Spring 2019

A Holistic View of Identity Theft Tax Refund Fraud

Andrew J. Hultgren
University of New Hampshire, Durham

A Holistic View of Identity Theft Tax Refund Fraud

Andy Hultgren, UNH Honors Undergraduate Student
John Hasseldine, Ph.D, FCCA

Faculty Advisor and Co-Author: Dr. John Hasseldine

A thesis submitted in partial fulfillment of the requirements for the degree of
BACHELORS OF SCIENCE IN BUSINESS ADMINISTRATION:
ACCOUNTING & FINANCE
at the
UNIVERSITY OF NEW HAMPSHIRE

2019

Table of Contents

Abstract

This thesis attempts to explain what identity theft tax refund fraud is and how the issue has developed over the years. It presents a holistic, historic view of the problem as well as how it has been addressed. It primarily relies on reports from the Internal Revenue Service (IRS), Treasury Inspector General for Tax Administration (TIGTA), Government Accountability Office (GAO) and National Taxpayer Advocate (NTA) in its assessment. It does not examine foreign tax administrations' methods of dealing with identity theft refund fraud or the extent of the issue in other principalities, and therefore this is an area in need of further research. This thesis does not attempt to make an argument for the efficacy of funding for the IRS either, which is an area that could be further studied. It also does not deal with employment related identity fraud, which some relate to identity theft refund fraud.

Background

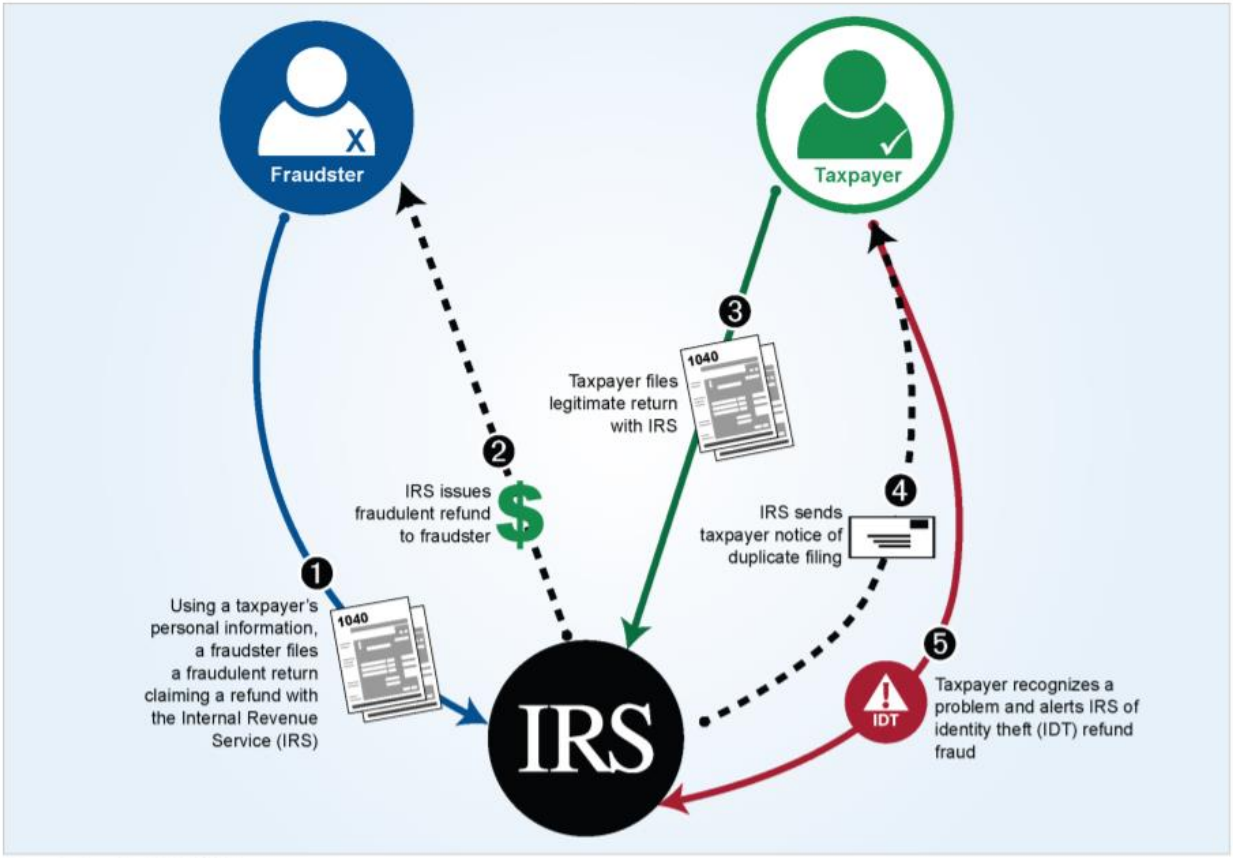
Identity theft (IDT) tax refund fraud has become a growing issue for the Internal Revenue Service (IRS) throughout the years, as well as at a state level. The first recorded instance of this type of fraud occurred in 1988 as the *Los Angeles Times* reported that Donald Penrod had been indicted with the first ever charge of fraudulently filing tax forms electronically to receive an illegitimate refund (Nigrini & Peters, 2018). By 1992 the Government Accountability Office (GAO) identified the filing of fraudulent returns electronically as a major issue to be monitored and throughout the 2000s this issue continued to increase (GAO, 1992).

This type of fraud is especially appealing to fraudsters due to their relative anonymity which makes prosecuting the perpetrators quite difficult. It also can be conducted by either an individual or a conglomerate. The exponential growth of the fraud occurred as in the Information Age, people's personally identifiable information (PII) is easier to obtain and the massive growth in e-filing allows this fraud to be perpetrated on a large scale. E-filing has drastically increased throughout the 21st century as in 2008 only 58% of returns were filed electronically, but this escalated to 81% in 2012 and to over 90% in 2016 (Weisman, 2017; Brody, Haynes, & Mejia, 2014). The IRS first recognized this as a problem at large when they issued their "Dirty Dozen" list of tax scams in 2011 when they grouped tax refund fraud in with phishing, but then escalated their evaluation of the problem the subsequently in 2012 as that year identity theft topped the list (McKonly & Asbury, 2011; Gudmundson, 2012). This was after IDT tax refund fraud had already grown to a substantial level and therefore the IRS was late in their assessment of the issue at hand, although they had taken some actions to prevent it before the Dirty Dozen was released. This paper will attempt to explain the development of this method of fraud and how the IRS has addressed it as well as external group's assessments of the IRS's actions.

Execution

The actual execution of the fraud is relatively straightforward and comprises three main parts that experts agree upon. It begins with a fraudster obtaining a victim's PII such as their name and social security number (SSN) at a bare minimum and then using this to file a fraudulent tax return that provides them with a refund which is mailed to an address, or more often directly deposited to a bank account or prepaid debit card. When the legitimate taxpayer consequently files their return, it will be denied and they will be forced into undertaking a lengthy process to right it (Thorne & Stryker, 2014; Holtfreter, McLeod, & Harrington, 2014). This is exemplified graphically through this depiction from the GAO's 2016 report on the issue.

Figure 2: Example of a Successful Identity Theft Refund Fraud Attempt



Source: GAO analysis. | GAO-16-508

Note: This figure's numbering shows the order in which events occur when fraudsters successfully commit IDT refund fraud.

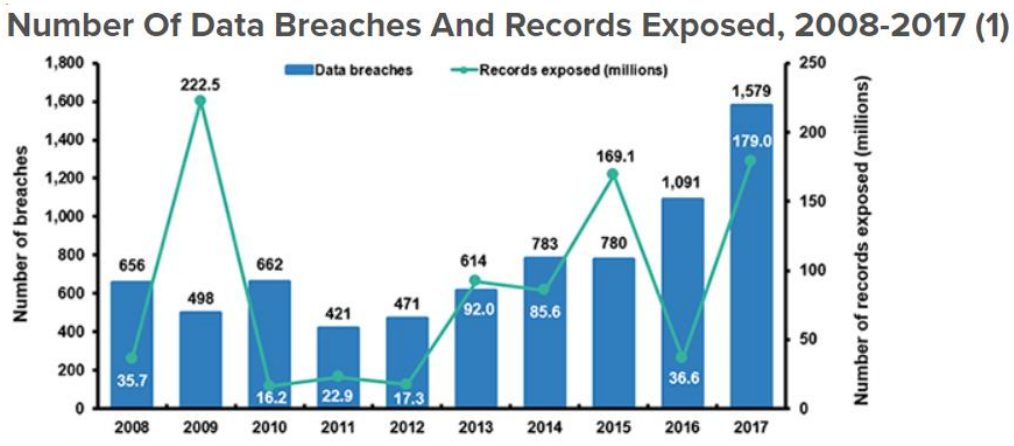
For the fraudster, obtaining the victim's PII is the initial barrier to perpetrating IDT refund fraud. Unfortunately, this is relatively easy in the modern era as fraudsters use a variety of tactics to obtain such information. One rampant method is through phishing. Phishing is when a fraudster contacts a potential victim through a medium such as telephone or email and poses as a legitimate enterprise such as one scam where fraudsters posed as the IRS in an email. The email will then direct the victim to a webpage that seems legitimate and thus the victim will enter in their information for some purpose, such as it being requested for their refund to be processed or to avoid a fee, or this link will download malware onto the victim's computer and then probe for their PII (Chambers & Zeidan, 2013). A recent major phishing scheme took place as fraudsters posed as company executives emailing their payroll and human resource departments requesting employees PII and their W-2s (GAO, 2018).

A method that has been all too common is employees stealing PII from databases through their employment and then either using the PII to file fraudulent returns themselves or selling it to fraudsters. There are many such businesses/institutions that have databases with vast amounts of PII that are necessary to their operation. There have been recorded instances of employees in prisons, educational institutions, medical facilities, and even within the IRS itself illegally downloading vast amounts of PII from databases for the purpose of committing IDT tax refund fraud (Nigrini & Peters, 2018).

Even the PII of deceased individuals can be used to commit this fraud. In the past this information was incredibly readily available as it was posted in newspaper obituaries. This took its form in the modern era as sites that provide individuals with hereditary data such as Ancestry.com and Genealogy.com reported SSN's of deceased individuals, although since then many have stopped this practice due to pressure from the IRS (Fisk & Stigile, 2012).

Another major technique employed by fraudsters is the old-fashioned technique of obtaining/stealing physical documents/equipment with PII on it. Fraudsters may "dumpster dive" and look through the trash of individuals looking for "discarded tax returns, bank records, credit card receipts or other records containing personal and financial information" or even discarded laptops that contain such info which they could use to perpetrate the fraud (Chambers & Zeidan, 2013). They may obtain such data through home robbery where they steal documents with PII or via pickpocketing a person's wallet, purse, or phone. They may even steal someone's mail either straight from their mailbox or more diabolically submit a change of address form to divert mail to an ulterior location (Fisk & Stigile, 2012).

Lastly a method that is becoming more and more pressing is the purchase of PII from mass data breaches and hacking attempts (Nigrini & Peters, 2018). This enables groups to commit substantial amounts of IDT tax refund fraud and the sum of data exposed by breaches is increasing at an alarming rate as this graph from the Identity Theft Resource Center portrays.



Large scale data breaches are practically becoming commonplace, such as the Equifax breach in 2017 which compromised varying amounts of PII for 143 million American consumers, or 44% of the population, further arming fraudsters of all types of IDT fraud (Marcus, 2018).

The actual creation of the fraudulent return is a relatively straightforward process. Unfortunately, the IRS does not release detailed information on what schedules are used or what kinds of numbers fraudsters use for the withholdings and credits as this would essentially create a series of step by step instructions on how to commit the fraud. It is relatively simple to make a return where the taxes due are less than the payments and credits, therefore generating a refund for the fraudster (Nigrini & Peters, 2018). Nowadays the more complex aspect of the fraud is creating a fraudulent return that is convincing enough to bypass the IRS's filters, which will be discussed later. The filters have gradually become more advanced throughout the years, thus causing fraudsters to continually evolve and hone their craft, creating gradually more convincing returns every year (IRS, 2018). The National Taxpayer Advocate (NTA) notes one such new, more sophisticated scheme where criminals use employer identification numbers (EINs) to file business tax returns that are fraudulent (2017). This means it is necessary for the IRS to continue to remain vigilant and anticipate these developments in the fraud so they can stop it preemptively.

The final step in the fraud is to actually obtain the refund from the IRS. The vast majority of fraudsters use prepaid debit cards or direct deposits, with a slight favoring for prepaid debit cards as these can be anonymously deposited without any direct tie to the fraudster (Chambers & Zeidan, 2013). There was a massive flaw in the tax system early in the decade where many returns could be filed with the same address, as according to the Treasury Inspector General for Tax Administration (TIGTA) over 2,000 returns were filed to an address in Lansing, Michigan as well as hundreds of returns being filed to other various addresses (2012). Thankfully, this issue as well as the issue of multiple returns being sent to an anonymous bank account have been alleviated as of October 15, 2013 thanks to IRS actions (TIGTA, 2012). Now refunds must be

made to a bank account or debit card in the taxpayer's name and the number of refunds allowed to go to a single source have been limited to three, but this has obviously not been enough to prevent this step of the fraud altogether.

Historical Assessment

Historically, the IRS was slow in assessing IDT tax refund fraud as a major issue. As was stated previously, the IRS did not seriously address this type of fraud with their Dirty Dozen list of scams until 2012 at which point the amount of attempted IDT refund fraud had already reached $20.7 billion by conservative estimates (Gudmundson, 2012). IDT tax refund fraud was increasing exponentially prior to this as it had doubled from 2011-2012 by some estimates (White, 2012). It should be noted that at this point the IRS was taking measures to combat this fraud as the next section will go into, but it was around this time that their efforts were of high priority within the organization. Throughout the years since then, identity theft has remained high on the Dirty Dozen list as it has vacillated between the first and third spots on the list throughout the subsequent years from 2013-2019 with it taking the 3rd spot in 2019 as the IRS notes that despite making "major improvements" IDT refund fraud is still a constant issue and threat to taxpayers who must remain vigilant (IRS, 2019).

Conversely, numerous other organizations realized the drastic increase in IDT refund fraud and were already making suggestions to combat it prior to the IRS's inclusion of it on the Dirty Dozen with several notable organizations being the GAO, NTA and TIGTA. The Government Accountability Office (GAO) first did an audit on electronic filing fraud back in 1992 when the system was first starting to experience major problems and the amount of refund fraud was in the millions rather than billions (Nigrini & Peters, 2018). Additionally, the NTA featured this method of fraud as one of their most serious problems in 2005 and noted that there

was an additional TIGTA report on identity theft that asserted the IRS had no concrete corporate strategy in place to address the growing concern of the fraud (NTA, 2005). In this report, it is noted that the number of complaints about tax return fraud that were sent to the Federal Trade Commission (FTC) had increased from 1.9% of their total complaints in 2002 to 3.8% of the total complaints in 2004. While this may not seem to be a rather significant number, it shows that the issue had escalated twofold in just three years' time. In 2007, both the NTA and TIGTA did an analysis of the problem and found that there had been a 396% increase in the total number of complaints directed to the FTC, which is the only substantial indicator of the issue given that the IRS did not begin closely monitoring it until later (Phillips, 2007; NTA, 2007). This trend continued as a report from the GAO noted that the total number of incidents of tax-related identity theft nearly quintupled from 2008-2010 as it grew from 51,702 to 248,357 cases (White, 2011) Overall, since 2005 the problem continued to worsen as shown by the fact that it has been consistently listed as one of the NTA's most serious problems (aside from 2006, 2010 and 2014 oddly), leading to increased IRS action regarding the phenomena throughout the last decade.

IRS Actions

While the IRS may have been late to address IDT tax refund fraud, it has undertaken substantial measures to combat the problem. Many of these solutions have come in part from recommendations from the GAO, TIGTA, and NTA as their annual reports on the issue routinely offer assistance. As the previous section suggests, the IRS has been slow to act and a 2012 NTA report shows just this. Within this report is a table that outlines various recommendations that the NTA had made within its annual congressional reports and their implementation years. While it is only a small sample size of eight recommendations from a single organization, it took the IRS an average of 4.38 years to implement the policy recommendation which is a shockingly long

amount of time even for a government entity (NTA, 2012). The NTA has critiqued the IRS overall as taking a reactive stance to IDT tax refund fraud as they have continuously advocated for a more proactive approach (NTA, 2007). It should also be noted that overall the IRS has sought to prevent individuals from being able to commit refund fraud rather than prosecute specific people as they have assessed this as being the more affective approach (Nigrini & Peters, 2018). Despite this, the Criminal Investigation branch of the IRS did manage to convict approximately 2,000 identity thieves from the years of 2013-2015 ("IRS States and Tax," 2016).

Over the years the IRS has developed their techniques, administrative bodies, and systems for dealing with IDT tax refund fraud. In 2005 they officially established the Identity Theft Program Office, later creating the Privacy, Information Protection, and Data Security and the Identity Theft and Incident Management office with an accompanying Advisory Committee in 2007 (NTA, 2007). In 2008, they began marking taxpayers accounts within the IRS database if they had been victims of this fraud, therefore helping to coordinate their efforts to help taxpayers across various divisions. They also established the Identity Protection Specialized Unit to help taxpayers who had been victims as well as a toll-free hotline for victims to get a better understanding of the process that they would need to complete (NTA, 2008).

In 2009 the IRS began implementing a series of filters or "business rules" that could automatically assess if a return seemed fraudulent and flag it for screening by an actual IRS employee. They also created the Identity Theft Affidavit, IRS form 14039 (which is still used to this day) in April 2009 so that taxpayers who knew they were victims of IDT tax refund fraud could notify the IRS of the issue, thereby streamlining the process somewhat for identity confirmation. Lastly, in this year they started their educational campaign against falling victim to identity theft. By educating taxpayers and practitioners on methods to prevent falling prey to

identity theft, the IRS could effectively diminish the tax related identity theft fraud and therefore was involved in over 40 events throughout the year, six of those being Nationwide Tax Forums (NTA, 2009).

From 2010-2011 the IRS began increasing their efforts against IDT tax refund fraud. In 2010 they implemented the Electronic Fraud Detection System, which is still in place to some extent to this day. This was a more developed form of the filters that they had used previously as it would analyze returns both based on a series of general filters and based on past years returns. From there it could "score" the returns and determine a probability of them being fraudulent, with those scoring above a certain percentage being subject to further screening and extremely high scores being treated as fraudulent automatically (TIGTA, 2010). In 2011 they created the Enhanced Return Processing program which sought to coordinate efforts throughout the IRS' various divisions as an NTA report found that 28 different subunits were involved in activities regarding identity theft (NTA, 2011). From this came a program that sought to quell the number of fraudulent returns being filed with deceased individuals' information. They accomplished this to some extent by working with the Social Security Administration (SSA) to begin marking the IRS accounts of deceased individuals and putting pressure on sites such as Ancestry.com to stop listing the PII of decedents (Fisk & Stigile, 2012).

As 2012 was the first year that the IRS listed IDT tax refund fraud on its Dirty Dozen tax scams, it is unsurprising that this year a number of improvements were made in the fight against fraudsters. This is due to the fact that the IRS assigned ample resources in this year as around 3,000 employees were dedicated to the issue and over $300 million was spent on it (Nigrini & Peters, 2018). One of the most substantial programs that the IRS further developed this year was the Identity Protection Personal Identification Number (IP PIN) program which began being

created in 2010 (NTA, 2012). This involves a taxpayer being assigned a specific IP PIN that they must use in order to file their return electronically, the medium that the fraud takes place in a for the most part. The only taxpayers who are outright assigned an IP PIN are those who have been victims of IDT tax refund fraud in the past, but additionally it was offered to taxpayers in Florida, Georgia, and the District of Columbia to opt into as these were the areas that the IRS assessed have the highest fraud rate per capita (Hammel & Murolo, 2016). In total, 251,500 IP PIN's were issued in 2012 and 12,936 taxpayers filed using an incorrect PIN, but this was later established to largely be due to human error when entering the PIN and not a problem with the system (White, 2012). The NTA report does note one issue with the program in that the IP PINs are all issued in one batch annually instead of issuing a PIN with every individual case that is brought to them throughout the year (NTA, 2012). Moreover, the IRS continued in its efforts to educate taxpayers through a digital approach. They created www.IRS.gov/identitytheft on which they regularly post the most up to date info on IDT tax refund fraud and also created a series of YouTube videos and podcasts titled *ID Theft: Protect Yourself from Identity Theft and ID Theft: Are You a Victim of Identity Theft?* in an attempt to reach a younger demographic (Fisk & Stigile, 2012). In 2012 they also decentralized their efforts to increase specialization and "utilize the unique skill sets and experience of dedicated employees" by creating 21 specialized subunits to address the issue, but unfortunately this approach did not see much success (NTA, 2012).

Additionally, a formal department was created to analyze the returns identified by the filters known as the Taxpayer Protection Program (TPP) which would also work with legitimate taxpayers who were falsely screened (TIGTA, 2018). Lastly, they created the Refund Fraud and Identity Theft Global Report, commonly referred to as simply the "Global Report." This sought to consolidate and condense information about IDT tax refund fraud from various IRS divisions,

and even other governmental bodies into one, standalone report. This would be used to further coordinate the IRS's efforts and serve as a management tool for responding to the issue. This was significant as previously subunits could be very compartmentalized and therefore this was seen as an excellent opportunity to create a more consistent strategic view (White, 2012).

Through 2013 and 2014 progress was not as rapid. As was stated earlier, the IRS implemented a ruling that limited the number of refund deposits made to a single bank account or prepaid debit card to three (Nigrini & Peters, 2018). In this same vein they also mandated that the account be in the filers name in an attempt to interfere with the second step of the fraudsters in acquiring the refund (TIGTA, 2012). A minor improvement was made to the IP PIN program in 2014 as previously taxpayers could only receive IP PINs and replacement PINs through the mail, but this year an online portal was created for PIN holders to retrieve their PIN (NTA, 2013). Congress also showed an interest in abating the fraud as they passed the Stop Identity Theft Act of 2014 (Thorne & Stryker, 2014). This increased penalties for committing the crime and also mandated the Department of Justice to collaborate with the IRS on future efforts and to provide an annual report to Congress with updates. To help with the analysis of the issue, the *Identity Theft Taxonomy*, or simply the *Taxonomy* was created to actually track and determine the amount of IDT tax refund fraud that was attempted and the amount of refunds actually issued to false filers, as previously the IRS was relying mostly on estimates (GAO, 2014).

In 2015 the IRS recommitted itself to preventing IDT tax refund fraud as it committed over 4,000 full-time employees or equivalents and spent approximately $470 million, but it noted that even more funding would prove useful (GAO, 2016). A major part of these efforts was revamping the Electronic Fraud Detection System (EFDS) as they began testing the new Return Review Process (RRP) which had been in development since 2009 (GAO, 2015). While the two

systems were running congruently, the system was known as the Dependent Database due to the fact that it would take time for the RRP to handle the full load of returns. The major benefit of the RRP is that in addition to the filters that were used in previous systems that relied on binary analysis, the RRP's filters consisted of both rules and models. Additionally, the system is much more flexible and fluid as it is much easier to make amendments to than the EFDS. Its efficacy was seen in the first year as its false detection rate (FDR), or in other words the percent of legitimate returns it flagged as fraudulent was only 37.9% in comparison to the EFDS' FDR of 54.5% (NTA, 2016). This year the IRS also consolidated their IDT victim assistance functions into the Wage and Investment division, doing away with the 21 specialized units that was established in 2012 in response to the Tax Refund Prevention Act of 2014, which was proposed by Senator Hatch from Utah, a longtime proponent of prevention (NTA, 2014). A major benefit of this would be that a victim of the fraud would now have all their communications with the IRS be through a single point of contact, instead of having to deal with numerous employees across different departments. There would still be some cases that would require special attention, but the majority of standard cases would now be streamlined, which the NTA advocated for in many prior years (2016). It was also reported that in this year they had increased the number of taxpayer accounts that had been marked as deceased to around 28.4 million (TIGTA, 2015).

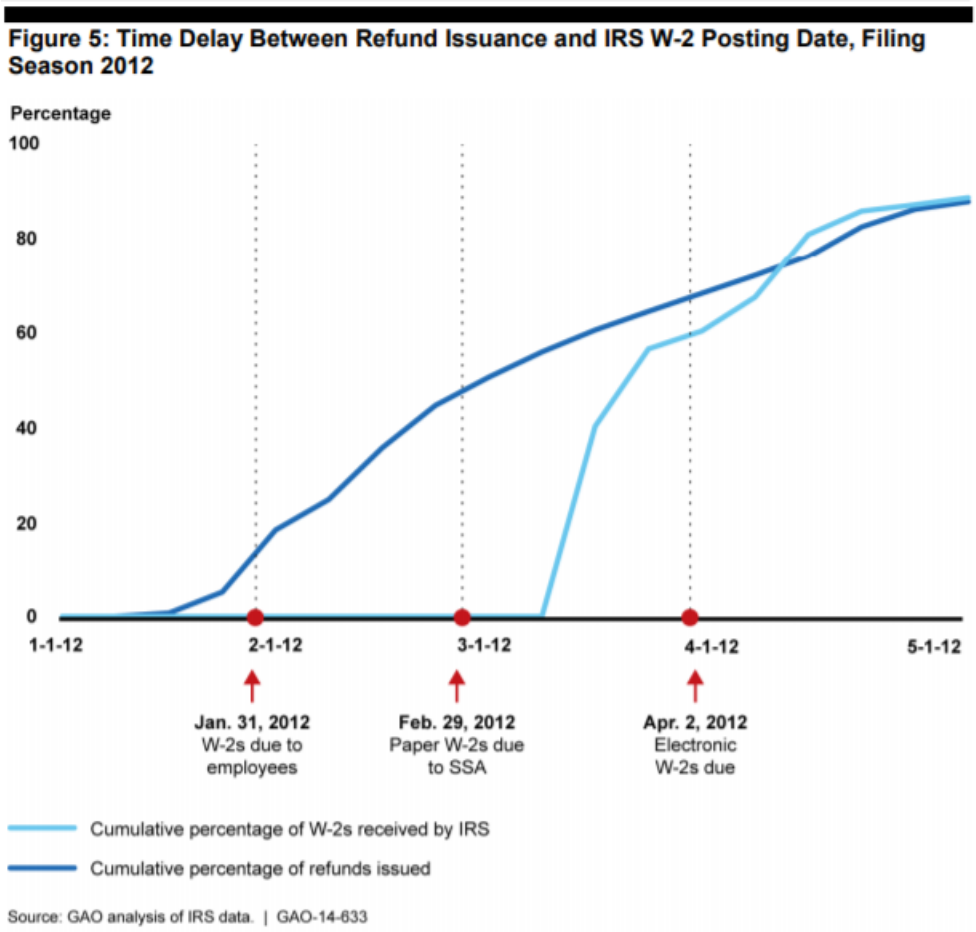
The undertaking from this year that will likely have the most profound effect going forward was the creation of the Security Summit, which was a meeting between "IRS officials, the chief executive officers (CEOs) of the leading tax preparation firms, software developers, payroll and tax financial product processors, and state tax administrators" to discuss ways they could collectively address IDT tax refund fraud (IRS, 2015). From this a public-private partnership was formed consisting of three working groups, these being based around

authentication methods, information sharing techniques, and a Strategic Threat Assessment and Response (STAR) working group that was designed to anticipate future issues. Out of these working groups came various ideas and initiatives such as improving the data elements in the filters and furthering external identity proofing procedures. They also worked on developing the External Leads Program for "financial institutions, software companies, prepaid card companies and other third parties" to share information with the IRS about developing trends in identity theft (IRS, 2015). Finally, they discussed creating the framework for the Tax Ecosystem Refund Fraud Information Sharing & Assessment Center (ISAC) and NIST Cybersecurity Framework (first proposed in 2014) to further contest fraudsters (IRS, 2015).

In 2016 some of the work of the Security Summit came to fruition as it further split into seven work groups. The Communication and Taxpayer Awareness Work Group launched several programs aimed at educating taxpayers and tax preparers such as "Taxes. Security. Together.", "Protect Your Clients; Protect Yourself" and the "National Tax Security Awareness Week" gaining nationwide media coverage ("Despite Major Progress," 2018). The Authentication Work Group collaborated with tax software providers to create uniform, more secure standards for password creation and security questions and the Information Sharing Work Group worked with these software providers to share confidential data elements from tax returns with the IRS. The Authentication Work Group also introduced a pilot program to add a 16-digit verification code to 2 million Forms W-2, *Wage and Tax Statements* in order to confirm that the submitted W-2s were real, accurate forms (Murolo, 2016). This would help prevent fraudsters from being able to concoct fictitious W-2s as it would create this additional verification step, thus forcing the fraudsters to either steal accurate W-2s to acquire the code, therein making the fraud more

complicated. The IRS planned on furthering the program to be included on 50 million W-2s in 2017 with hopes of eventually making it a national, all-inclusive program.

In 2017 another massive advancement was made regarding W-2s in the effort against IDT tax refund fraud, this being the accelerating of the W-2 deadline submission for employers. Although this had been suggested as early as 2011 and had been reiterated by numerous organizations for several years, it took so long because it required being passed by Congress to be implemented (White, 2011). As this graphic shows, previously W-2s were not due to the SSA



until February 29th in paper form and April 2nd electronically, quite late into the filing season (GAO, 14). There was an additional delay between when the SSA received the forms and when they would be sent to the IRS. This has been a problem due to the fact that it meant the IRS

could not match W-2 information to tax returns in real time, as shown by the fact that they had already issued nearly 60% of all refunds before they received a single W-2. This issue is further worsened by the fact that fraudsters would usually file very early in the tax season in an attempt to file before the legitimate taxpayer. However, in 2016 the passing of the Consolidated Appropriations Act moved the deadline for filing W-2s up to January 31st (although there would be some delay in them being transferred from the SSA to the IRS) for the 2017 tax season so that the IRS could match tax return information to W-2 information in real time (GAO, 2016). It has been noted that this may cause an increase in the correction rate of W-2s by employers causing them to have to resubmit them, but there is little research done on this currently. Additionally, there has not been any research into whether or not this has increased costs for private companies, but it should not be substantial as January 31st was previously the deadline that employers had to provide W-2s to their employees. Moving the deadline forward has proven to be effective as there was a 30% increase in received W-2 forms by March of 2017 ("Objectives Report," 2017).

There were numerous other measures in 2017 that were realized as well, notably the creation of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center (ISAC). The idea of Information Sharing and Analysis Centers was created in 1988 with Presidential Decision Directive 63 and have been used in "energy, financial services, and surface transportation to facilitate coordination between public and private entities" (GAO, 2017). Its purpose is to allow the IRS, states, and industry partners to quickly and efficiently share information about developments in IDT tax refund fraud through an online platform and the creation of a collaborative organization (GAO, 2017). When it was created, a total of 31 states, 14 tax preparation companies, and 3 financial institutions partnered with the IRS and the online

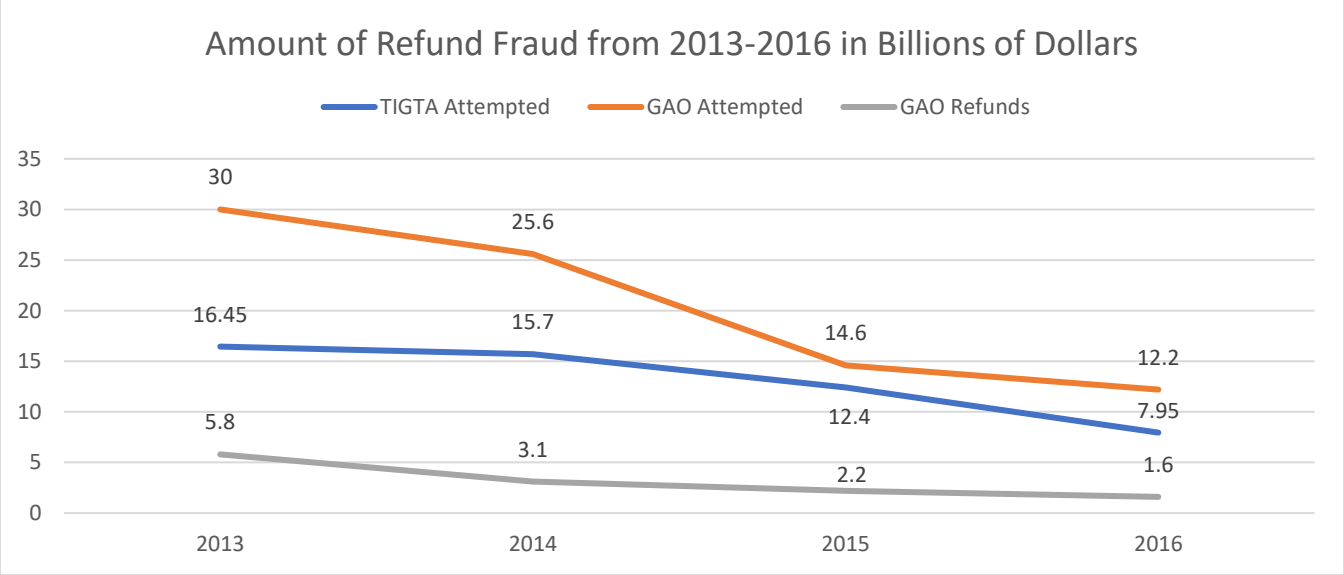
platform was launched on January 23rd, 2017. Since its inception, the partnership has grown drastically as currently around 60 private entities have engaged in ISAC and every state has joined to some extent (ISAC, 2018). Through the online portal, various entities may submit lead reports, more commonly referred to simply as "leads" of cyber threats for the IRS to analyze. In just the first year of its inception, the IRS received over 1.8 million leads, but there was some amount of trepidation from industry representatives who were unsure about the usefulness of their leads due to a lack of communication from the IRS. The necessary feedback on the leads is hampered by a lack of resources at the IRS and by IRS section 6103 which limits the IRS's ability to share taxpayer or record-level data due to confidentiality concerns, and the amount of information that can be shared with financial institutions is even further limited (GAO, 2017). This as well as further broadening the amount of users of the online portal may continue to facilitate the usefulness of ISAC and increase its efficacy in years to come (ISAC, 2018).

Lastly 2017 saw the deployment of the IRS's Rapid Response Team (RRT), which was created in 2016 to respond to events that created a significant amount of threat to IDT refund fraud within 24-72 hours. It would assess the situation and attempt to provide as much damage control as possible, and then around 2-3 days after the instance, it would provide action steps for future prevention and methods for alleviation of the threat. It was deployed in March 2017 in response to a threat created by the hacking of the IRS's Data Retrieval Tool which is a part of FAFSA.gov, a website for individuals to enter financial information to acquire need based financial aid from the government. It was estimated that around 100,000 individuals had their PII stolen in this manner and shows how fraudsters are employing increasingly clever techniques to steal even more detailed PII from potential victims. Thanks to the RRT's actions, the IRS was

able to prevent the issuance of over 8,000 fraudulent returns and has implemented new security measures associated with the Data Retrieval Tool (GAO, 2017).

Effectiveness of Actions

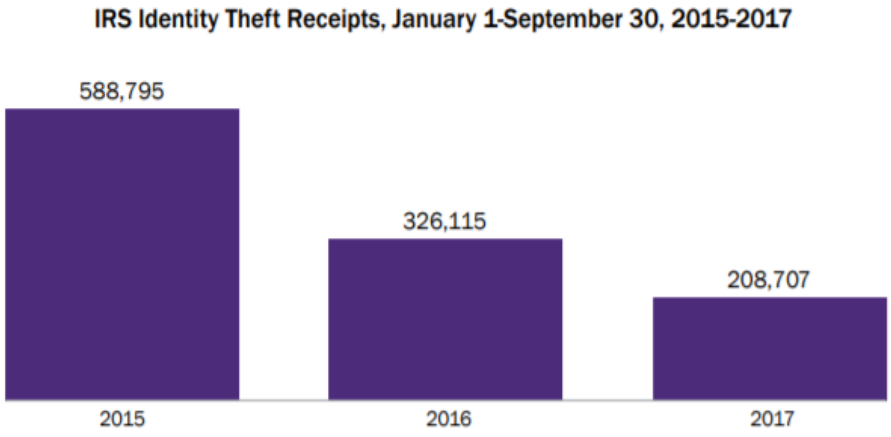
It is clear that the IRS has taken many steps to combat the issue, but the question of where or not these actions have had an impact on the amount of fraud and the rate at which the IRS is unable to identify it is an important metric. Unfortunately, this is a very difficult question to answer. This can be shown by the discrepancy between amounts of refund fraud reported by TIGTA and amounts of refund fraud reported by the GAO. This graph shows the reported amount of attempted refund fraud by the two organizations, as well as the amount of fraudulent refunds that were actually obtained by fraudsters according to the GAO. It is obviously apparent



that the GAO reports a much higher level of attempted fraud and thus also estimates a more significant amount of refunds issued to fraudsters. This is due to the fact that the GAO reports that the "IRS does not know the full extent of the occurrence of identity theft" (White, 2012). This is because if a fraudulent return passes by the IRS's preventative measures and is issued undetected, the IRS is unaware that this occurred if the legitimate taxpayer does not file a return

in that year. Even if they do manage to catch the fact that a fraudulent return has been issued, the IRS has had difficulty in the past aggregating this data to get an idea of the full extent of the issue (White, 2012). With this the GAO has also noted issues with the IRS's estimates. The Global Report, which the IRS uses to a high degree to analyze the amount of IDT tax refund fraud does not account for returns that pass underneath a certain threshold. Additionally, it has been shown to malfunction and count fraudulent returns that were caught as multiple instances as it counts each system that catches a fraudulent return, so if both the EFDS and the RRP catch a return, the Global Report double counts it. This leads to the GAO's recommendation of using return-level data to estimate the amount of fraud in both the Global Report and the *Taxonomy* as using primary data would provide Congress and other decision makers with more accurate information (2016). Overall it is heartening that the range between which the IRS is reporting the extent of fraud has decreased over the years, as shown by the convergence between the amounts reported by TIGTA and the GAO. This implies that the estimates that are being used are becoming more accurate as time goes on and the IRS has gotten a much better sense of the degree of the problem since first listing it on the Dirty Dozen in 2012.

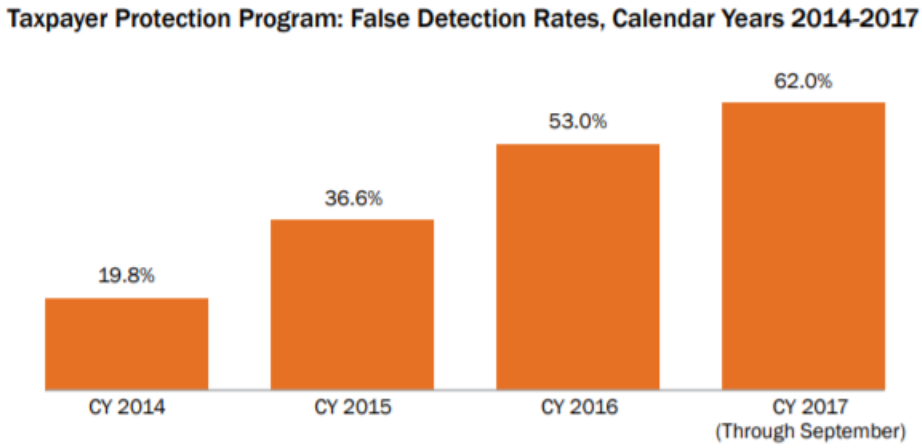
Even more encouraging is that it appears the amount of fraud perpetrated and the rate of successful fraud are on the decline. The NTA furthermore presents this from 2015-2017 based on the total number of cases of IDT tax refund fraud (2017). Despite the fact that the precise amount of fraud is incredibly difficult to estimate, as a whole the IRS has shown to be making strides



towards abating the problem. From 2015 there has been a 65% drop in instances of IDT tax refund fraud and from 2016 a 36% decline has been observed (NTA, 2017). While the IRS certainly has not eliminated the fraud in its entirety, its actions have been shown to be effective. It is practically impossible to point to a single tactic employed by the IRS to be most effective, but the NTA points to the improvement of the filters and systems the IRS uses, notably the implementation of the RRP, and the fact that the W-2 deadline was moved up as the primary drivers of the decrease in IDT tax refund fraud (NTA, 2017).

Has the IRS Gone too Far?

While the effectiveness of the IRS's actions are commendable, it has been asserted that the IRS has placed an undue, overreaching burden on the everyday taxpayer through their efforts. The GAO notes that the IRS is put in a difficult situation where they need to "prevent fraudsters from passing authentication using stolen taxpayer information, but it must balance that against the burden on legitimate taxpayers who must also authenticate" (GAO, 2018). A champion of this cause is the NTA who have been critical of the IRS for surpassing their bounds in their effort to prevent IDT tax refund fraud. Notably one way that the IRS has overburdened taxpayers was in the false detection rate (FDR) of the Taxpayer Protection Program's filters ("Objectives Report," 2018). This is the rate at which legitimate tax returns are flagged as fraudulent, therefore forcing the taxpayer to verify their identity with the IRS. As the graph shows, there has been a marked increase in the FDR of



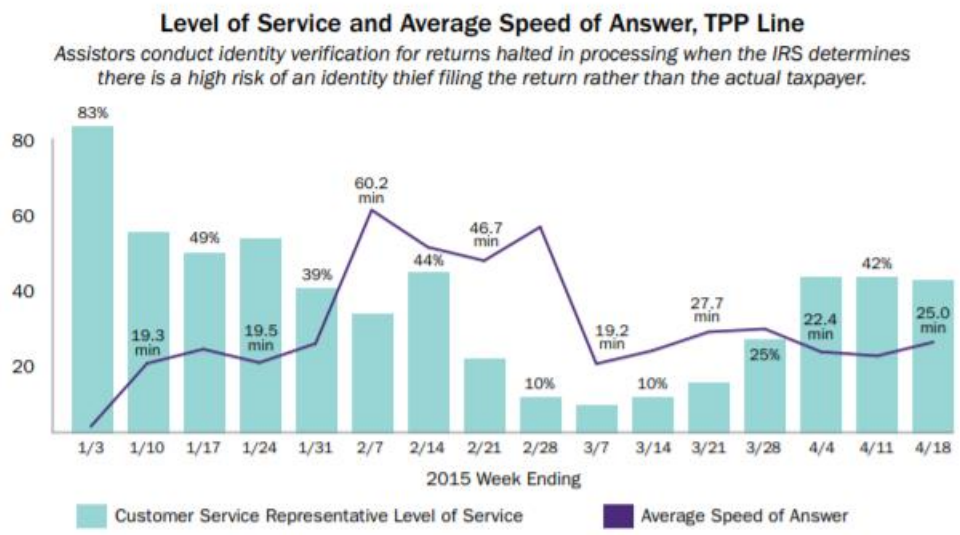
the filters over the years, even though the number of cases of IDT tax refund fraud has fallen over the years. In 2017, 1.9 million taxpayers were forced to verify their identities with 1.17 million completing the verification (GAO, 2018). In 2016 over $9 billion in legitimate refunds were delayed for an average of approximately 36 days (NTA, 2016). While this delay may not seem significant, it may impose significant hardship on low-income taxpayers who rely on their refunds. Low-income taxpayers often rely on their refund, of which the average was around $2,800 in 2016 to pay for various things such as heating bills, rent, groceries or for general quality of life and thus this delay can have a major impact in their lives (GAO, 2014; NTA, 2016).

One would expect the filters to have become more advanced and have a lower FDR over time as the number of filters has increased steadily over the years. TIGTA has reported that in 2014 only 114 filters were in place, but this number jumped to 196 in 2015 and has stayed around this level since then as 183 filters were in place in 2016, 197 in 2017 and most recently 200 in 2018. In the private sector, typically an FDR of 50% is considered acceptable, but is still obviously not optimal (NTA, 2018). The high FDR rate has both a monetary cost to the IRS as IRS employees must deal with the authentications of these legitimate taxpayers, but it also has the side effect of decreased employee morale. Studies have shown that when FPRs start to exceed 25:1, employees become more careless as they assume their actions will not actually uncover fraud, therein decreasing employee engagement (NTA, 2016).

The process by which the taxpayer must authenticate their identity has also been shown to be overly burdensome for the victim. High risk taxpayers must verify their identity at a Taxpayer Assistance Center (TAC), of which there are around 400, by providing a government issued ID (GAO, 2018). In some cases, the closest TAC may be hundreds of miles away, or the

closest one may not have available appointments for over a month, so if the taxpayer is of lower income and may not have steady access to transportation or be working multiple jobs, this is a daunting task that imposes substantial harm ("Objectives Report," 2017). Low risk taxpayers can verify their identity over the phone, and while this may not seem overly burdensome, in many instances it is. For the 2016 filing season, the TPP phone line received around 4.4 million calls, but it had a level of service (LOS), which is the percent of phone calls that are answered versus the taxpayer hanging up before a representative can see to them, of only 22.7% on average which was the worst performance for any high-volume line operated by the IRS ("Objectives Report," 2016). This graphic from the 2015 fiscal year sheds some light on why the LOS has fallen so low

FIGURE 1.16.3[18]



for this particular phone line (NTA, 2015). As shown by the week of February 7th, there were times taxpayers were forced to wait as long as an hour before they were processed through to an assistant, and this was when only around 35% of all calls were being sent to a representative. The IRS simply does not have sufficient resources devoted to the phone line for it to be an effective method of authentication and can be incredibly frustrating for a taxpayer to deal with. Victims are forced through this process of authentication at a time in their lives when they are under the

most stress as they must deal with their identity being stolen. In addition to having to deal with the issue of their identity being stolen and used for tax refund fraud, they most likely will also have to deal with it being misused for a variety of other types of fraud and it can be quite difficult for one to regain their identity in its entirety once it has been compromised. Psychiatrists have stated that the symptoms of identity theft victims are similar to those of people suffering from Post-Traumatic Stress Disorder, or PTSD, and thus it is cruel to put them through such a burdensome authentication process during such a vulnerable time (NTA, 2013).

Future Measures

With that in consideration, what can the IRS do moving forward to both combat IDT tax refund fraud while still adhering to taxpayer's needs? It certainly needs to improve its authentication services but opening more TACs or increasing its phone line staffing would both be costly options. The most cost-effective method of authentication for the IRS is currently its online methods, but these can only be used for very low risk cases where they must answer questions based on prior years tax returns, or for high-risk individuals who have set up multi-factor authentication with an IRS database. This can authenticate the taxpayer through methods such as sending a code to a mobile phone, thus ensuring the taxpayer possesses the phone, but if it has not been set up beforehand the taxpayer cannot use this method as a fraudster could simply set up the system with their own phone number, therefore making it worthless (GAO, 2018). If the IRS were to set up this sort of system with every taxpayer, then it could much more effectively, and more cheaply verify the identities of victims without making them jump through hoops and work through layers of red tape to do so.

The IRS could also work to improve their filters and systems to decrease the FDR and therefore the number of individuals who need to go through authentication. One possible way to

go about this would be to create a filter system that implements machine learning that relies on models instead of simple binary rules ("Objectives Report," 2018). It could also simply use predicative models to more accurately determine the number of filters necessary and adjust the filters more regularly, as in 2016 one filter had an FDR of around 91% and thus should have been discarded before the end of the filing season if they had kept up to date analytics with a fluid system (NTA, 2016). Overall, they should partner with "experts in the financial industry, including the Federal Financial Institutions Examination Council" who have experience and a proven track record creating such systems, and with the increased collaboration offered by ISAC, this seems like the perfect opportunity to do so (NTA, 2016). In a hearing before the House Committee on Oversight and Government Reform on April 17th, 2018 the IRS commissioner agreed to try to bring the FDR down to at least 50% ("Objectives Report," 2018). The exact methods to be employed are not known as of this date, or whether there are plans to attempt to further decrease the FDR subsequently, but it is certainly a step in the right direction.

The IRS could also seek to further prevent IDT tax refund fraud outright by expanding the IP PIN program into a national program. The number of PINs issued has steadily grown, going from around 250,000 in 2012 to roughly 3.5 million in 2017, but this has still only been for past victims of IDT refund fraud and residents of Florida, Georgia, and the District of Columbia who opt-in to it (Thorne & Stryker, 2014; GAO, 2018). By requiring every taxpayer to file with an IP PIN, the IRS could see impressive results as an estimated $193 of revenue was protected for every taxpayer who received an IP PIN in 2014. This is with a cost of issuing IP PINs being only around $36 for a three-year period, so therefore every dollar spent on the program has a return of something in the range of $5.36 (NTA, 2015). The question for where this funding would come from may already be answered. Currently if a company such as Equifax is to blame

for a massive data-breach, it will offer victims credit monitoring services, so the IRS could therefore attempt to put this financial burden off to the private sector to some extent, especially as the rate of large-scale data breaches is growing. The only issue with this program is that the IP PIN would therefore become another piece of PII that fraudsters could steal, although it would at least make the fraud more difficult. This has actually already occurred as in March of 2016 hackers were able to obtain over 100,000 IP PINs by exploiting the IP PIN retrieval tool, and thus this system is not without its faults (GAO, 2017).

The most effective, but also most controversial tactic of combating IDT tax refund fraud would be to delay the tax filing season or refund issuances. This would allow the IRS to fully match return data with the W-2s and give taxpayers more time to respond if their identity had been stolen. Unfortunately, as was aforementioned this would likely have a disastrous impact on low income taxpayers who rely on their tax refunds to survive. In total it would have a negative impact on a significant number of taxpayers as about 70% of taxpayers are issued a refund every year, thus making it a very undesirable motion to put forward in Congress. In the 2016 IRS Nationwide Tax Forum, various CPAs were polled about the legitimacy of pushing back the refund date, and consistently participants warned against it as it would be "difficult" to change taxpayer's expectations about when they would receive their refund (NTA, 2016). It is incredibly unlikely that the IRS would undertake this course of action due to how wildly unpopular it would be, but if the problem reversed its course, it may become necessary at a future date.

Individual Prevention

With all this in mind, it would be expected that one would wonder what they can do to ensure that they are not victims of IDT tax refund fraud themselves. There are numerous ways that one can go about this, all with varying levels of effectiveness.

The most obvious tactic that one can employ is to send in their tax return early in the filing season. If an individual files their return before fraudsters have the opportunity to, then they can eliminate the chance that they are victims of the fraud (Chambers & Zeidan, 2013). This is by far the most effective method, but also given the human nature to procrastinate, may be one of the most difficult for some people.

Another very important lesson for one to take away is to protect one's PII, which can take many forms. It is crucially important to understand how phishing attempts work and how one can avoid them. It can take many forms from a call saying someone won a sweepstakes, to an email that seemingly looks like it is from the IRS demanding action to avoid a fine, to even more advanced methods of emails that are "spoofed" to look like they come from an employee at a place of work. In general, it is good to just be aware that fraudsters are taking such efforts to steal your PII, but one can also view www.IRS.gov/identitytheft where the IRS regularly posts about new forms of phishing and what to be on the lookout for (Fisk & Stigile, 2012).

It is also important to protect physical forms of PII. It is important to secure physical copies of documents containing PII in one's home in a locked cabinet or safe, to never carry around such documents if it can be avoided, and to shred documents with such information when they are no longer needed as some fraudsters will go dumpster diving looking for such forms (Chambers & Zeidan, 2013). One should also protect their mail by avoiding using unsecured mailboxes and by putting a hold on their mail if going on vacation/a work trip and will be unable to pick up their mail (Fisk & Stigile, 2012). It is important to protect one's information when going online as well. This can be accomplished by keeping anti-virus software up to date, setting up a firewall on home networks, and in general by making sure websites that one goes on are secure by checking for a lock next to the URL or an https:// (Brody, Haynes, & Mejia, 2014). To

protect one's electronic information, make sure before being thrown away or sold, computers or phones are wiped of all data to make sure it does not end up in the wrong hands. It is also important to use strong, unique passwords as a rule of thumb. Moreover, one should regularly look at their credit report and bank statements to check for suspicious activity and ensure that they are not already a victim of identity theft (Fisk & Stigile, 2012). Finally, external parties can also be employed to protect/monitor one's identity such as Lifelock and IdentityForce (Kluwer, 2015).

If one is still concerned that they may fall prey to IDT tax refund fraud, they may employ additional measures to give themselves a sense of security. Often when one has their taxes done by an external party such as a CPA or a firm such as H&R Block, this other entity will deal with going through the authentication process should one's identity be stolen. Some may charge an additional fee if this is the case or have an "insurance" that can be purchased separately, and while this will not prevent the fraud from occurring, it will make it so that the taxpayer does not have to deal with the fallout from it themselves. One can also file IRS form 8821. This makes it so that if a return is filed in the taxpayer's name, they will receive a notification about it. Again, this is not a prevention method, but if one contacts the IRS before they issue a refund to the phony return, one can vastly accelerate receiving their own refund while simultaneously preventing a fraudulent one (Thorne & Stryker, 2014).

Conclusion

IDT tax refund fraud is so appealing to potential fraudsters due to the relative "safety" they have with the anonymity and the relatively low amount of PII needed to commit it. While the IRS has contributed significant resources to the issue since 2012, this was practically at the peak of the problem as they did not heed the warnings of other groups and address the problem

prematurely. Generally with their actions the IRS has still been far behind what external groups are recommending as they will often implement what has been recommended several years after the recommendation has been made, such as assigning a single representative to handle each case of refund fraud, as recommended by the NTA. IDT tax refund fraud will be a constant threat and area to watch moving forwards as fraudsters will not simply let the IRS "win" and will instead constantly become more advanced and evolve their techniques to circumvent the IRS's filters. The full extent of the problem is not even known, and while it seems that the IRS has been successful in abating it, this may be due to underestimates to ensure they appear effective in their Congressional reports. It is also concerning how far the IRS has gone in some areas as they have made the processes overly burdensome on taxpayers, but thankfully it does seem like actions are being taken in the right direction to alleviate this load. The problem of IDT tax refund fraud will not simply go away overnight and the IRS will likely be dealing with it in one form or another for decades to come, and should thus be closely monitored and it should be ensured that the IRS is held accountable for their efforts.

References

2005 Annual Report to Congress (Rep.). (2005, December 31). Retrieved April 30, 2019, from NTA website: https://www.irs.gov/pub/tas/section_1.pdf

2007 Annual Report to Congress (Rep.). (2007, December 31). Retrieved April 30, 2019, from NTA website: https://www.irs.gov/pub/tas/arc_2007_vol_1_cover_msps.pdf

2008 Annual Report to Congress (Rep.). (2008, December 31). Retrieved April 30, 2019, from NTA website: 2https://www.irs.gov/pub/tas/08_tas_arc_intro_toc_msp.pdf

2009 Annual Report to Congress (Rep.). (2008, December 31). Retrieved May 1, 2019, from NTA website: https://www.irs.gov/pub/tas/1_09_tas_arc_vol_1_preface_toc_msp.pdf

2011 Annual Report to Congress (Rep.). (2011, December 31). Retrieved May 1, 2019, from NTA website: https://www.irs.gov/pub/tas/irs_tas_arc_2011_vol_1.pdf

2012 Annual Report to Congress (Rep.). (2012, December 31). Retrieved May 1, 2019, from NTA website: http://www.taxpayeradvocate.irs.gov/2012-Annual-Report/downloads/Most-Serious-Problems-Identity-Theft.pdf

2013 Annual Report to Congress (Rep.). (2013, December 31). Retrieved May 1, 2019, from NTA website: http://www.taxpayeradvocate.irs.gov/2013-Annual-Report/downloads/Identity-Theft-The-IRS-Should-Adopt-a-New-Approach-to-Identity-Theft.pdf

2014 Annual Report to Congress (Rep.). (2014, December 31). Retrieved May 2, 2019, from NTA website: https://taxpayeradvocate.irs.gov/Media/Default/Documents/2014-Annual-Report/Volume-One.pdf

2015 Annual Report to Congress (Rep.). (2015, December 31). Retrieved May 6, 2019, from NTA website: Objectives Report to Congress Fiscal Year 2017 (Rep.). (2016, June 30).

Retrieved May 6, 2019, from NTA website: https://taxpayeradvocate.irs.gov/Media/Default/Documents/2017-JRC/Volume_1.pdf

2015 Security Summit Protecting Taxpayers from Identity Theft Tax Refund Fraud (Rep.). (2015). Retrieved May 2, 2019, from IRS website: https://www.irs.gov/pub/newsroom/2015 Security Summit Report.pdf

2016 Annual Report to Congress (Rep.). (2016, December 31). Retrieved May 2, 2019, from NTA website: https://taxpayeradvocate.irs.gov/Media/Default/Documents/2016-ARC/ARC16_Volume1.pdf

2017 Annual Report to Congress (Rep.). (2017, December 31). Retrieved May 7, 2019, from NTA website: https://taxpayeradvocate.irs.gov/Media/Default/Documents/2017-ARC/ARC17_Volume1_MSP_19_IDTheft.pdf

Additional Actions Could Help IRS Combat the Large, Evolving Threat of Refund Fraud (Rep.). (2014, August). Retrieved May 1, 2019, from GAO website: https://www.gao.gov/assets/670/665368.pdf

As Tax-Related Identity Theft Schemes Evolve, the IRS Must Continually Assess and Modify Its Victim Assistance Procedures (Rep.). (2017, December 31). Retrieved May 6, 2019, from NTA website: https://taxpayeradvocate.irs.gov/Media/Default/Documents/2017-ARC/ARC17_Volume1_MSP_19_IDTheft.pdf

Asbury, &. McKonly (2011, May 4). The Dirty Dozen Tax Scams of 2011. Retrieved from https://www.macpas.com/the-dirty-dozen-tax-scams-of-2011/

Brody, R. G., Haynes, C. M., & Mejia, H. (2014). Income Tax Return Scams and Identity Theft. *Accounting and Finance Research,3*(1). doi:10.5430/afr.v3n1p90

Chambers, V., & Zeidan, R. (2013). Stopping Tax Identity Theft: Practical Advice for CPAs and Clients. *Journal of Accountancy,* 60-64.

Despite Major Progress, Identity Theft Still on IRS 'Dirty Dozen' Tax Scams List [Press release]. IRS, Security Summit. (2018, March 7). Retrieved May 2, 2019, from https://www.irs.gov/newsroom/despite-major-progress-identity-theft-still-on-irs-dirty-dozen-tax-scams-list

Enhanced Authentication Could Combat Refund Fraud, but IRS Lacks an Estimate of Costs, Benefits and Risks (Rep.). (2015, January). Retrieved May 2, 2019, from GAO website: https://www.gao.gov/assets/670/667965.pdf

Fisk, S. M., & Stigile, C. (2012). Will the Real John Doe Please Stand Up?: Tax Identity Theft Developments. *Journal of Tax Practice & Procedure*, 21-71.

GAO. 1992. Tax administration: IRS can improve controls over Electronic Filing Fraud (GAO/GGD-93-27). Washington, DC: GAO.

Gudmundson, E. (2012, February 16). IRS Releases the Dirty Dozen Tax Scams for 2012. Retrieved April 24, 2019, from https://www.treasury.gov/connect/blog/Pages/IRS-Releases-the-Dirty-Dozen-Tax-Scams-for-2012.aspx

Hammel, S. W., & Murolo, S. B. (2016). IP PINs: Fraud protection places duties on preparers. *Tax Practice Corner,* 64-65.

Holtfreter, R., McLeod, T., & Harrington, A. (2014, March/April). Identity theft tax refund fraud. Retrieved from https://www.fraud-magazine.com/article.aspx?id=4294982014

Improved Collaboration Could Increase Success of IRS Initiatives to Prevent Refund Fraud (Rep.). (2017, November). Retrieved May 6, 2019, from GAO website: https://www.gao.gov/assets/690/688612.pdf

Interim Results of the 2010 Filing Season (Rep.). (2010, March 31). Retrieved May 1, 2019, from TIGTA website: https://www.treasury.gov/tigta/auditreports/2010reports/201041047fr.pdf

IRS. (2019, March 20). *IRS concludes "Dirty Dozen" list of tax scams for 2019: Agency encourages taxpayers to remain vigilant year-round* [Press release]. Retrieved April 25, 2019, from https://www.irs.gov/newsroom/irs-concludes-dirty-dozen-list-of-tax-scams-for-2019-agency-encourages-taxpayers-to-remain-vigilant-year-round

IRS Needs to Strengthen Taxpayer Authentication Efforts (Rep. No. 18-418). (2018, June). Retrieved April 25, 2019, from GAO website: https://www.gao.gov/assets/700/692712.pdf

IRS Needs to Update Its Risk Assessment for the Taxpayer Protection Program (Rep.). (2016, May). Retrieved May 1, 2019, from GAO website: https://www.gao.gov/assets/680/677406.pdf

IRS, States and Tax Industry Combat Identity Theft and Refund Fraud on Many Fronts. (2016, January 1). Retrieved April 30, 2019, from https://www.irs.gov/newsroom/irs-states-and-tax-industry-combat-identity-theft-and-refund-fraud-on-many-fronts

ISAC Annual Report (Rep.). (2018, April). Retrieved May 6, 2019, from ISAC website: https://www.irs.gov/pub/newsroom/IDTTRF ISAC April 2018 Annual Report.pdf

IRS, Security Summit. (2018, February 8). *Key IRS Identity Theft Indicators Continue Dramatic Decline in 2017; Security Summit Marks 2017 Progress Against Identity Theft* [Press release]. Retrieved April 25, 2019, from https://www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-theft

Kluwer, W. (2015). Tax Briefing: Identity Theft Update; As Identity Theft Grows, IRS and Practitioners React. *Journal of Tax Practice & Procedure,* 29-32.

Marcus, D. J. (2018). The Data Breach Dilemma: Proactive Solutions for Protecting Consumers' Personal Information. Duke Law Journal, 68 (555), 556-593.

Murolo, S. B. (2016). Security Summit touts improvements in its first year. *Journal of Accountancy,*78-78.

Nigrini, M. J., & Peters, J. S. (2018). Identity Theft Tax Refund Fraud: An Analysis of the Fraud Schemes Using IRS Investigation Summaries. *Journal of Forensic & Investigative Accounting, 10*(1), 38-55.

Objectives Report to Congress Fiscal Year 2017 (Rep.). (2016, June 30). Retrieved May 6, 2019, from NTA website: https://taxpayeradvocate.irs.gov/Media/Default/Documents/2017-JRC/Volume_1.pdf

Objectives Report to Congress Fiscal Year 2018 (Rep.). (2017, June 28). Retrieved May 2, 2019, from NTA website: https://taxpayeradvocate.irs.gov/Media/Default/Documents/2018-JRC/JRC18_Volume1.pdf

Objectives Report to Congress Fiscal Year 2019 (Rep.). (2018, July 27). Retrieved May 6, 2019, from NTA website: https://taxpayeradvocate.irs.gov/Media/Default/Documents/2019-JRC/JRC19_Volume1_AOF_04.pdf

U.S. Senate, Committee on Finance. (2007, April 12). *Filing Your Taxes: An Ounce of Prevention Is Worth a Pound of Cure* (M. R. Phillips, Author) [S. Rept.]. Retrieved April 30, 2019, from https://www.treasury.gov/tigta/congress/congress_04122007.htm

Results of the 2015 Filing Season (Rep.). (2015, August 31). Retrieved May 2, 2019, from TIGTA website: https://www.treasury.gov/tigta/auditreports/2015reports/201540080fr.pdf

The IRS Has Failed to Provide Effective and Timely Assistance to Victims of Identity Theft (Rep.). (2012). Retrieved April 30, 2019, from NTA website: http://www.taxpayeradvocate.irs.gov/2012-Annual-Report/downloads/Most-Serious-Problems-Identity-Theft.pdf

The Taxpayer Protection Program Includes Processes and Procedures That Are Generally Effective in Reducing Taxpayer Burden (Rep.). (2018, October 17). Retrieved May 1, 2019, from TIGTA website: https://www.treasury.gov/tigta/auditreports/2019reports/201940004fr.pdf

There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft (Rep. No. 2012-42-080). (2012). Retrieved April 25, 2019, from https://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.html

Thorne, B. M., & Stryker, J. P. (2014). The "Dirty Dozen" Tax Scams Plus 1. *Academy of Business Disciplines Journal*, 1-22.

Weisman, S. (2017, March 28). Beware of evolving income tax scams. Retrieved April 24, 2019, from https://www.usatoday.com/story/money/columnist/2017/03/28/beware-evolving-income-tax-scams/99408936/

White, J. R. (2011, June 2). *Status of IRS Initiatives to Help Victimized Taxpayers* (Rep. No. 11-721T). Retrieved April 30, 2019, from GAO website: https://www.gao.gov/assets/130/126344.pdf

White, J. R. (2012, November 29). *Total Extent of Refund Fraud Using Stolen Identities is Unknown* (Rep.). Retrieved May 1, 2019, from GAO website: https://www.gao.gov/assets/660/650365.pdf