MSP #19 IDENTITY THEFT: As Tax-Related Identity Theft Schemes Evolve, the IRS Must Continually Assess and Modify Its Victim Assistance Procedures

RESPONSIBLE OFFICIAL

Kenneth Corbin, Commissioner, Wage and Investment Division

TAXPAYER RIGHTS IMPACTED[1]

- *The Right to Quality Service*
- *The Right to Finality*

DEFINITION OF PROBLEM

Tax-related identity theft is an invasive crime that has significant impact on its victims and the IRS. Since 2004, the National Taxpayer Advocate has highlighted the need for the IRS to establish or improve procedures to assist victims of identity theft.[2] The IRS has gradually adopted many of our recommendations over the years. For example, one such change involved centralizing its identity theft victim assistance units, something for which TAS has long advocated.[3]

The IRS has made significant strides in revamping its identity theft victim assistance procedures. However, problems remain as cyber criminals continually evolve their schemes. In our review of the IRS response to identity theft, we found that:

- although identity theft case receipts are on the decline, there remains a significant inventory of unresolved identity theft cases;
- the IRS has adopted a centralized approach to identity theft victim assistance, including assignment of a sole contact person for certain victims;
- automated identity theft filters are still over-inclusive; and
- the IRS must be nimble as it counteracts emerging identity theft schemes, such as employer identity theft.

1 See Taxpayer Bill of Rights (TBOR), http://www.TaxpayerAdvocate.irs.gov/Taxpayer-Rights. The rights contained in the TBOR are now listed in the Internal Revenue Code (IRC). See Consolidated Appropriations Act, 2016, Pub. L. No 114-113, Division Q, Title IV, § 401(a) (2015) (codified at IRC § 7803(a)(3)).

2 See National Taxpayer Advocate 2015 Annual Report to Congress 180-87; National Taxpayer Advocate 2014 Annual Report to Congress vol. 2, 44-90; National Taxpayer Advocate 2013 Annual Report to Congress 75-83; National Taxpayer Advocate 2012 Annual Report to Congress 42-67; National Taxpayer Advocate 2011 Annual Report to Congress 48-73; National Taxpayer Advocate 2009 Annual Report to Congress 307-17; National Taxpayer Advocate 2008 Annual Report to Congress 79-94; National Taxpayer Advocate 2007 Annual Report to Congress 96-115; National Taxpayer Advocate 2005 Annual Report to Congress 180-91; National Taxpayer Advocate 2004 Annual Report to Congress 133-36.

3 See National Taxpayer Advocate 2007 Annual Report to Congress 115.

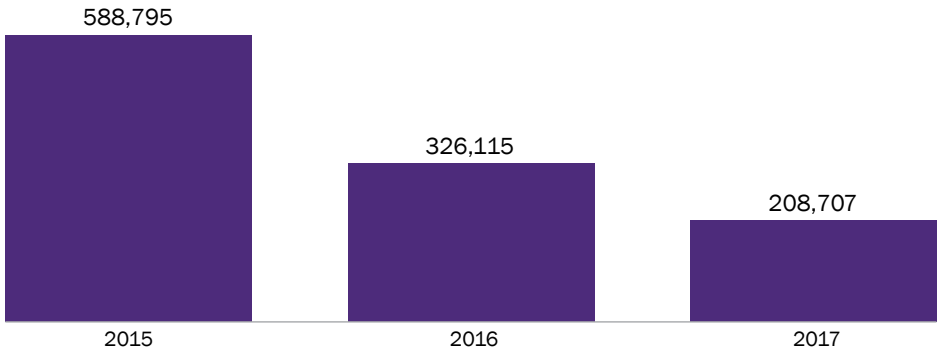
ANALYSIS OF PROBLEM

Although Identity Theft Case Receipts Are on the Decline, There Remains a Significant Inventory of Unresolved Identity Theft Cases

While still pervasive and having significant impact to victims, tax-related identity theft has been on the decline in recent years. There has been a downward trend in identity theft case receipts IRS-wide from 2015.

FIGURE 1.19.1[4]

IRS Identity Theft Receipts, January 1-September 30, 2015-2017



Through September 30, 2017, there has been a 36 percent drop in identity theft case receipts compared to the prior year, and a 65 percent drop compared to 2015.[5]

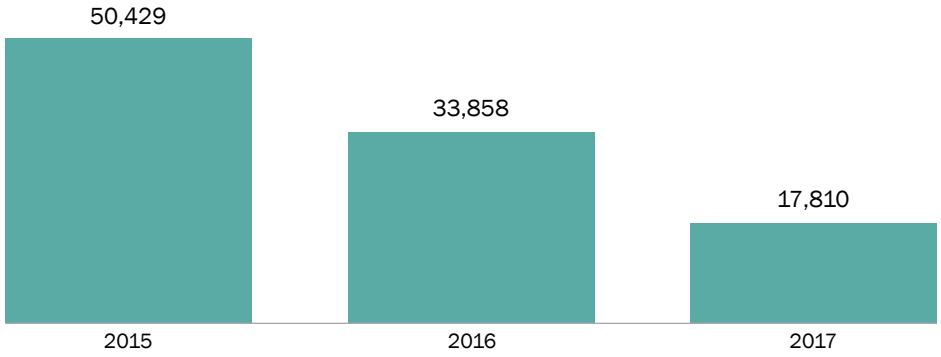
Within TAS, we have experienced a similar decline in our identity theft case receipts over the past year, which is a reversal of the upward trend in previous years.

4 IRS, *Global Identity Theft Report* (Sept. 2017). Identity Theft Victim Assistance (IDTVA) accounts for the majority of the cases, but the inventory also includes a small amount from Small Business/Self-Employed (SB/SE) (Field Exam), Large Business and International (LB&I), and Appeals.

5 Note that the 2015 and 2016 data in the table does not include inventories for Business Master File and Compliance Designated Identity Theft Adjustment, which are included in 2017 inventory.

FIGURE 1.19.2[6]

TAS Identity Theft Receipts, January 1-September 30, 2015-2017



It is not clear what the primary driver of the reversal is that caused the downward trend of identity theft case receipts. However, we believe that improvements to the IRS's identity theft filters and earlier access to information return data, has led to the decline in identity theft case receipts.

We also believe that part of the decline may be attributable to the way the IRS calculates identity theft case receipts. When the IRS revised the layout this year of the Global Identity Theft Report that is distributed monthly to its executives, it does not include all identity theft cases worked outside of the Identity Theft Victim Assistance (IDTVA) unit in Victim Assistance Servicewide Inventory. For example, identity theft cases may be worked by the Return Integrity & Compliance Services (RICS) and Submission Processing (SP) functions, but are not included in the roll-up of victim assistance identity theft case receipts reported in the Global Report.[7]

To get a sense of the volume of open identity theft cases, TAS Research conducted a query of unique taxpayers with unreversed open identity theft claim markers input during calendar years 2014–2016 and through April 1, 2017.[8] TAS Research looked for identity theft cases that have been open for more than the 180-day normal processing time that have not had an identity theft closing marker. There are more than 178,000 such taxpayers, substantially more than the inventory of 36,333 identity theft cases reported by the IRS in the IRS Global Identity Theft Report for the corresponding period.[9]

6 Data obtained from Taxpayer Advocate Management Information System (TAMIS) (Jan. 1, 2015, Jan. 1, 2016, Jan. 1, 2017; Oct. 1, 2015, Oct. 1, 2016, and Oct. 1, 2017).

7 IRM 25.23.2.21(1), *IMF Identity Theft Worked by Functions Outside Accounts Management IDTVA* (Oct. 13, 2016): "*The re-engineering effort brought accounts management and certain compliance functions under the Accounts Management Identity Theft Victim Assistance Organization. There are pockets of employees outside the new organization who will be working ID theft related issues identified using systemic applications and other applications and methods.*"; IRS, *Global Identity Theft Report* (Sept. 2017) (With Identity Theft Victim Assistance (IDTVA) making up the majority of the cases, the inventory also includes a small amount from SB/SE (Field Exam), LB&I, and Appeals).

8 IRS, Compliance Data Warehouse (CDW), Individual Master File (IMF), Transaction History table. Taxpayers are only counted once per year, but may be included more than once if their identity theft case spans multiple years. IRS did not provide information to confirm or disprove the figures during the TAS fact check process.

9 IRS, *Global Identity Theft Report* (Sept. 2017). This does not necessarily mean that the taxpayer's primary identity theft issue has not been resolved, but it does means that the IRS has not taken all actions to protect the taxpayer from further harm — for example, a closing marker is required for a taxpayer to be eligible to receive an Identity Protection Personal Identification Number (IP PIN).

The analysis completed by TAS Research yielded cases with unresolved identity theft markers servicewide, regardless of which IRS function controlled the case. In contrast, the IRS Global Identity Theft Report omitted identity theft case receipts worked by some functions, such as RICS or SP. By opting to include only a portion of its identity theft case receipts, the IRS does not provide a complete perspective and may undermine its case for sufficient funding to prevent identify theft and assist victims. While the IRS has improved its fraud detection measures and streamlined its processing of identity theft cases in certain situations, the overall problem is more pervasive that the IRS "Global" report suggests. When funding decisions are made, it would do a disservice to taxpayers if Congress were to rely on incomplete data as evidence that identity theft is no longer a serious problem for tax administration.

The IRS Has Adopted a Centralized Approach to Identity Theft Victim Assistance, Including Assignment of a Sole Contact Person for Victims

In addition to improved identity theft filters, the IRS recently overhauled its approach to identity theft victim assistance. In July 2015, the IRS established the IDTVA unit, centralizing victim assistance functions under one umbrella within the Wage and Investment (W&I) division.[10] In this centralized model, there is a core group of employees who receive specialized training in working identity theft cases.

Recently — for cases that do not require interaction with other IRS functions (such as RICS and SP) — IDTVA changed its procedures to designate a single employee as the sole contact person for an identity theft victim, from beginning to end.[11] The IDTVA assistor will provide the taxpayer with his or her name, direct phone extension, and tour of duty.[12] While we applaud the decision to provide a sole contact person — something the National Taxpayer Advocate has recommended since 2012[13] — we urge the IRS to extend this privilege to identity theft victims facing multiple issues and dealing with multiple IRS functions; these are the taxpayers most likely to have their cases fall between the cracks.

Shortly after standup in 2015, IDTVA convened a team (comprised of members from across various IRS organizations, including TAS) to overhaul the identity theft victim assistance procedures. This Identity Theft Re-engineering Team made many recommendations that allow the IRS to provide better service

For cases that do not require interaction with other IRS functions, Identity Theft Victim Assistance changed its procedures to designate a single employee as the sole contact person for an identity theft victim, from beginning to end — something the National Taxpayer Advocate has recommended since 2012.

10 While the IRS centralized most functions under IDTVA, some functions (such as Return Integrity & Compliance Services and Submission Processing) continue to work identity theft cases outside of IDTVA.

11 IRM Exhibit 25.23.4-6, *IDTVA Routing Matrix* (Oct. 1, 2017) ("With IDT, in most cases, there should be one single point of contact for a taxpayer.").

12 IRM 25.23.4.18, *Telephone Contact Procedures for IDTVA Paper Employees Only* (Oct. 27, 2017) ("Upon receiving those calls, the employee should try to answer the taxpayer's questions.... Provide the taxpayer the toll-free number, employee's name extension and Tour of Duty (TOD) when available based on the TP's time zone.").

13 *See* National Taxpayer Advocate 2012 Annual Report to Congress 67.

to victims of identity theft. For example, the team strengthened the global account review procedures to ensure all actions are taken prior to closing an identity theft case. The re-engineering team also expanded the role and scope of the Identity Protection Specialized Unit (IPSU), enabling certain types of identity theft cases to be addressed by IPSU employees. The Taxpayer Protection Program (TPP) End-to-End (E2E) Improvement Team improved the taxpayer's experience by making several process improvements, which includes updating TPP letters to encourage taxpayer response, creating an internal TPP website to shorten average handle time, and improve taxpayer authentication.

One preventive measure the IRS continues to use is the Identity Protection Personal Identification Number (IP PIN). This IP PIN is a unique number assigned to victims of identity theft to use in conjunction with their tax identification number (TIN, usually a Social Security number) when filing tax returns in future years, after their account issues have been fully resolved and their identity and address have been verified. Once the IRS assigns an IP PIN to a taxpayer, it will not accept an e-filed tax return without this IP PIN and paper return processing will be delayed by a manual review to verify the taxpayer's identity. The IRS issued 3.5 million IP PINs for use in the 2017 filing season.[14] Since the IRS began using IP PINs in 2011, it has been a very effective safeguard that prevents fraud from recurring.

Automated Identity Theft Filters Are Still Over-Inclusive

As tax-related identity theft refund fraud schemes become more sophisticated, the IRS continues to evolve its various filters, rules, and data mining models to combat these schemes. For example, the TPP is a process where the IRS uses a series of filters to stop certain tax returns it suspects are filed by an identity thief. TPP filters can be adjusted during the filing season if the data suggests that either the filters are too sensitive or not sensitive enough.[15] The IRS will not issue a refund for a return flagged by the TPP until the taxpayer can verify his or her identity by calling the TPP toll-free phone line and answering certain "high risk authentication" questions.[16]

As of September 30, 1.9 million suspicious tax returns were selected by the TPP identity theft filters in calendar year (CY) 2017.[17] In past years, we have had concerns regarding the high false detection rate.[18] High false detection rates can lead to significant downstream consequences for both the IRS and taxpayers. When legitimate taxpayers are ensnared in an over-reaching IRS fraud detection mechanism, they may experience protracted refund delays as they navigate the authentication processes to prove they are the true tax return filers.

In CY 2016, the false detection rate for TPP identity theft filters was 53 percent, which means that of all returns flagged as potentially fraudulent, more than half turned out to be legitimate.[19] In CY 2017 through September 30, the false detection rate for identity theft filters overall increased to 62 percent.[20]

14 IRM 25.23.2.20, *Identity Protection Personal Identification Number (IP PIN)* (Sept. 15, 2017); IRS, *Global ID Theft Report* (Aug. 2017).

15 IRS response to TAS information request (Nov. 6, 2017).

16 For taxpayers failing oral authentication with a phone assistor or for taxpayers deemed at high risk for identity impersonation (*i.e.*, data breach victims), the only option is to visit a Taxpayer Assistance Center (TAC). IRM 25.25.6.3.2, *Referring the Caller to the Taxpayer Assistance Center (TAC) - Taxpayer Protection Program (TPP) Toll Free Assistors* (July 14, 2017).

17 IRS response to TAS information request (Nov. 6, 2017).

18 National Taxpayer Advocate 2016 Annual Report to Congress 151-60 (Most Serious Problem: *The IRS's Failure to Establish Goals to Reduce High False Positive Rates for Its Fraud Detection Programs Increases Taxpayer Burden and Compromises Taxpayer Rights*).

19 IRS Wage & Investment Division, *Business Performance Review* 9 (Feb. 9, 2017).

20 *Id.*

In calendar year 2017 through September 30, the false detection rate for identity theft filters overall increased to 62 percent. The IRS asserts that the identity theft filter false detection rate was a result of several large-scale data breach incidents from external organizations, which made it easier for identity thieves to access sensitive taxpayer information and more difficult for the IRS to create filters that can differentiate between legitimate and illegitimate tax returns.

RICS, the function that is in charge of the TPP, asserts that the identity theft filter false detection rate was a result of several large scale data breach incidents from external organizations (see discussion below), which made it easier for identity thieves to access sensitive taxpayer information and more difficult for the IRS to create filters that can differentiate between legitimate and illegitimate tax returns.

The IRS Must Be Nimble As It Counteracts Emerging Identity Theft Schemes, Such As Employer Identity Theft

As the IRS gets more adept at detecting identity theft, fraudsters get more sophisticated in their schemes. The IRS needs the ability to quickly identify and react to new schemes. It cannot afford to let months or even weeks go by without plugging a vulnerability in their filters.

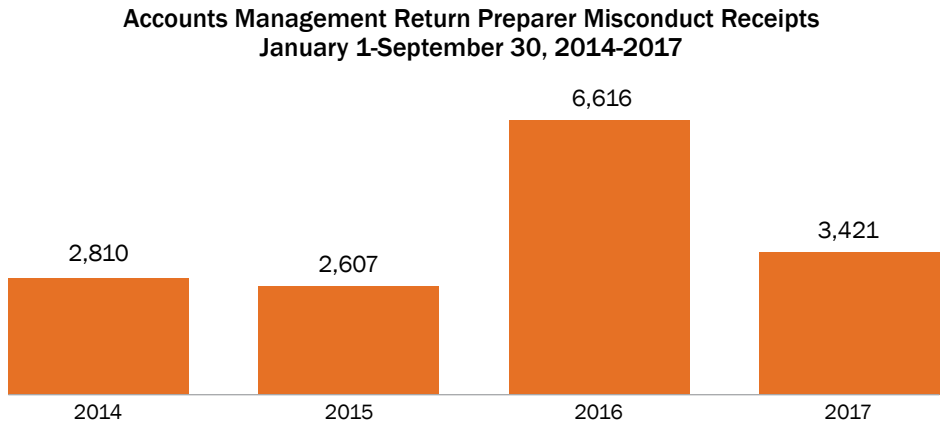
One emerging identity theft scheme involves the reporting of false data that is filed on stolen employer identification numbers (EINs) or tax returns. Criminals have long used stolen EINs to perpetrate tax fraud by creating falsified Forms W-2, *Wage and Tax Statement* or Forms 1099, *Miscellaneous Income*, but in the past couple of years there has been an increase in the filing of fraudulent business tax returns.[21] The IRS is aware of these types of schemes and has created a team to respond to employer identity theft issues.

Return preparer misconduct (RPM) is another type of refund fraud scheme that, like employer identity theft, is likely to bypass traditional identity theft filters because the perpetrator has access to the legitimate filer's tax return information. The IRS began tracking return preparer misconduct cases in 2014.[22] While the raw number of RPM cases may be relatively low, this type of fraud is particularly traumatic because taxpayers are being victimized by people they entrusted with their very personal information.

21 See IRS, FS-2017-10, *Information on Identity Theft for Business, Partnerships and Estate and Trusts* (July 25, 2017).

22 IRM 25.23.2.19.1.2, *TC 971 AC 504 - Miscellaneous Field Code SPCL1, SPCL2, RPM1, RPM2, RPM3, RPM4, and EAFAIL* (Sept. 15, 2017).

FIGURE 1.19.3[23]



Large Scale Data Breaches May Cause a Reversal in the Downward Trend of Identity Theft Case Receipts

The IRS must also develop procedures to assist victims of new schemes in a timely manner. Recent schemes have targeted businesses and other large organizations to gain access to personal information of their employees or customers. For example, the sensitive personal information of over 145 million American consumers was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies.[24] The IRS must assess how best to assist victims of these large-scale data breaches. With so many taxpayers made vulnerable by having their personal identifying information available to hackers, we can expect that tax-related identity theft will ramp up. Taxpayer personal information may include their full name, Social Security number, address, and even information from their last filed return or Form W-2, *Wage and Tax Statement*.

Given the risk that an identity thief could have full access to an individual's personal information, the IRS may need to reconsider how secure allowing online or phone authentication will be. The IRS will need to consider alternative methods of validating a taxpayer's identity.

In the past, we recommended that the IRS expand the use of IP PINs to allow taxpayers in every state the ability to receive an IP PIN to protect their accounts.[25] There was concern about the cost of administering the IP PIN program (new IP PINs must be generated each year, and phone lines must be staffed to assist the percentage of taxpayers who will invariably misplace the IP PIN) and the IRS did not adopt our recommendation.[26] We recognize that there is a cost to providing an IP PIN, but we also know that there is a considerable cost to **not** protecting taxpayer accounts from fraud.

23 IRS response to TAS information request (Nov. 6, 2017).

24 See Equifax, http://www.prnewswire.com/news-releases/equifax-announces-cybersecurity-firm-has-concluded-forensic-investigation-of-cybersecurity-incident-300529345.html.

25 See National Taxpayer Advocate 2015 Annual Report to Congress 187.

26 See National Taxpayer Advocate 2016 Objectives Report vol. 2, 105 (*IRS Responses and National Taxpayer Advocate's Comments Regarding Most Serious Problems Identified in the 2015 Annual Report to Congress*).

If the IRS finds it too cost-prohibitive to expand the IP PIN program under its current budget constraints, it should explore other ways to fund the cost. When a company is at fault for allowing a large-scale data breach, it often offers to pay for credit monitoring service for impacted individuals. The IRS should enter into similar agreements with these companies and have them pay for the cost of the IRS issuing IP PINs to impacted individuals.

RECOMMENDATIONS

The National Taxpayer Advocate recommends that the IRS:

1. Include identity theft case receipts received IRS-wide — including RICS and SP receipts — in its Global Identity Theft Report.
2. Expand its procedures so that all identity theft victims – including those with multiple tax issues and needing to interact with IRS functions outside of the Identity Theft Victim Assistance function — are assigned a sole contact person to assist them until all identity theft-related issues are resolved.
3. Set a limit of 35 percent for the false detection rate for its Taxpayer Protection Program identity theft filters for 2018 and 20 percent for 2019 and thereafter.
4. Expand the IP PIN program by offering it to all taxpayers to proactively protect their tax accounts against tax related identity theft.
5. Develop procedures to address large scale data breaches while minimizing the burden on victims.