Resolving Identity Theft Issues

Diana Leyden
Keith Fogg
Craig D. Bell

Repository Citation
Leyden, Diana; Fogg, Keith; and Bell, Craig D., "Resolving Identity Theft Issues" (2017). William & Mary Annual Tax Conference. 764. https://scholarship.law.wm.edu/tax/764
### Table of Contents

- **Introduction** ......................................................................................................................... 1
- **Tax Related Identity Theft** .................................................................................................. 4
- **IRS Structure for Addressing Identity Theft** ..................................................................... 6
  - Identity Protection Specialized Unit ....................................................................................... 6
  - Accounts Management ............................................................................................................. 7
  - Criminal Investigation ............................................................................................................ 8
  - Return Integrity and Correspondence Services ....................................................................... 9
- **Identity Theft Supporting Documentation** ........................................................................... 10
- **Identity Protection Personal Identification Number** ........................................................... 12
- **Obtaining Taxpayer Information to Resolve Identity Theft Cases** .................................. 12
- **Refund Suits** ....................................................................................................................... 16
- **Tax Court** ............................................................................................................................ 16
- **Practical Tips** ...................................................................................................................... 17
- **Conclusion** ........................................................................................................................... 19
For the past decade, identity theft has been the leading form of consumer complaint to the Federal Trade Commission and a leading source of problems for the IRS. The term "identity theft" encompasses a wide range of activities where an individual’s or a business’ identifying information is misused for the benefit of the thief. Based on the most recent FEDERAL TRADE COMMISSION, CONSUMER SENTINEL NETWORK DATA BOOK, published in March of 2017, employment and tax-related fraud were the most common form of identity theft, accounting for 34% of all reported cases. In 2016, tax-related identity theft comprised approximately 20% of the Taxpayer Advocate Service’s case receipts.

The National Taxpayer Advocate first tagged identity theft as a most serious problem in her 2004 annual report to Congress. The financial consequences of tax-related identity theft may include frozen or delayed refunds, loss of tax benefits, assessment of additional taxes, imposition of liens and levies to collect the incorrectly assessed taxes, and issues with non-tax benefits tied to income (such as housing or food stamps) due to attribution of additional income. Persons facing identity theft will experience a long path to clearing their identity and will face significant obstacles in gaining information about the theft. A Treasury Inspector General for Tax Administration (“TIGTA”) analysis of tax returns filed during the 2014 filing season revealed that the Service potentially paid out around $1.6 billion in fraudulent refunds attributable to undetected identity theft. The initial attempts by the IRS to address identity theft were clumsy.
and uncoordinated; however, the news is not all bad. In recent years, the IRS has made significant strides to address this issue and to combat this type of fraud.

A May 2012 report released by TIGTA reported that the IRS provided ineffective and untimely assistance to victims of identity theft.\(^4\) A follow-up audit, completed in 2015, revealed case resolution time still averaged 278 days.\(^5\) A January 2017 report released by the Government Accountability Office ("GAO") determined that the IRS had reduced the time an identity theft case was open, to an average of 106 days in 2016.\(^6\) A June 2017 report released by TIGTA found case closure time frames for identity theft refund cases had decreased to an average of 166 days.\(^7\)

The following chart illustrates the scope of the problem from 2010 through 2013.

**Identity Theft Incidents and Taxpayers Affected During CY 2010 Through CY 2013\(^8\)**

<table>
<thead>
<tr>
<th>Calendar Year</th>
<th>IRS-Identified Incidents</th>
<th>Taxpayer-Initiated Incidents</th>
<th>Total Incidents</th>
<th>Taxpayers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>338,753</td>
<td>101,828</td>
<td>440,581</td>
<td>270,518</td>
</tr>
<tr>
<td>2011</td>
<td>1,014,884</td>
<td>110,750</td>
<td>1,125,634</td>
<td>641,052</td>
</tr>
<tr>
<td>2012</td>
<td>1,508,375</td>
<td>277,491</td>
<td>1,785,866</td>
<td>1,219,208</td>
</tr>
<tr>
<td>2013</td>
<td>2,542,488</td>
<td>376,996</td>
<td>2,919,484</td>
<td>2,416,773</td>
</tr>
</tbody>
</table>

The volume of identity-theft incidents in IRS inventory peaked in calendar year 2013.\(^9\) It has dropped in each of the subsequent years. In 2016, the IRS statistics through September showed that it “stopped 787,000 confirmed identity theft returns, totaling more than $4 billion”, compared to 1.2 million returns worth approximately $7.2 billion for the same time period in 2015.\(^10\)

---

4 See TIGTA, 2012-40-050, MOST TAXPAYERS WHOSE IDENTITIES HAVE BEEN STOLEN TO COMMIT REFUND FRAUD DO NOT RECEIVE QUALITY CUSTOMER SERVICE 5, 8, 12-13 (May 3, 2012).

5 TIGTA, 2015-40-024, VICTIMS OF IDENTITY THEFT CONTINUE TO EXPERIENCE DELAYS AND ERRORS IN RECEIVING REFUNDS 5 (Mar. 20, 2015).


8 TIGTA, 2015-40-024, supra note 5, at 2.

9 Id. at 3.

10 IRS, SECURITY SUMMIT PARTNERS EXPAND IDENTITY THEFT SAFEGUARDS FOR 2017 FILING SEASON, BUILD ON
What has IRS done to combat identity-theft?

1) Increased criminal prosecutions
2) Improved detection models
3) Partnered with private and state actors to obtain better information
4) Obtained legislation pushing back time for payment of refund in EITC returns, moving up the due dates for payers’ submission of W-2, W-3, and 1099-MISC forms to January 31st (effective in 2017) and providing access prisoner database.
5) Promulgated regulations permitting the use of Truncated Taxpayer Identification Numbers (TTINs), where not prohibited by the Code, applicable regulations, or other official IRS guidance.

In 2015, the IRS hosted the first security summit in an effort to bring together a broad coalition of players involved in defeating identity theft. While the IRS has made significant progress, the problem remains a serious problem and identity thieves have not given up. The recent Equifax data breach exposing significant information about almost all American adults raises concerns for identity-theft efforts in the future. To the extent that the IRS has made significant strides to resolve the issues caused by identity-theft over the past several years, it has done so by devoting resources to this issue at a time of significant strain on its overall resources due to dwindling budgets. It is difficult to measure the true cost of identity-theft because it has diverted


12 Protecting Americans from Tax Hikes Act of 2015 (“PATH Act”), Pub. L. No. 114-113, Division Q, § 201(b)

13 Id. at § 201.


15 Reg. § 301.6109-4(b).


significant IRS resources from examination and collection to prevention and unwinding of the problems caused by the fraudulent activity.

**Tax Related Identity Theft**

Three main types of theft exist:

1) *Employment related* – this type of identity theft occurs when individuals need identification in order to obtain employment. Usually, the individuals engaging in employment related theft seek to do so because they are undocumented. Using the social security number of someone else allows these individuals to work as employees. (While an undocumented person can file a tax return with an ITIN, the ITIN does not permit the person to work as an employee.) This type of theft does not generally seek to harm the true owner of the social security number ("SSN") but has the collateral effect of doing so. When the employer sends to the IRS the Form W-2 or Form 1099 information regarding the identity thief employee, the information ends up on the account of the true owner of the SSN and gets picked up by the IRS when it runs the Automated Underreporter (AUR) program. The true owner of the SSN then receives correspondence from the IRS asking about the failure to report the income and begins a lengthy journey with the IRS to resolve the correct reporting of this income.

This type of theft also has consequences for the thief if the thief later seeks to become documented and enter the path to citizenship or permanent residence. In order to obtain legal status in the United States, the thief needs to show compliance with the tax laws. This can result in an arduous effort to unwind the use of stolen identification in order to properly report the income.

The issue has consequences beyond the IRS. Almost always this activity implicates Social Security records of earnings and other agencies as well. The victim, if a recipient of government benefits, can have those government benefits removed because of the reports issued to the IRS and the SSA showing additional income. The victim must go through a similar effort with the agencies providing the benefits to unwind the improper reporting of this income similar to the effort it must expend with the IRS.

Victims who are low income are particularly vulnerable because they do not have resources and skills to address the problems raised by the additional income appearing on their records. Commonly, these individuals will fail to respond to the IRS or other agencies in a timely manner when notices are issued and as a result end up with a tax assessment which results in an offset of refunds, a notice of federal tax lien and other collection action or lose benefits critical to their well-being.\(^\text{18}\)

---

2) **Refund related** – this type of identity-theft seeks to use the victim’s identity in order for the thief to obtain a refund to which they are not entitled. This is the type of theft that breaches like the one at Equifax make much easier, though the data obtained in that breach could also be used for employment related identity-theft. Here the thief will use the taxpayer’s identity to file a tax return claiming deductions or credits that result in a refund and steal money from the government. This type of theft frequently seeks to obtain refundable credits because those types of refunds do not require withholding credits on account with the IRS.

The thief typically files early in the filing season in order to be the first return filed with that SSN. Later, when the true taxpayer files, the IRS will reject the return of the true taxpayer because it already has on file the return of the thief. The true taxpayer will take months unwinding the fraudulent transaction in order to get the IRS to accept the correct return. This will significantly delay the receipt of any refund by the true taxpayer as well as cause the true taxpayer, and the IRS, much effort to fix the problem.

In the case of low income taxpayers, the return filed by the thief may be the only return filed because the true taxpayer does not have a filing requirement. In these circumstances, the detection of the fraud becomes more difficult for the IRS and for the victim. The victim may not know of the fraud until contacted by a third party notifying the true taxpayer of the loss of benefits as a result of the additional income. In the case of an elderly taxpayer who may reside in a nursing home, the unwinding of the theft may fall upon family members seeking to assist the relative but unequipped to easily do so. While the primary problem created by refund-related identity theft is a direct loss of funds by the government to the thief, the collateral consequences to the true owner of the identity can mirror the problems created for the victim of employment-related identity theft.

3) **Business related** – this type of identity theft occurs when someone creates, uses or attempts to use a business’s identifying information without authorization to obtain tax benefits. This type of theft involves both active and closed business. The thief generally seeks to use the business identity in order to receive refundable business credits or to perpetuate individual identity theft. Victims are often unaware that their identities

---

19 I.R.M. 25.23.1.4.1. In order to e-file a fraudulent tax return and receive a refund based upon falsified income and withholding information, the thief only needs a victim’s name, SSN (or other tax identification number), and date of birth.

20 The decision of the IRS to suspend its program of preparing substitute for returns for taxpayers who do not file may cause a delay in the true taxpayer learning about the theft of their identification. See http://procedurallytaxing.com/automated-substitute-for-return-asfr-program-suspended/ and http://procedurallytaxing.com/follow-up-to-yesterdays-post-on-suspension-of-asfr-program/

21 I.R.M. 25.23.4.1.

22 I.R.M 25.23.9.1.

23 This type of theft does not typically involve undocumented workers because they can operate a business with an ITIN. So, the typical person engaging in business Identity theft does so specifically for the purpose of stealing from
have been compromised until they receive a notice or bill from the Service. Business-related identity theft tends to be more complex and cross-functional in nature than individual identity theft. As with the theft of an individual’s identity, this theft can create significant adverse consequences for the targeted business. The business could suffer damage to its reputation, direct financial loss, high cost of professional representation to rectify the situation and lost business opportunity for the time and effort needed to resolve the problem.24

As the IRS has improved its performance regarding refund identity theft, more thieves have turned to business related identity theft in order to stay ahead of the curve.

**IRS Structure for Addressing Identity Theft**

When the problem first attracted widespread attention ten years ago, the IRS created the Privacy, Information Protection, and Data Security Office, which, it renamed the Privacy, Government Liaison, and Disclosure (“PGLD”) Office in 2011.25 The IRS created this office to oversee the use of Personally Identifiable Information (“PII”) and to find ways to maintain the security of this information.26 Inside of PGLD, the IRS established the Office of Incident Management27 and the Office of Privacy Policy and Knowledge Management.28

In 2015, in an effort to provide consistent treatment to victims of tax-related identity theft,29 the Service created the Identity Theft Victim Assistance (“ITVA”) Headquarters, a new headquarters operation affiliated with the Identity Protection Strategy and Oversight Program (“IPSO”).30 IPSO seeks to help taxpayers by providing victim assistance, outreach, and prevention of future identity theft. The IPSO Program has fifteen distinct responsibilities, including: responsibility for developing, defining, monitoring, and executing identity theft policies and procedures; reducing taxpayer burden and improving service options while addressing and resolving identity theft cases; and protecting revenue through increased vigilance at the point of return submission.31 IPSO now formulates the guidelines that the IRS uses to handle identity theft cases.

---


25 TIGTA, 2012-40-050, supra note 4, at 3.

26 See I.R.M. 10.5.1.2(3).

27 I.R.M. 10.5.1.7.12.

28 I.R.M. 10.5.1.7.1.


30 I.R.M. 25.23.1.3(4).

31 I.R.M. 25.23.1.3.1(2).
The IRS has created a Technical Working Group to identify ways to assist victims, an Identity Theft Advisory Council ("IDTAC") through which it shares ideas on how to attack the problem of identity theft with other interested parties and an Identity Theft Executive Steering Committee ("IDTESC") to provide oversight. Because of the scrutiny of this issue by Congress and the need for coordination with numerous other agencies, the IRS devotes much energy to this problem.

Identity Protection Specialized Unit

The Identity Protection Specialized Unit ("IPSU") was established in 2008 in Wage & Investment, Accounts Management, to provide individualized assistance to taxpayers who are, or may become, victims of identity theft.\(^{32}\) IPSU was generally seen as a failure in its early years and has never lived up to the purpose for which it was originally intended which was to provide individualized assistance to victims by assigning a specific IRS employee to assist that person in resolving the problem. In 2015, IPSU was consolidated into the Identity Theft Victim Assistance ("IDTVA") Directorate.\(^{33}\) IPSU quickly evolved into a place that did not resolve problems but rather monitors identity theft cases worked by other IRS functions. Practitioners generally found IPSU difficult to work with. The IRS thought that having a central point of contact for a taxpayer trying to work through an identity theft problem would be the most helpful and it might have been if that point of contact had the authority to and did actually work to fix the problem. In its role as a coordinator, IPSU never fulfilled the initial vision.

Taxpayers may report identity theft affecting their tax accounts directly to IPSU by calling the identity theft hotline at (800) 908-4490. This number will connect taxpayers directly to an IPSU customer service representative who can provide general information and answer basic questions. Taxpayers may also self-report identity theft to IPSU before it has impacted their tax accounts.\(^{34}\) IPSU will then serve as an intake, referral, and liaison unit for other Service functions that ultimately work the case and make account adjustments.\(^{35}\)

Accounts Management

The vast majority of identity theft cases get worked by the Accounts Management function. Six specialized groups within Accounts Management work identity theft cases.\(^{36}\) Starting in 2013 the IRS tried to get a jump start on fixing the problem created by refund identity theft. It created Form 14039 Identity Theft Affidavit ("ITA"). This form seeks to treat signal to the IRS that it should treat the return filed by the true taxpayer as the real return and not as a duplicate filing as previously done. If the taxpayer attaches this affidavit to the return, Accounts Management should mark the

---

\(^{32}\) TIGTA, 2016-40-003, IMPROVEMENTS ARE NEEDED IN THE IDENTITY PROTECTION SPECIALIZED UNIT TO BETTER ASSIST VICTIMS OF IDENTITY THEFT 1, 8-11 (Oct. 27, 2015).

\(^{33}\) I.R.M. 25.23.1.3(5).

\(^{34}\) Id. at 1.

\(^{35}\) See id.; see also I.R.M. 8.6.5.1.1(10).

\(^{36}\) Id.
return with a specialized code and send it to one of the specialized groups within Accounts Management for immediate processing.\(^{37}\) Adopting this procedure has significantly reduced the time it takes to fix the problem for the true taxpayer.\(^{38}\)

**Criminal Investigation**

The IRS created the Identity Theft Clearinghouse ("ITC") in 2012 within CI.\(^{39}\) As of March 2016, the Clearinghouse had received over 10,750 identity theft leads since its inception.\(^{40}\) The IRS increased the number of offenses it authorized special agents to investigate in relation to identity theft. The matters that special agents can now investigate in connection with identity theft include: forging endorsements on Treasury checks, theft of public money, fraud in connection with access devices, mail fraud, and wire fraud. CI joined with the Department of Justice Tax Division to make these investigations a much higher priority and issued DOJ-Tax Directive 144, which delegates authority to the United States Attorney's Offices to authorize tax-related grand jury investigations, to file federal criminal complaints, and to apply for seizure warrants.\(^{41}\) If an investigation covered by this directive goes forward, the U.S. Attorney must notify CI if it proceeds with a grand jury investigation so that the prosecution may take advantage of access to tax returns and return information under section 6103(h). Because of the limited resources in CI, making identity theft a high priority on its investigation list has led to a number of high profile criminal investigations in the past few years in this area where previously almost none existed.

CI has developed the Identity Theft Victim Disclosure Waiver Process in an effort to aid state and local law enforcement agencies pursuing identity theft investigations.\(^{42}\) Generally, section 6103 forbids the disclosure of tax returns and return information to third parties including state and local law enforcement. The Waiver Process allows victims of identity theft to authorize the release of tax information to the designated state or local law enforcement official conducting the investigation. Disclosure issues pervade the area of identity theft and this is just one example of how the IRS and victims might work around the disclosure issues presented by identity theft. This workaround does expose information about the victims and that can be a concern. More discussion

\(^{37}\) See id. at 6.

\(^{38}\) TIGTA, 2015-40-024, supra note 5.

\(^{39}\) Examining the Skyrocketing Problem of Identity Theft Related Tax Fraud at the IRS: Hearing before the Subcomm. on Gov't Operations of the H. Comm. on Oversight and Gov't Reform, 113th Cong. 15-17 (Aug. 2, 2013) (Written Testimony of Daniel Welfel, Principal Deputy Commissioner, IRS).


\(^{41}\) DOJ-Tax, Dir. No. 144, Temporary Delegation of Authority to Authorize Grand Jury Investigations, Criminal Complaints, and Seizure Warrants for Certain Offenses Arising from Stolen Identity Refund Fraud, ¶¶ 2, 4.

\(^{42}\) Examining the Skyrocketing Problem of Identity Theft Related Tax Fraud at the IRS: Hearing before the Subcomm. on Gov't Operations of the H. Comm. on Oversight and Gov't Reform, 113th Cong. 17 (Aug. 2, 2013) (Written Testimony of Daniel Welfel, Principal Deputy Commissioner, IRS).
of disclosure issues will be addressed infra. One area where the IRS could improve is in the pursuit of prisoners who seek refunds through identity theft. If it could leverage the resource of the parole boards with respect to these crimes, it could gain enforcement muscle without having to expend significant CI resources.43

Over the past three fiscal years, CI has helped convict over 2,100 identity thieves.44 In fiscal year 2016 alone, IRS Criminal Investigation enforcement efforts resulted in 613 prosecutions in which the thief was sentenced for a crime related to identity theft.45 Of course, the devotion of this much CI resources to this problem comes at the expense of the prosecution of other tax crimes. Some people see the use of CI resources to pursue identity theft as a use that is not completely consistent with its mission; however, devoting this much effort to pursuing this crime can have a very positive impact on stopping the activity. Because some of the identity theft occurs offshore, it can present significant difficulties in reaching the perpetrators and bringing them to justice.

Return Integrity and Correspondence Services

Within the IRS, the Return Integrity and Correspondence Services (“RICS”) function, which falls under the Wage & Investment (“W&I”) Division, seeks to identify and stop refund-related identity theft before it occurs.46 If this function works correctly, it protects both individual taxpayers and the system as a whole. This function is critical to the overall integrity of the tax refund system. Each year, tens of thousands of attempts are made to breach the IRS system and find weaknesses to exploit that would result in significant refunds going to thieves. Within RICS, the Integrity and Verification Operations (“IVO”)47 function supports the Service’s pre-refund fraud detection and prevention efforts.48 The IVO strives to protect revenue by identifying potentially fraudulent tax returns, verifying the accuracy of reported income and withholding information, and stopping the refund of returns that do not meet specified criteria.49 If a tax return gets identified as meeting identity theft criteria, it is then routed to the IVO function’s Taxpayer Protection Program

43 See discussion in article cited in footnote 14, supra note 14.


45 Id.


47 IVO was formerly known as the Taxpayer Assurance Program under Accounts Management (AMTAP). In 2013, the Service moved AMTAP out of the Accounts Management function to RICS and renamed it as well. I.R.M. 25.23.2.21.2(1) (Oct. 13, 2016).

48 TIGTA, 2016-40-006, IMPROVEMENTS ARE NEEDED TO BETTER ENSURE THAT REFUNDS CLAIMED ON POTENTIALLY FRAUDULENT TAX RETURNS ARE NOT ERRONEOUSLY RELEASED 1 (Nov. 12, 2015).

49 Id. at 2.
This part of the effort against identity theft does not rely on reporting by an individual victim but identification in the system of returns that should not be processed. The IRS is constantly seeking to refine its filters to catch the bad returns at the outset. For example, it will no longer send 500 refunds to the same address as it did several years ago. If the same address is used for refunds on more than a specified number of returns, the IRS filters will kick in and prevent the issuance of the refunds until further investigation can occur.

Identity Theft Supporting Documentation

For persons who find themselves the subject of identity theft or who suspect that they might be the subject of identity theft, the IRS has a process for them to use to alert the IRS. If the IRS did not catch the identity theft with its filters, it will begin to take action toward the true taxpayer that alerts the true taxpayer that something is amiss. The true taxpayer may first discover that her personal information has been compromised upon receipt of a CP2000 notice for a prior filing year. The notice will typically come as quite a surprise because it will contain income or other information of which the true taxpayer has no knowledge. The true taxpayer will wonder why the IRS has contacted them and sent incorrect information. By denying that she ever earned the income or lived in the state in which that income was earned, the true taxpayer begins the process of alerting the IRS. Because the IRS encounters some of the same claims in situations in which there has not been identity theft, it must carefully listen to the taxpayer and will require the taxpayer to provide documentation in support of their story. At this point, the true taxpayer in an identity theft case will feel particularly put upon because they must, in effect, prove a negative.

Alternatively, a taxpayer may have her electronically filed return rejected by the Service, as an identity thief has already filed a return using that taxpayer’s TIN. Upon notification by the taxpayer, the Service will flag the taxpayer’s account with an identity theft indicator. If the Service employee cannot properly determine the ownership of the SSN used on the potentially fraudulent return, then the employee may request that the taxpayer provide identity theft supporting documentation to verify that the taxpayer is the true holder of the TIN. A driver’s license, state I.D. card, passport, or Social Security card are acceptable as proof of identity. In addition to these documents, the IRS requires that the taxpayer file some evidence of identity theft: either a police report or the IRS Form 14039 IRS Identity Theft Affidavit. The Service requires that the taxpayer provide this documentation once per incident. The taxpayer provides this

50 TIGTA, 2016-40-008, CONTINUED REFINEMENT OF THE RETURN REVIEW PROGRAM IDENTITY THEFT DETECTION MODELS IS NEEDED TO INCREASE DETECTION 2 (Dec. 11, 2015).

51 The indicator is TC 971 AC 522 PNDCLM. I.R.M. 25.23.2.16(1).

52 I.R.M. 25.23.2.17(3).

53 I.R.M. 25.23.2.17(1)(1).

54 I.R.M. 25.23.2.17(1)(2).
information only one time when there may be multiple years in question, but all of which are investigated as a result of one incident.\(^{55}\)

The information provided by the true taxpayer is valid for three years after the date that the Service receives the information from the taxpayer.\(^{56}\) The IRS default position is that a once it has sent the taxpayer a proposed adjustment, the true taxpayer’s failure to submit the documentation requested by the IRS indicates that the true taxpayer is not an identity theft victim.\(^{57}\) While the position of the IRS concerning response to its notices is logical and necessary, the taxpayer finds themselves in a situation that demands immediate and significant attention. Not all taxpayers are equipped to adequately assist the IRS (and themselves) in fixing the problem. This puts a burden on the system and the taxpayer.

Assuming that the taxpayer can timely submit the requested documents completely and legibly, the IRS will usually notify the taxpayer that it has classified the matter as one of identity theft and that it is working toward resolution of the problem. It will also notify the taxpayer that resolution may take six months.\(^{58}\) Once the IRS has reached the initial conclusion that identity theft occurred, it should update the taxpayer’s account, if necessary, to accurately reflect the type of identity theft suspected.\(^{59}\) When the IRS employee handling the case verifies that the person who provided the supporting documentation is a victim of identity theft and confirms that she is the owner of the SSN at issue, the employee should update the address associated with the true taxpayer and make sure that notices are not sent to the address of the perpetrator.\(^{60}\)

When the IRS determines that identity theft occurs and adjusts the true taxpayer’s account to reflect their correctly filed return or to remove income from the fraudulent return, it should notify the taxpayer. It generally includes in that correspondence the name of an employee at IPSU to contact if there are questions or continuing concerns. In a recent case at the Harvard clinic, I called this number on behalf of a client in order to verify that the account had been properly adjusted. The IPSU employee told me that she would not provide me with a copy of the client’s account transcript and that I would need to obtain that transcript through ordinary channels. I pointed out to her that once the identity theft indicator is placed onto an account it cannot be obtained through e-Services

\(^{55}\) I.R.M. 25.23.2.17(11).

\(^{56}\) I.R.M. 25.23.2.17(10).

\(^{57}\) I.R.M. 25.23.2.17(3).

\(^{58}\) I.R.M. 25.23.2.10.

\(^{59}\) Currently, there are five different Tax Administration Source Codes that the Service may apply: INCOME, MULTFL, INCMUL, NOFR, and OTHER. I.R.M. 25.23.2.17.3(3). The Service uses INCOME when income has been reported under the taxpayer’s SSN without his consent or knowledge. \(\text{Id.}\) It uses MULTFL when two or more returns are filed for the same tax period under the same SSN. \(\text{Id.}\) If a combination of both income and improper returns are at issue, then the Service uses the INCMUL code. \(\text{Id.}\) If the issue arises out of an account for a taxpayer who normally does not have a filing requirement, then the Service codes the incident as NOFR. \(\text{Id.}\) Finally, if the matter does not fit into any of the tax administration codes, then the Service uses the OTHER code. \(\text{Id.}\) These codes are useful to the Service as they direct further investigation and research into the identity theft matter.

\(^{60}\) I.R.M. 25.23.2.8.
or through calling the Practitioner Priority Hotline. Nonetheless, the IPSU employee declined to provide an account transcript showing the correction of the account. With a few months the client received another notice from the IRS which made clear that the IRS had not cleared up the account. In order to resolve the issue, it became necessary to involve the Local Taxpayer Advocate. This is an example of the burden that identity theft places on the system and the taxpayer, as well as the failure of some of the IRS procedures to fully address the problem of identity theft.

**Identity Protection Personal Identification Number**

In an effort to prevent any further harm to victims of identity theft, the IRS can issue an Identity Protection Personal Identification Number (IP PIN) after the case is fully resolved. IP PINs started as a pilot program in 2011. In 2014, the Service expanded the use of IP PINs to select taxpayers, not all of whom were victims of identity theft. The IP PIN is primarily used to prevent electronic filing fraud, but may also be used on a paper return. IP PINs offer an additional level of security for the taxpayer who has been or fears becoming a victim of identity theft. If the IRS issues an IP PIN to a taxpayer, any tax return filed with the taxpayer's TIN without the IP PIN will not post to the taxpayer's account. For the taxpayers' safety, the IRS issues new IP PINs each year in December for use in the coming filing season. In the event an IP PIN is lost or misplaced, the taxpayer can request a new one from the IRS but must go through proper authentication processes to ensure that the taxpayer is authorized to receive the IP PIN. Because of rampant identity theft fraud in certain parts of the country, the program was expanded in recent years to allow opt-in by taxpayers who reside in Georgia, Florida, or the District of Columbia. Prior to the 2015 filing season, the Service sent notices to select groups of taxpayers identified as at risk for possible identity theft, informing them that they may elect to receive an IP PIN for their own protection. Due to the recent information breach at Equifax, advocates have requested that the IRS consider making IP PINs available nationwide, but the IRS has rejected this proposal to date.

**Obtaining Taxpayer Information to Resolve Identity Theft Cases**

The disclosure laws generally protect a taxpayer's information and prevent identity theft; however,
when a taxpayer is the known victim of identity theft the IRS procedures can make it very difficult for the taxpayer to access their own information. In part, the issue stems from the IRS desire to provide extra protection for an account in which a thief possesses the kind of information that might, in ordinary circumstances, allow the thief access to the taxpayer’s information at the IRS by having the ability to answer identifying questions. In part, the issue stems from the IRS duty to protect the fraudulent return of the thief which is not the return of the taxpayer. Threading the needle to provide taxpayer’s necessary information while preventing further identity theft provides quite a challenge to the IRS.

In confirmed or suspected cases of identity theft, the IRS marks a taxpayer’s account with various types of identity theft indicators. When these markers exist, the practitioner will generally find it difficult to obtain any “return” or “return information” from the Service reported under a client’s SSN because IRS employees are trained to be more cognizant in these cases about the potential for unauthorized disclosures of taxpayer information protected by section 6103. One approach that practitioners sometimes take when they have a client who they suspect is the victim of identity theft is to obtain all of the information on their client’s account before disclosing to the IRS that the client is a victim of identity theft. Before the markers are on the account, the practitioner will usually experience little difficulty in accessing the information through the normal channels.

On April 4, 2014, the IRS re-announced through its weekly e-News for tax professionals (April 4th Notice) that it would no longer process or release requests for taxpayer transcripts through TDS when a taxpayer’s account contained an identity theft indicator. Presently, when a taxpayer’s authorized representative attempts to pull a transcript through the TDS system on behalf of a victim (or Service suspected victim) of identity theft, the practitioner will receive a notice, which states, “We apologize for the inconvenience but we are not able to process your request at this time. Please have your client contact the Identity Protection Specialized Unit (IPSU) at 800-908-4490.” The taxpayer then receives a paper copy in the mail of the same notice for every year and transcript type the representative attempted to get off TDS. The notice also instructs tax professionals with a POA on file that they may contact IPSU to obtain client transcripts.

As discussed above, a large part of the reluctance regarding whether to release taxpayer

67 See I.R.M. 8.6.5.2(8); I.R.M. 25.23.2.15.
68 See, e.g., I.R.M. 21.2.3.5.8.
70 Letter from Patricia LaPosta, Director, Electronic Products & Services Support, IRS, to Taxpayer (name redacted) (Apr. 20, 2014) (on file with author, Rachael Rubenstein).
72 In practice, phone assistants who answer the toll-free IPSU line, as well as the practitioner priority service (PPS) line, seem unsure whether they are permitted to release various transcripts and other confidential information when the account contains any type of identity theft indicator. It is not uncommon for these calls to end with the practitioner unable to receive any requested information.
information associated with identity theft turns on the issue of whose “return” or “return information” is it: the taxpayer’s or the return of the identity thief? While the IRS appears to recognize the need for identity theft victims and their representatives to have access to information in the taxpayer’s account in order to properly address the issue, the Office of Chief Counsel has issued several, not always consistent, opinions concerning the legal interpretation of section 6103 disclosure issues related to identity theft.

Since first addressing the issue in a 2008 PMTA document, the Service’s position has evolved to better assist victims but would really benefit from a statutory fix. Presently, the Service takes the position that once the invalid return is submitted, it becomes the return information of both the true owner of the SSN and the identity thief because the information relates to the potential investigation of liability with respect to both parties. Under this analysis, a victim of identity theft, and her designated representative, generally has a right to a copy of the bad tax return as long as disclosure would not impair federal tax administration. If a criminal investigation, for example, is underway with respect to the fraudulent return, the true taxpayer could find themselves in a waiting game to get the information because the IRS does not want to release the information and possibly impair the investigation.

The authority for the most recent opinion of Chief Counsel’s Office that allows greater dissemination to the true taxpayer of the fraudulent return is found in section 6103(e)(7), which allows for disclosure of return information to persons authorized to have access to the return of a taxpayer as long as disclosure would not “seriously impair federal tax administration.” The new rationale is that while the identity thief’s return submission contains “return information,” it is not a valid “return” as contemplated by section 6103(b)(1) because it is “not filed by the true taxpayer or with the taxpayer’s consent.” Because the true owner of the SSN did not sign the filed tax return, the return lacks a valid signature, as required by the Beard test. The bad return also cannot

---


75 PMTA 2012-005, supra note 70, at 3-4; PMTA 2015-019, supra note 71, at 6-7 (where the identity thief files a fraudulent return in the name of an otherwise legitimate business, the return information created and gathered as part of that fraudulent filing is the return information of the business victim; however, where the identity thief uses an individual victim’s identity information to obtain an EIN and/or file fraudulent tax returns for a fictitious business (other than a sole proprietorship), the information would not be the return information of the individual victim because the individual does not have liability under the Code).

76 PMTA 2012-005, supra note 70, at 5-6.

77 Id. at 5; I.R.C. § 6103(e)(7). The most recent Chief Counsel memorandum entitled “Identity Theft – Disclosure Issues under I.R.C. 6103” is dated July 8, 2016 and was released on August 25, 2017. It is labeled DISSP-138861-15 and is copied in its entirety at the end of this outline.

78 PMTA 2012-005, supra note 70, at 3; PMTA 2015-019, supra note 71, at 4-5.

79 Id.; Under Beard v. Commissioner, the test to determine whether a document constitutes a valid return filing contains
be considered a valid return under the *Beard* test because it does not represent “an honest and reasonable attempt to comply with federal tax laws.” Even though the bad return is treated as a nullity from the standpoint of its validity as a return, it does contain return information as defined by section 6103(b)(2) because it includes “information received, acquired, or generated by the Service in connection with the determination of a taxpayer’s liability.” Some of the opinions written about how or whether to allow the true taxpayer to see everything in their own account seem maddeningly complex because the Chief Counsel lawyers are struggling to deal with a statute that was not designed to address identity theft and because the consequences to an IRS employee of wrongful disclosure are severe. No one wants to see the case in which an identity thief successfully sues the IRS for a disclosure violation related to the turning over of information from the fraudulent return.

In 2015, the IRS set out procedures allowing identity theft victims have access to important tax account information, including copies of fraudulent tax returns. Through these procedures, identity theft victims can obtain a redacted copy of a fraudulent return that was filed and accepted by the Service using the identity theft victim’s name and TIN. In order to comply with federal privacy laws, the Service requires that the victim’s name and TIN be listed as either the primary or the secondary taxpayer on the fraudulent return. If, for example, the fraudulent return lists the victim as a dependent, the Service will not release the fraudulent return information to her because she would not meet the test under the privacy laws as the IRS currently interprets them. The IRS will only do this if the case involves a Form 1040 Series tax return. Currently, it will not release business tax returns under this process.

In order to request the return, the taxpayer or her representative must complete Form 4506-F, *Request for Copy of Fraudulent Return*. The form must be mailed to the following address:

IRS
Fresno, CA 93888-0025

four elements: “First, there must be sufficient data to calculate tax liability; second, the document must purport to be a return; third, there must be an honest and reasonable attempt to satisfy the requirements of the tax law; and fourth, the taxpayer must execute the return under penalties of perjury.” *Beard v. Commissioner*, 82 T.C. 766, 777 (1984).

PMTA 2012-005, *supra* note 70, at 3 (citing *Beard*, 82 T.C. at 777).

Id. (citing *Payne v. United States*, 289 F.3d 377, 382 (5th Cir. 2002)); see also PMTA 2015-019, *supra* note 71, at 6.


Instructions for Requesting Copy of Fraudulent Returns, *supra* note 79.

Id.

Id. Prior to October 1, 2016, the IRS had asked taxpayers send a letter providing similar information to Form 4506-F, however the lack of a standardized form led to processing errors. See TIGTA, 2017-40-011, *supra* note 79, at 6.

Returns being sent via private delivery service should instead be mailed to: IRS, 5045 East Butler Avenue, Fresno,
Refund Suits

When the taxpayer has been the victim of refund related identity theft, the IRS is not making adequate progress towards resolution and the return of the taxpayer seeks a refund, the taxpayer can turn to the “normal” refund litigation process to seek an expedited review of the request for refund. If six months have passed since the taxpayer filed the return seeking a refund which is being held up while the IRS seeks to resolve the identity theft issue, the taxpayer can file suit. Before embarking on this route, the practitioner should make sure the client does not have other compliance issues with the Service or identity theft problems affecting other tax years, especially years in which a refund suit is not an appropriate remedy. Further, the case must involve a tax year (or years) where the victim has experienced true identity theft refund fraud, as opposed to a case where the taxpayer victim had her tax refund(s) offset due to collection issues resulting from prior year identity theft issues. If the taxpayer is low income, both courts offer petitioners the option of filing suit without paying the normal filing fee. At least one low income taxpayer clinic has had success in bringing refund suits as a method for forcing earlier resolution of refund identity theft and getting the refund to the client.

Tax Court

Victims of identity theft can most easily end up in Tax Court because they will receive a notice of deficiency based on their failure to report income earned by employment related identity theft or the claim of a deduction or credit in the case of business related identity theft. The thief may have used the taxpayer’s address or the IRS has reviewed their records and found the victim’s address. In that case, the IRS will send a notice of deficiency to the victim. If the IRS does not send a notice of deficiency to the victim’s last known address, the victim may whether challenge the notice of deficiency is valid.

If the taxpayer receives the notice of deficiency either because it is sent to his or her last known address or he or she somehow gets a copy, before filing with the Tax Court, the victim may utilize Rev. Proc. 98-54 to ask the IRS to rescind the notice of deficiency and work to correct the account. Once the taxpayer files a petition with the Tax Court, however, the IRS will not rescind the notice of deficiency.87

Once a petition is filed, the taxpayer should work with IRS counsel to try to resolve the case. The good news in a Tax Court case is that frequently taxpayers can use section 6201(d) to put the burden of proof on the IRS with respect to the income reported on the Form W-2 or Form 1099. This section came into the code in 1996 as a part of Taxpayer Bill of Rights 2 legislation and piggybacks on the 5th Circuit decision in Portillo v. Commissioner, 932 F.2d 1128 (1991), holding that a “naked” Form 1099 reporting income to a taxpayer was insufficient to cause the taxpayer to have a deficiency. Section 6201(d) placed the burden of proof on the IRS if a taxpayer contests the validity of an information return and cooperates with the IRS during the examination phase of


87 See Chief Counsel Memorandum CC;PA:06-MEAvruteine April 9, 2012.
the case. The IRS must go out to the sender of the Form 1099 and verify the correctness of the information. For someone who is the victim of identity theft, this will generally result in a successful resolution of the case for the true taxpayer.

Representatives should carefully review any proposed stipulations of settled issue or decision documents in settled Tax Court cases to see whether respondent may be trying to assert penalties that were not in the original notice of deficiency. To assert such penalties, such as late file or late pay, respondent is required to amend the answer to raise it and then has the burden of proof.

If the victim did not file an original tax return and can now do so representative should consider whether spouses should or can join in a newly filed original return. If the IRS allows a joint return to be filed, it will summarily assess the spouse who is not the victim.

Other issues can present themselves in Tax Court when a taxpayer is the victim of identity theft. Practitioners should be alert to clients raising issues of concern about information in their case and use informal or formal discovery of the IRS to gain access to information in the IRS files that might shed light on the issue.

**Practical Tips**

Certain issues come up with enough frequency that there are some actions a practitioner with a client facing an identity theft issue can use to make the process smoother. The discussion here does not follow a specific order but rather offers random pieces of advice that might not occur in the order discussed here.

1) If you suspect identity theft, get a POA, contact the IRS and obtain all of the taxpayer’s transcripts (wage and income, tax return and account transcripts) for as many periods as you think will be needed in order to resolve the issue before you file the identity theft form with the IRS. Once you make it known to the IRS that your client is or may be a victim of identity theft and the indicators go onto their account, your ability to obtain the transcripts, which may be critical to piecing together what has happened may be significantly limited.

2) Let your client know that fixing an identity theft case can take a long time. It is important to provide the client with a picture of the length of the process in order to avoid significant frustration.

3) If your client has filed a tax return seeking a refund and more than six months has passed with no action from the IRS on the refund and no action in sight, consider bringing a suit for refund as a means of moving the case. If the IRS allows a joint return to be filed, it will summarily assess the spouse who is not the victim.

4) Check the client’s credit reports to determine if the identity theft is limited to a tax problem.

---

88 Camara v. Commissioner, 149 T.C. No. 13 (September 28, 2017)


17
Put a fraud indicator on the credit report to prevent further use by the thief of the taxpayer’s identity.

5) Obtain an IP PIN number for filing with future tax returns. The IRS readily provides these numbers to individuals in certain states but not others. It will provide the IP PIN for someone who it recognizes as a victim of tax identity fraud.

6) Go to your Local Taxpayer Advocate’s office if you are having problems getting the IRS to assist you. Identity theft has been the biggest inventory issue for the Taxpayer Advocate Service for almost the past decade. The recent decline in cases has also resulted in a relatively dramatic decline in these cases in the TAS offices but because of their past experience these offices have a lot of expertise and are generally more accessible than the IPSU units which are remote and not as customer friendly.

7) Expect the unexpected. One victim of identity theft had a fraudulent refund return filed on his behalf which resulted in the refund being offset as part of the federal offset program and the refund paid his outstanding student loan debt. Then as the IRS began to unwind that transaction more problems ensued for the taxpayer, the IRS, and probably the Department of Education.

8) Be aware that the additional income that could appear because of employment theft can have an impact on a client’s benefits and be proactive about finding the possible points of impact before the taxpayer loses benefits.

9) Be alert to the possibility of identity theft when the client comes in complaining of IRS correspondence or collection action they cannot understand. Because many clients put their head in the sand regarding the IRS, it can be easy to become jaded about clients complaining about IRS correspondence. Sometimes these complaints have a legitimate basis due to the IRS pursuing the true taxpayer based on information in the system generated by a thief. An example can be an elder taxpayer who no longer has a filing requirement who suddenly finds the IRS seeking to collect based on income earned by a thief, followed by exam notices going to the thief’s address and then the Collection division of the IRS locating the true taxpayer and demanding payment.

10) Obtain multiple original copies of identity documents (perhaps 5-8), so the practitioner does not have to make copies of copied identity documents when later submitting multiple Identity Theft Affidavits (ITAs) to various Service functions. If the identity documents submitted along with the ITA are illegible the affidavit may not be accepted and, instead,

---

90 https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. The Internal Revenue Service (IRS) had previously made available Identity Theft PINs for consumers in Florida, Georgia, and the District of Columbia, and consumers in those states should consider getting the pin (which they should do before getting a freeze).


92 Ivy v. IRS, 197 F.Supp.3d 139 (D.D.C. 2016). An appeal was filed on August 24, 2016 to the D.C. Circuit.
11) Obtain proof of identity theft from the taxpayer. At a minimum, the practitioner will need documents sufficient to satisfy the Service’s substantiation requirements, a copy of a police report or a completed ITA, and a copy of a valid U.S. federal or state government issued form of identification. If the taxpayer possesses multiple types of identity documents, it’s preferable to obtain copies of whatever the taxpayer can produce. Examples of acceptable identity documents include: passport, driver’s license, and Social Security Card. A birth certificate may be helpful as a secondary form of identification, but it cannot be the only document used to establish identity.

12) Soon after the detailed interview with the taxpayer, the practitioner should memorialize a specific yet concise version of the client’s story in the narrative section of the ITA. The ITA should be completed with the taxpayer. Finally, several (perhaps 5-8) original copies of the ITA should be printed, reviewed, and signed. There is a good chance the practitioner may need to use this form to prove the client’s identity to several Service functions where the identity theft has negatively impacted the client’s tax accounts for various tax years.

13) If the true taxpayer has not already visited a police station to report the identity theft, the practitioner should exercise caution when recommending that the client make an in person police report due to the potential for outstanding arrest warrants as a result of the actions by the thief. At a minimum, the client should be advised about a possible arrest when visiting a police station if a warrant exists under her identity.

14) Consider checking the taxpayer’s earnings history from the SSA both to obtain an independent source of the taxpayer’s earnings and to check with SSA to make sure that nothing the thief has done will adversely impact the taxpayer’s SSA account.

Conclusion

The IRS has come a long way over the past decade to improve its system of dealing with victims of identity theft. The numbers of cases have declined significantly but still remain large in absolute terms. Clients will feel especially put upon in paying for representation in these cases because they are the victim. They will want quick resolution of a problem that will not usually go away quickly. Understanding the IRS systems for approaching identity theft, familiarizing yourself with the disclosure issues presented, and quickly pursuing the available avenues for resolution will keep your client from suffering more than necessary, but nothing will prevent them from significant pain once someone has stolen their identity and used it in a way that implicates the IRS.

93 I.R.M. 25.23.2.17. Under the I.R.M., only one copy of a valid U.S. federal or state government issued form of identification must be sent along with the IRS ITA. Id.
Office of Chief Counsel  
Internal Revenue Service  

Memorandum

Number: AM2017-004  
Release Date: 8/25/2017

CC: PA: ?: JEGerdyZogby DISSP-138861-15

UILC: 6103.00-00

date: July 08, 2016

to: Joanne B. Minsky  
Division Counsel (Wage & Investment)

from: Drita Tonuzi /s/  
Associate Chief Counsel (Procedure & Administration)

subject: Identity Theft - Disclosure Issues under I.R.C. § 6103

Several offices have requested assistance in determining which disclosures are appropriate in the identity theft context. This memorandum consolidates previous legal advice with regard to disclosure issues under section 6103 in cases involving identity theft.

Although this memorandum provides a broad overview of identity theft disclosure issues in the context of identity theft, it does not purport to discuss or provide formal legal guidance with respect to all potential identity theft factual scenarios that could exist. The discussion below represents scenarios that have previously been provided and analyzed, but identity theft scenarios are constantly evolving. The legal analysis involved in identity theft disclosure issues can vary significantly based on any number of factual details, such as where the victim’s information appears on a particular filing and the context in which a return was filed with the Service. Thus it is recommended that all novel identity theft disclosure issues be referred to P&A for legal review and advice.

The advice in this memorandum only applies to certain situations in which identity theft is an issue. Applying this advice in non-identity theft contexts

could result in an unauthorized disclosure and possible civil and criminal penalties under I.R.C. §§ 7431 and 7213.

ISSUES AND CONCLUSIONS

1. Is a return filed by an identity thief protected under section 6103?
   - Some identity theft "returns" are not returns for 6103 purposes.
   - Identity theft "returns" are "return information" protected under section 6103.

2. Whose return information is it?
   - A fraudulent refund return is the return information of both the victim and the thief from the moment it is filed with the Service.
   - If a victim is listed as a dependent on a fraudulent return, the return is not the return information of the victim.
   - For returns filed by an employer, the return information is generally the employer's, the employee's, and the victim's.
   - A return filed using a fraudulent EIN, which was obtained using a stolen SSN, is not the return information of the victim.

3. Who may receive the disclosure?
   - The Service may disclose a taxpayer's return information to the taxpayer, but an identity thief is not necessarily a taxpayer.
   - A taxpayer may consent to the disclosure of his or her own return information.
   - The Service is not authorized to disclose the identity thief's separate and distinct return information to an identity theft victim.
   - The Service is authorized to disclose return information to other employees of the Department of the Treasury.
   - The Service is authorized to disclose return information in a Federal or State judicial or administrative tax proceeding.
   - Legal guardians of minor victims may obtain copies of the minor victim's return information.
   - In some circumstances, the Service may disclose return information, but not "taxpayer return information," to other Federal agencies.
   - The Service may only disclose return information to state and local officials if they are considered Federal employees for section 6103 purposes.
   - The Service may disclose information to confirm a return's legitimacy.

4. To what extent may impairment of tax administration be considered in making a disclosure determination?
• Information from an identity theft return should not be disclosed if that information would seriously impair Federal tax administration.
• Victims may obtain copies of fraudulent returns.

DISCUSSION OF AUTHORITIES

I. BACKGROUND

In recent years identity theft and other refund fraud schemes have proliferated across the country. In response, the Department of Justice created an Identity Theft Task Force ("ITTF"), which is comprised of Federal agencies including the Service, the Postal Service, the Secret Service, and Immigration and Customs Enforcement, as well as state and local law enforcement.

Identity theft can take many forms, but there are some common scenarios that typically confront the Service. The first is refund fraud, in which the perpetrator who has stolen an identity files a tax “return” early in the filing season using a Form 1040, U.S. Individual Income Tax Return, in the name or with the taxpayer identification number ("TIN"), e.g., Social Security Number ("SSN") or Employer Identification Number ("EIN"), of the victim, who has not yet filed a return for the tax year. For example, the perpetrator will often attach to the Form 1040 one or more false Forms W-2 showing bogus wages and withholding credits that exceed the wages, thereby providing the basis for the purported refund. The Form will also instruct that the refund be directly deposited into a bank account under the perpetrator’s control. When the identity theft victim later files a legitimate return for the tax year, the Service will likely flag it because of the significant discrepancies with the prior filed return and, pending resolution, freeze any refund claimed on the second return. Eventually, through investigation, the identity theft and the fraud will become apparent. A variation of this scenario involves filing return forms in the name of a business to claim a fraudulent refund. In other situations, an identity thief uses another taxpayer’s information to claim that taxpayer as a dependent in order to create additional deductions.

In another common scenario, an undocumented worker, who does not have the legal status to work in the United States, uses the victim’s stolen SSN to appear workeligible. The undocumented worker provides the SSN to the worker’s employer, and the employer in turn files a Form W-2 reporting the worker’s wages and tax withholding under the SSN provided. The undocumented worker then files a return, along with Form W-2, that, between the two forms, reflect the identity theft victim’s SSN and name along with the actual wages and tax withheld of the undocumented worker. In processing the return, the Service may attribute the wages to the identity theft victim and determine additional tax due. Another variation on this scenario would involve the undocumented worker utilizing the victim’s SSN on the Form W-2, but would vary in that the return would contain the Individual Taxpayer Identification Number ("ITIN"), along with the actual wages and tax withheld, of the undocumented worker, and the only information of the
victim would be the SSN on the Form W-2 submitted with the return. In this variation, there are no tax consequences to the victim as the wages are not attributed to the victim, but, nonetheless, the victim's account is marked with an indicator of employment-related identity theft.

When the Service confronts identity theft and refund fraud, complex disclosure questions often arise. The determination of whether to release certain information depends on numerous factors, including what kind of return information is involved, whose return information it is, and who would receive the information in a disclosure.

II. LEGAL ANALYSIS

A. DISCLOSURES GENERALLY

Section 6103(a) provides that "returns" and "return information" are confidential and shall not be disclosed except as authorized in section 6103 or elsewhere in Title 26. Section 6103(b)(1) defines "return" to mean any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for that is filed with the Secretary, on behalf of, or with respect to any person, and any amendment and supplement thereto, including supporting schedules and attachments to the return. The term "return information" is broad and includes any information "received by, recorded by, prepared by, furnished to, or collected by" the Service with regard to a taxpayer's liability under the Code. See I.R.C. § 6103(b)(2)(A); McQueen v. United States, 264 F.Supp.2d 502, 516 (S.D. Tex. 2003), aff'd, 100 F. App'x 964 (5th Cir. 2004); LaRouche v. Dep't of Treasury, 112 F.Supp.2d 48, 54 (D.D.D. 2000); Hull v. IRS, 656 F.3d 1174, 1195-96 (10th Cir. 2011).

There is a subset of return information known as "taxpayer return information" that is subject to additional restrictions. Taxpayer return information is "return information . . . which is filed with, or furnished to," the Service "by or on behalf of the taxpayer to whom such return information relates." I.R.C. § 6103(b)(3). In other words, taxpayer return information is return information provided by the taxpayer himself. Taxpayer return information enjoys special protections and is particularly relevant when determining whether information may be disclosed to other Federal agencies for nontax crimes, as discussed later in this memorandum.

Taxpayers generally may access their own return information under section 6103(e). See Linsteadt v. IRS, 729 F.2d 998, 1000 (5th Cir. 1984). For example, an individual has a right to view his or her own return under section 6103(e)(1)(A)(i), and section 6103(e)(1)(C) generally\(^\text{95}\) allows any member of a partnership during the period covered by the return to receive disclosure of the

\(^{95}\) I.R.C. § 6103(e)(10) imposes significant limitations.
return information of that partnership. The Service must withhold return information if disclosing such information would “seriously impair Federal tax administration.” I.R.C. § 6103(e)(7).

Although taxpayers generally may access their own return information, access to the return information of others is strictly limited. The Service may disclose the return or return information for a particular taxpayer to anyone whom the taxpayer may designate. I.R.C. § 6103(c). In other words, a taxpayer may consent to the release of that taxpayer’s own return information to a third party.

The Service may disclose certain information under section 6103(k)(6) when the Service is attempting to gather information that is otherwise not reasonably available in connection with a tax investigation. Treas. Reg. § 301.6103(k)(6)-1(a)(1) allows a Service employee to disclose return information to the extent the disclosure is necessary to obtain information related to official duties. Additional exceptions may also allow for disclosure, e.g., disclosure to state tax officials, state and local law enforcement agencies, and disclosure to certain Federal officers and employees for purposes of tax administration. I.R.C. § 6103(d) and (h).

To determine to whom an item of return information “belongs,” a critical issue is the identity of the person or entity with respect to whose liability the information was generated or received by the Service. Martin v. IRS, 857 F.2d 722, 724 (10th Cir. 1988). The determining factor is whether the information relates to the Service’s investigation or determination of another taxpayer’s liability. Id. at 724. In certain circumstances, material can constitute the return information of more than one taxpayer. Solargistic Corp. v. United States, 921 F.2d 729, 731 (7th Cir. 1991). If a taxpayer requests access to a record with return information of more than one taxpayer, the Service must not release any return information that does not “belong” to that taxpayer unless an exception to section 6103 protection applies.

In the context of identity theft, various factors must be considered before determining whether returns and return information may be disclosed.

**B. IS A RETURN FILED BY AN IDENTITY THIEF PROTECTED UNDER SECTION 6103?**

To determine whether something filed with the Service by an identity thief is protected from disclosure, the Service must first determine if the record is covered under section 6103. Since most documents filed with the Service by

---

96 Additional information about disclosure to persons having material interest in the return information of different types of taxpayers may be found at section 6103(e).
identity thieves are on return forms, the Service must determine if the document filed by an identity thief is a return under section 6103.

1. Some identity theft “returns” are not returns for 6103 purposes.

If a Form 1040 or other return form is not a valid return, the document itself does not qualify for disclosure protections under section 6103. See “Identity Theft Returns and Disclosures Under Section 6103,” June 8, 2008, PMTA 2009-024, available at http://www.irs.gov/pub/lanoa/pmta2009-024.pdf; Zellerbach Paper Co. v. Helvering, 293 U.S. 172, 180 (1934). An invalid return is not “required by, or provided for or permitted under” the Code, as described in section 6103(b)(1), so if a document is not a valid return, it may not be afforded disclosure protection under section 6103.

Requirements for a valid return include that the return be filed as part of an honest and reasonable attempt to comply with the tax laws and that the return be signed by the purported taxpayer under the penalties of perjury. See Beard v. Commissioner, 82 T.C. 766, 777 (1984) (listing the requirements for a filing to be a valid tax return). A return form that is filed by an identity thief using a victim’s name and TIN and attempts to intercept the victim’s refund is generally not a valid return and therefore is not afforded protection under section 6103(b)(1).

The method through which the identity thief obtains stolen information likely will not make a difference in whether the document is a valid return. For example, if an identity thief steals the EIN of a company to file a fraudulent return and take the company’s refund, the return is invalid. If, instead, the identity thief steals an SSN and then applies for an EIN under that stolen name, the return form filed using that fake EIN is still invalid because it was not filed as part of an honest and reasonable attempt to comply with the tax laws and is not signed by the person in whose name the purported return is filed. The form of the fraud, at least in this case, does not matter for the determination of whether the return is valid.97

Note that this rule does not apply in the case of an undocumented worker who uses a stolen SSN, but otherwise reports actual wages. This would be a valid return because, under the circumstances, it represents a reasonable effort to comply with the tax laws.

To illustrate this rule, there is a legal difference between a Form 1040 filed by an identity thief and a Form W-2 filed by an employer using a stolen SSN. The employer is filing the W-2 in order to comply with employment tax responsibilities, and although there are penalties for filing information returns with missing or incorrect information under section 6721, this Form W-2 is not a sham return like a fictitious refund return. The form reflects a real employment relationship with associated wage payments and tax withholding and is filed as a good-faith

97 The form of the fraud does matter for determining whose return information the return is, as discussed below.
information return. Unlike a Form 1040 from an identity thief reporting a phony set of facts, the Form W-2 in this scenario is not a fiction, and though potentially subject to a penalty, the Form W-2 would still constitute a valid return. As a result it is a return as defined in section 6103 as well.

2. Identity theft "returns" are "return information" protected under section 6103.

Although the return of an identity thief seeking a fraudulent refund is a nullity, the return may be legally protected "return information" under the broad definition of return information in section 6103(b)(2)(A). The document is return information because it is "received by, recorded by, prepared by, furnished to, or collected by" the Service as part of a determination of liability, or potential liability under the Code. I.R.C. § 6103(b)(2)(A).

Assuming there is some potential liability to be determined under the Code, the document does qualify as return information, and it can only be disclosed as authorized by the Code. I.R.C. § 6103(a). By knowingly filing a false return, the identity thief subjects himself to possible other liabilities (e.g., under section 7207), and any information furnished to and received by the Service with respect to the "determination of the existence, or possible existence of liability of [the identity thief] for an offense under the Code" is return information. See, e.g., O'Connor v. IRS, 698 F. Supp. 204, 206 (D. Nev. 1988), aff'd without op., 935 F.2d 275 (9th Cir. 1991) (a threat against a Service employee is a violation of section 7212 and information collected with respect to that offense is return information). Thus, any information collected by the Service with regard to the identity thief's potential liability would be the return information of the identity thief.

C. WHOSE RETURN INFORMATION IS IT?

In the enactment of, and subsequent amendments to section 6103, Congress did not expressly provide for the situation in which one individual files a fraudulent return using the name or TIN of another taxpayer. As noted above, in determining to whom a particular item of return information belongs, the Service considers the identity of the person or entity with respect to whose liability the information was generated or received by the Service. Martin, supra at 724.

In certain circumstances, a particular item may be return information of more than one taxpayer. Solargistic, supra. Return information related to identity theft is often the return information of both the victim and the thief. To determine whether section 6103 allows for disclosure of returns or return information, the Service must determine the "owner" of the return or return information.

1. A fraudulent refund return is the return information of the victim and the thief from the moment it is filed with the Service.

When a fraudulent refund return is first filed with the Service, the Service will assume it is the return information of the victim, since the victim's identifying information is on the return. Information such as the date the return was filed, the
document locator number assigned to it, the liability and payment amounts reported on the return, and the steps taken to process the return (including any refund) will all be posted to the victim’s account for that taxable year. All this information was collected by the Service with respect to the possible tax liability of the victim, making that information the victim’s return information. Section 6103 does not incorporate any temporal limit on the designation or identification of returns and return information of being that of a particular taxpayer, so the return would remain the return information of the victim.98

At the same time, as discussed above, the identity thief, by knowingly filing a false return, subjects himself to other possible liabilities, so the return is the thief’s return information as well. See, e.g., O’Connor, supra. As a result, the return filed in an identity theft scenario is often the return information of both the victim and the thief. Even though the Service may not be aware that the return or return information belongs to the thief until the identity theft is discovered, it is still the return information of the identity thief from the moment it is filed with the Service.

2. **If a victim is listed as a dependent on a fraudulent return, the return is not the return information of the victim.**

In one variation of the identity theft scenarios, the identity thief claims the victim as a dependent for fraudulent refund purposes. Being claimed as a dependent could affect the determination of the victim’s liability, specifically with regard to what deductions the victim could take (e.g., I.R.C. § 63(c)(5) (limiting the standard deduction for dependents); I.R.C. § 151(b) (limiting the personal exemption for dependents). The document, however, would not be the return information of the victim listed as a dependent on the fraudulent return because being listed as a dependent on a tax return does not, in and of itself, subject the dependent to any liability under the Code.

It should be noted, however, that the Service could examine a victim’s return because the Service noticed that the victim was taking certain deductions. If the Service is determining the allowance or denial of deductions based on the conflicting information contained in the return filed by the identity thief, it is possible that the identity thief’s return information could become germane to the determination of the victim’s liability. In that case, the portion of the return that would be relevant to the victim’s liability could be disclosed under section 6103(h)(4), which allows disclosures related to judicial or tax administration proceedings. The Service should redact any information that the victim is not

---

98 Even if the Service were to confirm the “bad return” as fraudulent before it is processed and take no action with respect to the victim’s account, the submission of a purported return bearing the victim’s name and/or SSN, and the unsuccessful attempt to affect the victim’s tax account by means of a “bad return” in
entitled to or that might seriously harm tax administration, as discussed below, before disclosing that information to the victim.  

3. *For returns filed by an employer, the return information is generally the employer's, the employee's, and the victim's.*

The type of return may also be relevant to determining the “owner” of the return information. For example, when an employer files a Form W-2 with the Service, the information contained in that return is return information both of the employer and the employee. As a result, in the case of an undocumented worker using someone else's SSN, the return information belongs to the employee/undocumented worker, to the employer, and to the victim, based on the analysis above.

the victim's name or TIN would nevertheless constitute the victim's return information just as if it were processed.

6 See the discussion below, under “Other Considerations,” for information on how a victim can request a copy of a fraudulent return even if he or she is not involved in a judicial or tax administration proceeding.

4. *A return filed using a fraudulent EIN, which was obtained using a stolen SSN, is not the return information of the victim.*

If an identity thief steals an EIN and files a fraudulent return for a business, that return is the return information of both the identity thief and the business victim. If, however, the identity thief steals an SSN, applies for an EIN using that SSN, and then files a fraudulent return for the EIN, then the return is not the return information of the individual victim because the fraudulent return is not related to the liability of the individual. Simply being listed on the application for an EIN does not in and of itself create a tax liability. As a result, that information may only be disclosed to the victim if otherwise authorized under Title 26.

**D. WHO MAY RECEIVE THE DISCLOSURE?**

The Service must determine to whom any return information would be disclosed before releasing that information because the exceptions to section 6103 are often based on who is receiving the disclosure. For example, the Service may disclose to a taxpayer his or her own returns or return information, but the Service is limited in who else may receive disclosures.

1. *The Service may disclose a taxpayer's return information to the taxpayer, but an identity thief is not necessarily a taxpayer.*

Section 6103(e)(1)(A)(i) and (7) authorize the Service to release returns and return information of any taxpayer to the taxpayer himself. As a result, if information related to an identity theft return is the victim’s return information, the Service may disclose that information to the victim. Additionally, an
undocumented worker's return or return information may be disclosed to the worker.

There is an argument, however, that a refund fraud identity thief must demonstrate that he is a taxpayer before the Service can disclose return information to him as the taxpayer under section 6103(e)(7). Section 7701(a)(14) defines the term "taxpayer" as "any person subject to any internal revenue tax." An identity thief generally has not filed the fraudulent return because he is subject to some internal revenue tax. Unless the identity thief can demonstrate that he is subject to an internal revenue tax, the identity thief is not entitled to his return information.99

2. A taxpayer can consent to the disclosure of his own return information.

Although a taxpayer may generally have access to his own return information, access to another taxpayer's return information is limited. Section 6103(c) allows for a taxpayer to consent to the disclosure of returns or return information. A victim of identity theft may wish to have a copy of a fraudulent return sent to state or local authorities or another designee, and if the victim consents to the release of his return information, the Service may disclose that information to the victim's designee.100 Once again, the refund fraud identity thief must demonstrate that he is a taxpayer before he may take advantage of section 6103(c).

3. The Service is not authorized to disclose the identity thief's separate and distinct return information to an identity theft victim.

The Code provides no authority for disclosure of an identity thief's separate and distinct return information to an identity theft victim. The victim is not even entitled to disclosure of the identity thief's identity. Cf. Hodge v. IRS, 2003 WL 22327940 (D.D.C. 2003) (the name and address of a person who used plaintiff's social security number on her tax return was third party return information that could not be disclosed to the plaintiff). However, where the information is the return information of both the victim and the thief, the Service may legally disclose the information to the victim. The Service, however, may conclude as a matter of policy that disclosure of return information of the thief to the victim will impair tax administration and accordingly refuse to make such disclosures. See I.R.C. § 6103(e)(7).

99 Most identity thieves would not request return information, and the specific facts in any such scenario will be relevant in determining whether to release the return information to the identity thief.

100 See the discussion below, under "Impairment and Policy Considerations," for information on how a victim can request a copy of a fraudulent return.
It should be noted, however, that the Service now allows victims to obtain redacted versions of identity thieves' returns. The method for obtaining such a return is discussed below.

4. The Service is authorized to disclose return information to other employees of the Department of the Treasury.

Since more than one Service operating division may be working on either the victim's or the identity thief's case, employees may need to share return information in the performance of tax administration duties. See I.R.C. § 6103(h)(1). Internal sharing of documents does not, however, mean that the shared information becomes return information of another taxpayer. If information from one case is copied and placed in other case files, it should clearly be labeled as third-party return information.

5. The Service is authorized to disclose return information in a Federal or State judicial or administrative tax proceeding.

Section 6103(h)(4) allows the disclosure of a taxpayer's return information to a third party if the disclosure meets one of four tests. For example, in the case of a victim who was claimed as a dependent on a fraudulent refund return, the victim's own liability may be at issue in an examination. Section 6103(h)(4) would authorize disclosing the relevant portion of the fraudulent refund return in order to resolve the examination of the victim's liability. The fraudulent refund return is not the victim's return information, but the Service can disclose it to the victim.

6. Legal guardians of minor victims may obtain copies of the minor victim's return information.

Section 6103(e)(2) provides that if an individual is legally incompetent, the individual's return or return information may be disclosed to the "committee, trustee, or guardian of his estate." In this regard, a minor is legally incompetent and this provision allows parents to access the return or return information of a minor if, under state law, the parent is the legal guardian of the minor's estate. See IRM 11.3.2.4.10; IRS Publication 4639, Disclosure & Privacy Law Reference Guide at 2-14 (rev. 10-2012). As a result, the parent may only request the minor's return information if that parent is the legal guardian under state law. Once it is clear that a parent may request the return information of the minor, the Service must then analyze what portions, if any, of the identity theft return would be considered the return information of the minor. For example, if the minor were listed as a dependent on a fraudulent return, that information would not generally

101 Section 6103(h)(4) authorizes disclosure of returns and return information in a tax proceeding (1) if either the taxpayer is a party to the proceeding or the proceeding arose out of or in connection with determining the taxpayer's liability or collection of taxes owed by the taxpayer under the Code; (2) if the
be the minor’s return information. If, however, the minor were listed as the primary or secondary taxpayer on the return, then that return would be the return information of the minor because it was collected by the Service as part of a determination of the minor child’s liability under the Code. It might also be the return information of the parent since, under section 6201(c), an unpaid assessment against a minor is also considered to be an unpaid assessment against the parent, to the extent the assessment is based on compensation for the minor’s services.

7. In some circumstances, the Service may disclose return information, but not “taxpayer return information,” to other Federal agencies.

There are offenses related to identity theft that are not related to tax administration. Section 6103(h) does not provide the ability to disclose return information to other Federal agencies for nontax crimes.

Section 6103(i)(3)(A), however, does provide limited authority for the Service to make proactive disclosures of return information, other than taxpayer return information,

treatment of an item on the third party’s return is directly related to the resolution of an issue in the tax proceeding; (3) if the third party’s return or return information directly relates to a transactional relationship between the third party and the taxpayer whose liability is at issue and the third party’s return or return information directly affects the resolution of an issue in the tax proceeding; and (4) if certain requirements are met in certain criminal proceedings. For additional information regarding disclosures under section 6103(h)(4), please see the Disclosure and Privacy Law Reference Guide, infra.

that may constitute evidence of the commission of a Federal nontax crime “to the extent necessary to apprise the head of the appropriate Federal agency charged with the responsibility of enforcing such law.” I.R.C. § 6103(i)(3)(A)(i) (emphasis added). Because the statutory text uses the word “apprise,” the scope of return information disclosed under section 6103(i)(3)(A) should be limited so as to only alert the Federal nontax criminal law enforcement agency about the possible existence of a nontax crime.

Such disclosures are authorized regardless of whether the Service has concurrent jurisdiction over the crime. While the statute does not require that the return information be conclusive, the return information should sufficiently identify the specific criminal act to which it relates.

The Service may not, however, disclose “taxpayer return information” to other Federal agencies for nontax crimes. Taxpayer return information is return information that is “filed with, or furnished to, the Secretary by or on behalf of the taxpayer to whom such return information relates.” I.R.C. § 6103(b)(3). A Form W-2 is entirely taxpayer return information. The employer files it for his own liabilities, so it is his taxpayer return information. The employer files it on behalf
of the employee for the employee's liability, even if that employee is an undocumented worker. The employer also files it on behalf of the victim, and it will likely have an effect on the victim's liability. As a result, a Form W-2 (or similar document) is almost always taxpayer return information.

Note, however, that if the Federal nontax criminal law enforcement agency decides to investigate the matter, it can seek the disclosure of returns and any additional return information (including any taxpayer return information) pursuant to sections 6103(i)(1) and (2).102

8. *The Service may only disclose return information to state and local officials if they are considered Federal employees for section 6103 purposes.*

Generally speaking, there is no authority under the Code to disclose information to state and local law enforcement for nontax administration purposes. *Cf.* I.R.C. § 6103(d). State and local law enforcement personnel, however, may be considered Federal employees for the purposes of section 6103 so long as they are formally appointed as Federal employees (rather than merely detailed), they are assisting in a Federal investigation, and are supervised by a Federal employee.

It should be remembered that a taxpayer may always consent to the disclosure of his or her own return information under section 6103(c). In the case of a victim of identity theft, the taxpayer could consent to the disclosure of his or her own tax return information to state and local law enforcement. The Service, however, would need to ensure that such a disclosure would not seriously impair Federal tax administration, as discussed below. Additionally, a copy of any consent should be retained for at least a three-year period.

9. *The Service may disclose information to confirm a return's legitimacy.*

The Service may disclose enough information necessary to determine whether a return is legitimate under section 6103(k)(6). The Service must reasonably believe that the information is not otherwise available or doing so must be necessary to carry out the employee's official duties. Treas. Reg. § 301.6103(k)(6)-1(a)(2). In the identity theft context, when an employer files a document, such as a W-2, that includes a stolen SSN, the Service may contact the employer to inform the employer that the SSN does not match. The Service

---

102 Federal agencies may obtain tax information for use in nontax criminal investigations pursuant to an *ex parte* order of a federal district court judge or magistrate. I.R.C. § 6103(i)(1). Information obtained from a source other than the taxpayer or the taxpayer's representative may be disclosed in response to a written request from the head of a federal agency or its Inspector General or by certain designated Department of Justice employees. I.R.C. § 6103(i)(2). For additional information regarding disclosures under section 6103(i), please see the Disclosure and Privacy Law Reference Guide, supra.
must be cautious, however, in what exactly is revealed to the employer. The Service may inform the employer that the name and SSN do not match, but the Service may not inform the employer of the identity of the true owner of the SSN.

Additionally, if the Service determines a mismatch between the name and other contact information on a return and the SSN on, for example, a Form W-2, then the Service may contact the employee to investigate the discrepancy. The Service should take care, however, not to disclose information related to the victim, including the victim’s identity, to the employee.

E. IMPAIRMENT AND POLICY CONSIDERATIONS

Before disclosing any additional information, the Service should also consider the following issues.

1. **Information from an identity theft return should not be disclosed if that information would seriously impair Federal tax administration.**

   The Service must withhold information that would seriously impair tax administration, even if it would otherwise be eligible for disclosure under section 6103, including certain third-party return information. See I.R.C. § 6103(c), (e)(7). Once a potential identity theft has occurred, the Service should consider whether to withhold information, either through redaction or other means, regarding third-party identity theft victims and other third parties if disclosing that information would seriously impair Federal tax administration. It is a business decision what information might need to be withheld based on the damage that might be done to tax administration if such information were disclosed. In determining whether to redact certain third-party information, the Service should consider Hodge, in which the court found that the name and address of a person who used plaintiff’s SSN was third-party return information that could not be disclosed to the plaintiff. Hodge, supra.

2. **Victims may obtain copies of fraudulent returns.**

   The Service has determined that a victim of identity theft may request a copy of a return that was filed using his or her own information, though it may be heavily redacted. Redactions will include many of the issues discussed in this memorandum. For example, in some cases, a fraudulent return may list multiple victims’ information, and the Service should redact the other victims’ return information before disclosing any of the victim’s return information. For additional information, the victim should visit [https://www.irs.gov/Individuals/Instructions-for-Requesting-Copy-of-Fraudulent-Returns](https://www.irs.gov/Individuals/Instructions-for-Requesting-Copy-of-Fraudulent-Returns).

Please call Joy Gerdy Zogby at (202)317-4927 if you have any further questions.