that "Some people may try to pass their tax preparer identification number off as a license, but it's just an ID from the IRS. It's not a sign of authenticity or knowledge…You want someone with a license, a reputation, a permanent shop…You're giving this person all your information: your Social Security number, your bank routing number" (Renzulli, 2015).

Another tip in this paper is to file early. Troy Lewis, chairman of the American Institute of CPA's tax executive committee, states "You've got to beat the crooks to the punch…Since January 20, it's been open season, and they know that the first filer wins" (Renzulli, 2015).

In summary, the authors 12 tips (which could be called the "Clean Dozen,") are:

- Select a legitimate tax preparer (if you use one).
- File early.
- Be sure your tax preparer's security software is current.

- Use a very strong password if you file your own return electronically.
- Delete tax return information from your hard drive. You may want to store it on an external device.
- File IRS Form 8821.
- Remember the Internal Revenue Service does not contact taxpayers by email, text messages, or social media channels to request personal or financial information.
- If the mobile application is dubious, have it removed and evaluated by a technical team to ensure appropriateness. It is recommended that individuals wait until applications have been thoroughly proven to be secure before downloading
- Do not click on hyperlinks within an email. Type in a company's correct web address.
- Only download from legitimate websites that you know.
- Never give your Social Security number to any charity.
- Check www.charitynavigator.org for various Top Ten Lists of charities.

Identity theft, tax return scams, phishing, and data breaches have become an unfortunate part of the twenty-first century advanced technological world. Although this paper focuses on the problem within the United States, future research needs to investigate the effects of this crime globally.

# References


Becker, B. (2014, October 28). Report: IRS leaves out 500K ID theft victims. Retrieved November 6, 2014, from http://thehill.com/policy/finance/222093-report-irs-leaves-out-500k-id-theft-victims

CBS *60 Minutes*: The Tax Refund Scam. (2014, September 21). Retrieved November 7, 2014, from http://www.cbsnews.com/news/irs-scam-identity-tax-refund-fraud-60-minutes

Charity Navigator: Your Guide to Intelligent Giving: Top Ten Lists. (2014). Retrieved November 13, 2014, from http://www.charitynavigator.org

Cohn, M. (2014 April). IRS Fends Off Frivolous Anti-Tax Arguments. *Accounting Today* (USA) April 11, 2014 Newswire, 2pp, Database: NewsBank.

Consumer Sentinel Network Data Book for January – December 2013. (2014, February). In *Federal Trade Commission Protecting America's Consumers*. Retrieved September 14, 2014, from http://www.ftc.gov/reports/consumer-sentinel-network-data-book-january-december-2013

Equipping Consumers in the Fight Against Identity Fraud: Fraud Prevention Checklist. (2014, February). Retrieved February 4, 2014, from https://www.javelinstrategy.com/brochure/315

Examples of Abusive Return Preparer Investigations - Fiscal Year 2014. (2014). Retrieved December 7, 2014 from http://www.irs.gov/uac/Examples-of-Abusive-Return-Preparer-Investigations-Fiscal-Year-2014

Examples of Identity Theft Schemes – Fiscal Year 2014. (2014). Retrieved December 7, 2014 from http://www.irs.gov/uac/Examples-of-Identity-Theft-Schemes-Fiscal-Year-2014

Examples of Non-filer Investigations – Fiscal Year 2013. (2013). Retrieved December 8, 2014 from http://www.irs.gov/uac/Examples-of-Nonfiler-Investigations-Fiscal-Year-2013

Examples of Non-filer Investigations – Fiscal Year 2014. (2014). Retrieved December 8, 2014 from http://www.irs.gov/uac/Examples-of-Nonfiler-Investigations-Fiscal-Year-2014

Fake charities shoot up faster than Ebola. (2014, October 26). In *The Columbus Dispatch*. Retrieved November 17, 2014 from http://www.dispatch.com/content/stories/business/2014/10/26/fake-charities-shoot-up-faster-than-ebola.html

Famous Fridays: Willie Nelson, The IRS's Most Famous Musician. (2014, January 24). Tax Trials: Developments in Federal and State Tax Litigation. Retrieved December 9, 2014 from http://taxtrials.com/?tag=tax-shelter

Form 8821, Tax Information Authorization. (2014, November 4). Retrieved November 13, 2014, from http://www.irs.gov/uac/Form-8821,-Tax-Information-Authorization

Form 990, Return of Organization Exempt From Income Tax. (2014, April 10). Retrieved November 13, 2014, from http://www.irs.gov/uac/Form-990,-Return-of-Organization-Exempt-From-Income-TaxFormer Carolina Panthers Player Latest Victim of IRS Telephone Scam. Time Warner Cable News. July 18, 2014.Retrieved December 4, 2014 from http://centralnc.twcnews.com/content/news/709946/former-carolina-panthers-player-latest-victim-of-irs-telephone-scam/Harbor Financial Services. "Why Go Offshore?" Retrieved January 31, 2015 from http://www.hfsoffshore.com/why-go-offshore.aspxHastings, Deborah. "IRS warns of sophisticated tax scammers who call your phone." New York Daily News (October 31, 2014). Retrieved December 4, 2014 from http://www.nydailynews.com/news/national/irs-warns-sophisticated-tax-scammers-call-phone-article-1.1994769H.R.744 Stop Identity Theft Act of 2014: Major Actions - H.R.744 - 113th Congress (2013-2014). Retrieved November 12, 2014, from https://www.congress.gov/bill/113th-congress/house-bill/744/actions

H.R.744 Stop Identity Theft Act of 2014: Text – H.R.744 - 113th Congress (2013-2014). (2014, September 9). Retrieved November 12, 2014, from https://www.congress.gov/bill/113th-congress/house-bill/744/text

Holtfreter, R. (2010 May-June). Insidious Dubious Apps: Mobile Banking Phishing Scams. *Fraud Magazine.* Vol. 24, No. 3. Retrieved November 13, 2014, from http://www.acfe.com/article.aspx?id=4294967562

How to spot a bogus charity. (n.d.). Retrieved November 15, 2014, from http://www.volusiasheriff.org/charity.htm

IRS Employee Indicted in Connection with the Electronic Filing of a Fraudulent Tax Return. (2014, October 14). In *TIGTA Treasury Inspector General for Tax Administration Highlights*. Retrieved November 13, 2014, from http://www.treasury.gov/tigta/oi_highlights.shtml#75

IRS Makes Changes to Offshore Programs; Revisions Ease Burden and Help More Taxpayers Come Into Compliance. (2014, June 18). Retrieved December 9, 2014 from http://www.irs.gov/uac/Newsroom/IRS-Makes-Changes-to-Offshore-Programs;-Revisions-Ease-Burden-and-Help-More-Taxpayers-Come-into-Compliance

IRS Releases the "Dirty Dozen" Tax Scams for 2014; Identity Theft, Phone Scams Lead List. (2014, February 19). Retrieved April 23, 2014, from http://www.irs.gov/uac/Newsroom/IRS-Releases-the-%E2%80%9CDirty-Dozen%E2%80%9D-Tax-Scams-for-2014;-Identity-Theft,-Phone-Scams-Lead-List

IRS Repeats Warning about Phone Scams. (2014, August 13). Retrieved August 14, 2014, from http://www.irs.gov/uac/Newsroom/IRS-Repeats-Warning-about-Phone-Scams

IRS Warns of New Email Phishing Scheme Falsely Claiming to be from the Taxpayer Advocate Service. (2014, March). Retrieved from http://www.irs.gov/uac/Newsroom/IRS-Warns-of-New-Email-Phishing-Scheme-Falsely-Claiming-to-be-from-the-Taxpayer-Advocate-Service

Johnston, D. (1995, November 4). Tax Shelter of Rich and Famous has Final Date in Court. Retrieved December 10, 2014 from http://www.nytimes.com/1995/11/04/business/tax-shelter-of-rich-and-famous-has-final-date-in-court.html

Justice Department Sues Regional Tax Preparation Firm's Owner and Franchisees and Managers To Stop Alleged Systematic and Pervasive Tax Fraud. (2014, September 24). Retrieved December 11, 2014 from http://www.justice.gov/tax/2014/txdv141030.htm

KC Man Sentenced to 13 Years for Leading $100 Million Nationwide Tax Fraud Conspiracy. (2014, March 13). The United States Attorney's Office Western District of Missouri Press Release. Retrieved December 9, 2014 from http://www.justice.gov/usao/mow/news2014/poynter.sen.html

Kelleher, J. M. (September 1, 2013). FATCA Regulations' Effective Date Approaching Quickly. *The Tax Adviser*, 586-588. Retrieved February 1, 2015 from http://www.aicpa.org/publications/taxadviser/2013/september/pages/clinic-story-06.aspx

Lauridsen, M. (2014, July). Tax Simplification: Key to Fighting Tax Return Identity Theft. *The Tax Adviser*, 506-507.

Lee, M. Wegelin & Co. Account Holder Sentenced to Prison Term. Tax Controvery Watch (November 2, 2014). Retrieved from http://taxcontroversywatch.com/2014/11/02/wegelin-co-account-holder-sentenced-to-prison-term/

McCoy, K. (2014 May). Businessman admits hiding $1.5M offshore. USA Today Online (May 27, 2014). Retrieved December 5, 2014 from http://www.usatoday.com/story/money/business/2014/05/27/kordash-offshore-tax-evasion-plea/9644527/

O'Brian, G. (2011, March). 10 Celebrities Convicted of Tax Evasion. Retrieved December 9, 2014 from https://www.legalzoom.com/articles/10-celebrities-convicted-of-tax-evasion

Oldenburg, Ann. (2013, April). Wesley Snipes finishes jail time for tax evasion. *Forbes*, April 5, 2013. Retrieved December 7, 2014 from http://www.usatoday.com/story/life/people/2013/04/05/wesley-snipes-finishes-jail-time-for-tax-evasion/2057455/

Renzulli, K. A. "7 Way to Keep Your Money Safe from Thieves" (2015, January 26). Retrieved January 31, 2015 from http://time.com/money/3678278/tax-refund-fraud-identity-theft/

Scam Phone Calls Continue; IRS Identifies Five Easy Ways to Spot Suspicious Calls (2014, August 28). Retrieved August 29, 2014, from http://www.irs.gov/uac/Newsroom/Scam-Phone-Calls-Continue;-IRS-Identifies-Five-Easy-Ways-to-Spot-Suspicious-Calls

Scam Phone Calls Continue; IRS Unveils New Video to Warn Taxpayers (2014, October 31). Retrieved November 16, 2014 from http://www.irs.gov/uac/Newsroom/Scam-Phone-Calls-Continue-IRS-Unveils-New-Video-to-Warn-Taxpayers

Sciammacco, S. (2014, November 12). New Guide Warns of Dirty Dozen Food Additives. Retrieved on November 12, 2014, from http://www.ewg.org/release/new-guide-warns-dirty-dozen-food-additives

Smith, C. (1990, July 20). New York Times. Rose Sentenced to 5 Months For Filing False Tax Returns. Retrieved December 11, 2014 from http://www.nytimes.com/1990/07/20/sports/rose-sentenced-to-5-months-for-filing-false-tax-returns.html

Statement by IRS Commissioner John Koskinen. (2014, June 18). Retrieved December 9, 2014 from http://www.irs.gov/uac/Newsroom/Statement-of-IRS-Commissioner-John-Koskinen

Swarts, P. (The Washington Times, October 18, 2013). Medicare cards still put Social Security Numbers at risk. Retrieved March 1, 2014 from http://www.washingtontimes.com/news/2013/oct/18/medicare-cards-still-put-social-security-numbers-r/#ixzz2up95AYv7

Tax Returns Expose SSNs to Public: Study. Retrieve November 13, 2014, from http://www.identityfinder.com/us/business/lookup990

The Truth about Frivolous Tax Arguments. (2014, March). Retrieved December 7, 2014 from http://www.irs.gov/Tax-Professionals/The-Truth-About-Frivolous-Tax-Arguments-Introduction

The Truth about Frivolous Tax Arguments Section 1: D to E (2014, March). Retrieved December 7, 2014 from http://www.irs.gov/Tax-Professionals/The-Truth-About-Frivolous-Tax-Arguments-Section-I-D-to-E

There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft: Highlights of Reference Number: 2012-42-080 to the Internal Revenue Service Commissioner for the Wage and Investment Division. (2012, July 19). Retrieved November 12, 2014, from http://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.html

TIGTA recommends identity theft safeguards. (2012, October 2012). Retrieved November 12, 2014, from http://www.journalofaccountancy.com/Issues/2012/Oct/TaxMatters.htm?action=print

Tressler, C. (2014, October 16). How to guard against Ebola-related charity scams. Retrieved November 15, 2014 from http://www.consumer.ftc.gov/blog/how-guard-against-ebola-related-charity-scams

Two More Defendants Sentenced in Stolen Identity Tax Refund Scheme Resulting in Millions of Dollars in Fraudulent Activity. (2014, July 7). Retrieved from http://www.fbi.gov/miami/press-releases/2014/two-more-defendants-sentenced-in-stolen-identity-tax-refund-scheme-resulting-in-millions-of-dollars-in-fraudulent-activity

Weisman, S. (2015). *Identity Theft Alert: 10 Rules You Must Follow to Protect Yourself from America's #1 Crime* (pp. 1- 174). Upper Saddle River, NJ: Pearson Education.

What Are Some of the Most Abusive Tax Schemes? (2014, February 12). Retrieved December 9, 2014 from http://www.irs.gov/uac/What-are-some-of-the-Most-Common-Abusive-Tax-Schemes%3F

Wood, R. (2012, August). Wesley Snipes Turns 50 in Prison But Didn't File False Tax Return." *Forbes,* August 1, 2012. Retrieved December 7, 2014 from http://www.forbes.com/sites/robertwood/2012/08/01/wesley-snipes-turns-50-in-prison-but-didnt-file-false-tax-return/

Yearout, J. (2012, November 14). Schuette Announces Prison Sentence and Restitution Ordered in Face Veterans Charity Scam. Retrieved December 8, 2014 from http://www.michigan.gov/ag/0,4534,7-164-17337_18095_56114-289878--,00.html

2014 Identity Fraud Report: Card Data Breaches and Inadequate Consumer Password Habits Fuel Disturbing Fraud Trends (2014, February). In *Javelin Strategy & Research*. Retrieved September 14, 2014, from https://www.javelinstrategy.com/brochure/314

# Appendix A

## Top Ten Tips to Thwart Trouble

- Obtain annual free credit report from each of the three major credit bureaus (stagger quarterly for year-round monitoring). Report any discrepancies in writing by mail

immediately to the credit bureaus. Order your free annual credit report at: www.annualcreditreport.com or call 877-322-8228.

- Change your passwords often. Avoid using easily obtainable information (high school, mother's maiden name, your pet's name) in your password.
- Do not use the same password for multiple sites. Use different passwords for different sites.
- Don't carry your SSN! Leave it home! If a company requests your SSN, ask them to request a different form of identification.
- Don't carry your original Medicare card. Make a paper copy of your Medicare card with all your Social Security numbers except the last four digits cut out or scratched out.
- Prepare Now! Search the web for protection tips.
- Consider subscribing to a credit monitoring service.
- Use a cross-shredder to shred sensitive information, such as unsolicited credit card applications, financial statements, or billing statements
- Check your credit card and bank statements frequently!
- NEVER transmit personal and financial information if you use a public Wi-Fi spot.

# Appendix B

## Top Ten To-Do Tasks (if you become a victim)

- File a report with local law enforcement; obtain a copy of this report.
- Report the theft to the Federal Trade Commission.
- Check your credit report for all incorrect information (unfamiliar addresses, incorrect telephone numbers, debts not incurred; credit inquiries for others' loans); dispute everything that is incorrect with your credit report in writing by mail.
- Contact one of the three major credit bureaus and ask for an extended alert on your credit report (The credit bureau you call will notify the other credit bureaus).
- Report the theft to the Social Security Administration
- Contact credit card companies; close any affected accounts.
- Consider credit freeze.
- Contact affected banks.
- Contact Immigration Services (if passport is stolen).
- React with your head, not your heart! In other words, THINK and try not to be emotional.