MSP #9 FRAUD DETECTION: 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

RESPONSIBLE OFFICIAL

Debra Holland, Commissioner, Wage and Investment Division

TAXPAYER RIGHTS IMPACTED[1]

- *The Right to Quality Service*
- *The Right to Pay No More Than the Correct Amount of Tax*
- *The Right to Privacy*
- *The Right to a Fair and Just Tax System*

DEFINITION OF PROBLEM[2]

Over the past decade, fraud and identity theft have increasingly plagued consumers, businesses, and financial institutions.[3] The IRS has also been impacted. A 2015 Treasury Inspector General for Tax Administration (TIGTA) report found that the IRS processed approximately 1.5 million returns for tax year (TY) 2010 with characteristics of identity theft, issuing potentially fraudulent refunds totaling $5.2 billion.[4]

To detect and prevent identity theft and other tax refund fraud, the IRS has established a complicated screening process.[5] When a return is flagged by one of the multiple IRS systems that scrutinize returns for characteristics of refund fraud or identity theft, the refund is held until the taxpayer can authenticate

1 See Taxpayer Bill of Rights (TBOR), 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 Volume 3 of the 2016 Annual Report to Congress contains an extended literature review related to this topic. Literature Review: *Reducing "False Positive" Determinations in Fraud Detection*, vol. 3, *infra*.

3 See *also* American Bankers Association (ABA), *Banks Stop $11 Billion in Fraud Attempts in 2014* (Jan. 27, 2016), http://www.aba.com/press/pages/012716depositsurvey.aspx. While attempted fraud against bank deposit accounts reached $13 billion, banks' prevention measures stopped $11 billion in fraudulent transactions. Bureau of Justice Statistics (Sept. 27, 2015), www.bjs.gov. An estimated 17.6 million persons, or about seven percent of U.S. residents age 16 or older, were victims of at least one incident of identity theft in 2014.

4 Treasury Inspector General for Tax Administration (TIGTA), Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 24, 2015).

5 The IRS Return Integrity & Compliance Services (RICS) uses three independent systems to identify returns when it suspects identity theft has occurred or that the return is fraudulent — the Dependent Database (DDb), the Return Review Program (RRP), and the Electronic Fraud Detection System (EFDS).

his or her identity, or until the information on the return can be verified.[6] Although these systems do identify improper returns and prevent improper refunds from being issued, they also have a high degree of inaccuracy, which results in unnecessary refund delays and reduced taxpayer morale.[7]

Over the past 13 years, the National Taxpayer Advocate has consistently advocated for taxpayers whose legitimate refunds have been unreasonably delayed by the IRS and recommended improvements to reduce taxpayer burden while preventing identity theft and refund fraud.[8]

The National Taxpayer Advocate remains concerned that:

- IRS fraud detection systems have a high false positive rate (FPR).[9] For calendar year (CY) 2016 through September, IRS filters and business rules used for detecting fraudulent returns and identity theft had many FPRs over 50 percent. These improper selections delayed approximately 1.2 million tax returns associated with about $9 billion in legitimate refunds for more than an additional 30 days on average. Notably, one IRS process for reviewing returns for identity theft had an FPR of roughly 91 percent.[10]
- The issuance of refunds that were improperly identified by IRS systems as being returns likely resulting from identity theft or fraud was significantly delayed. On average, these refunds were delayed an additional 36 days, meaning it took taxpayers nearly two months to receive their refunds.[11]

6 The IRS has distinct screening processes for identity theft and refund fraud. For purposes of this report, we will refer to refund fraud in its broadest sense, to include identity theft as a subset of refund fraud. *See also* National Taxpayer Advocate 2015 Annual Report to Congress 45-55 (Most Serious Problem: *Revenue Protection: Hundreds of Thousands of Taxpayers File Legitimate Tax Returns That Are Incorrectly Flagged and Experience Substantial Delays in Receiving Their Refunds Because of an Increasing Rate of "False Positives" Within the IRS's Pre-Refund Wage Verification Program*). The IRS uses identity theft filters to select and suspend the processing of tax returns it suspects were filed by identity thieves. When the IRS stops a return, it will send the taxpayer a letter asking him or her to either call the Taxpayer Protection Program (TPP) phone number, visit the ID verify website, or appear in person at a Taxpayer Assistance Center (TAC) to verify his or her identity. Internal Revenue Manual (IRM) 25.25.6.1, *Taxpayer Protection Program* (May 26, 2015).

7 Gregg S. Henzel *et al.*, *Using Model Calibration and Optimization to Reduce Fraud Risk: How Financial Institutions Can Identify Fraud More Effectively While Reducing Costs* 3-4 (Crowe Horwath 2015), https://www.crowehorwath.com/folio-pdf/Using-Model-Calibration-and-Optimization-to-Reduce-Fraud-Risk-Article-RISK-16007-008A.pdf. *See also* Most Serious Problem: *Voluntary Compliance: The IRS Is Overly Focused on So-Called "Enforcement" Revenue and Productivity, and Does Not Make Sufficient Use of Behavioral Research Insights to Increase Voluntary Tax Compliance*, *supra*.

8 *See, e.g.*, National Taxpayer Advocate 2015 Annual Report to Congress, 45-55, 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, 95-110; 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 25-54, 180-91; National Taxpayer Advocate 2004 Annual Report to Congress 133-36; and National Taxpayer Advocate 2003 Annual Report to Congress 175-81.

9 A false positive occurs when a system selects a legitimate return and delays the refund past the prescribed review period. IRS response to TAS information request (Nov. 3, 2016).

10 *Id.* The returns reviewed by this process include taxpayers who have previously been victimized by identity theft, and therefore these filters are more stringent, which may account in part for this high false positive rate (FPR).

11 *Id.* The normal timeframe for processing a refund is 21 days. These refunds were delayed 36 days beyond that normal processing time, meaning that the average processing time for these refunds was 57 days. *See* IRS Newswire, *As Holidays Approach, IRS Reminds Taxpayers of Refund Delays in 2017*, IR-2016-152 (Nov. 22, 2016). "As the IRS steps up its efforts to combat identity theft and tax refund fraud through its many processing filters, legitimate refund returns sometimes get delayed during the review process."

- IRS fraud detection systems are antiquated and the IRS's ability to adjust the systems in real time is limited, placing them outside the industry standard for fraud detection systems.[12]

IRS systems that improperly flag legitimate tax returns and delay refund issuance can create a financial hardship for taxpayers, expend unnecessary IRS resources to resolve the issues, and negatively impact taxpayers' voluntary compliance. Thus, as literature has shown, in order to reduce FPRs, it is extremely important that the IRS identify the necessary elements to establish a robust fraud detection system.[13] This objective can be met by regularly consulting with other government entities and private industry about best practices for effectively designing systems to accurately detect fraud. Through this process, the IRS should establish aspirational goals for reducing FPRs. This goal is within reach after Congress passed legislation moving the deadline for third-party information reporting up from the end of February (and the end of March for electronic filers) to January 31, providing the IRS more time to match the wage and tax information reported on the taxpayer's return against the information submitted by third parties.[14]

ANALYSIS OF PROBLEM

Background

The return integrity program, a process critical to the IRS's strategy to address identity theft and detect and prevent improper fraudulent refunds, is complex and multifaceted.[15] The Return Integrity & Compliance Services (RICS) Integrity and Verification Operation (IVO) — a part of the Wage & Investment (W&I) Division — uses filters, rules, data mining models, and manual reviews to identify potentially false returns, usually through wages or withholding reported on the returns, to stop fraudulent refunds before the IRS issues them.[16]

The IRS electronically screens tax returns using three independent systems: the Dependent Database (DDb), the Return Review Program (RRP), and the Electronic Fraud Detection System (EFDS).[17] If one of these systems flags a return as potentially fraudulent, the return goes to the Taxpayer Protection Program (TPP) or the Income Wage Verification (IWV) program for further scrutiny.

In addition to the RICS programs, the IRS began employing additional filters known as the Identity Theft business rules in January 2009. The business rules are applied to any return filed with a Social Security number (SSN) associated with an identity theft indicator. These returns are not allowed to post

12 "The heart of an efficient fraud prevention solution is a strong analytics engine, which can use the available data intelligently, recognize and identify patterns, provide real time visibility into threats, and signal discrepancies. It should enable the solution to detect and respond swiftly to suspicious or fraudulent transactions." Vasudevan Easwaran, *The Combination to a Safe Future for Banking Using Technology in the Banking Industry to Prevent Fraud*, WIPRO (2015).

13 See Literature Review: *Reducing "False Positive" Determinations in Fraud Detection*, vol. 3, *infra*.

14 Section 201 of the Protecting Americans From Tax Hikes (PATH) Act amended IRC § 6071 to require that certain information returns be filed by January 31, generally the same date as the due date for employee and payee statements, and are no longer eligible for the extended filing date for electronically filed returns under section 6071(b). *See* Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Division Q, Title IV, § 201 (2015). This legislative change is consistent with prior National Taxpayer Advocate recommendations. *See, e.g.*, National Taxpayer Advocate 2015 Annual Report to Congress 45-55; National Taxpayer Advocate 2013 Annual Report to Congress vol. 2, 86-88; National Taxpayer Advocate 2012 Annual Report to Congress 180-91; National Taxpayer Advocate 2011 Annual Report to Congress 284-95; National Taxpayer Advocate 2009 Annual Report to Congress 338-45.

15 Internal Revenue Manual (IRM) 25.25.1.1 (Feb. 19, 2015).

16 IRM 25.25.2.1(1) (Aug. 20, 2015).

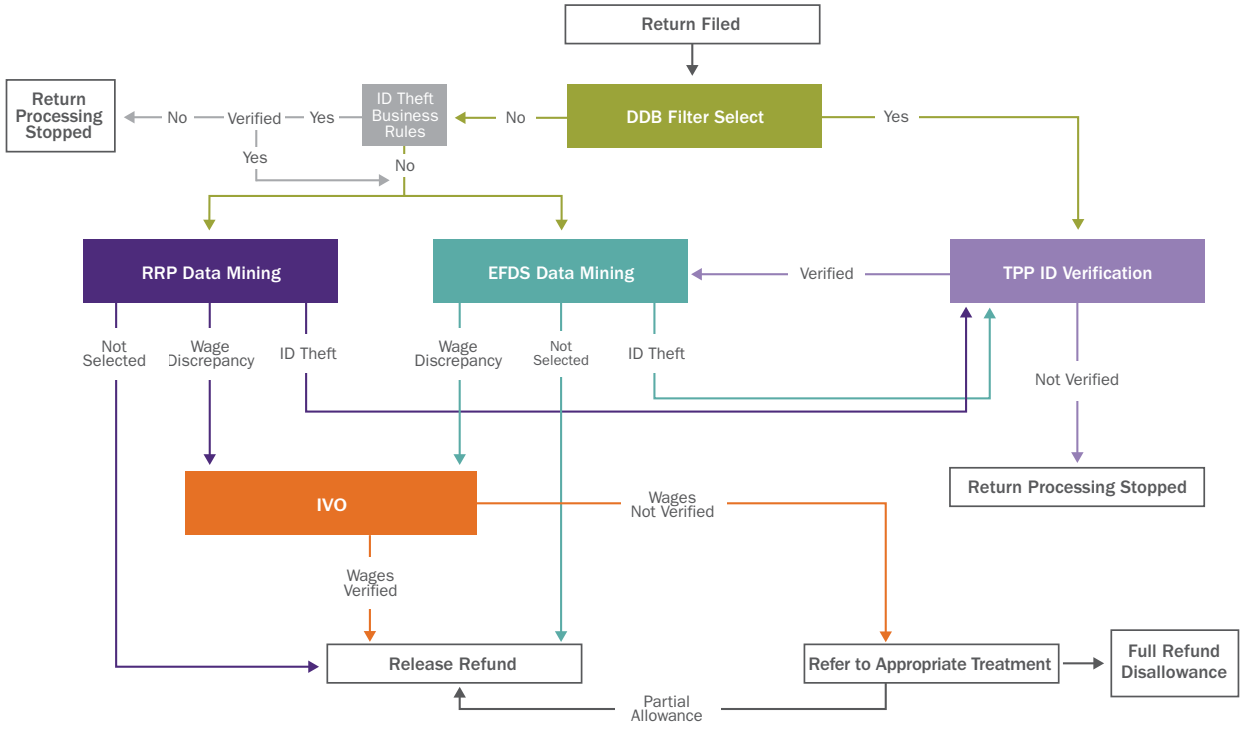
17 IRM 25.25.6.1 (Aug. 26, 2016).

to taxpayers' accounts (these are called "unpostable" returns) until the IRS can review the returns and accounts, and determine that they belong to the valid SSN owners.[18]

Figure 1.9.1 provides a simplified flow chart of the complicated processes the IRS uses to screen returns claiming refunds for identity theft and fraud.

FIGURE 1.9.1

Flow Chart of Refund Return Screening for Identity Theft and Fraud



As illustrated above, when a refund return is subject to the TPP, it will first be analyzed by the DDb system which will look for identity theft characteristics. As of CY 2016 through September, the DDb system has selected 1,184,976 returns with an FPR of 49 percent, and the affected returns took an average of 57 days to be processed.[19]

The RRP will select returns for both the TPP and the IWV programs. RRP then generates scores that relate to the predictive value of possible identity theft or fraud, or both.[20] For CY 2016 through

18 National Taxpayer Advocate 2009 Annual Report to Congress 307-17.

19 IRS response to TAS information request (Nov. 3, 2016). The IRS generally allows 21 days for a return to be processed. The processing of these returns took about 36 days beyond the normal 21 day processing time, meaning that the total return processing time for these returns was about 57 days. After the return is scrutinized by the DDb system, returns filed with an Social Security number associated with the identity theft indicators are subjected to a separate set of business rules. For calendar year (CY) 2016 through September, the IRS suspended the processing of 736,111 returns that did not pass the business rules with an FPR of 91 percent and an average processing delay of 30 days. The IRS has committed to eliminating the business rules that are outside of the TPP in CY 2017.

20 *See* TIGTA, Ref. No. 2015-20-060, *The Return Review Program Enhances the Identification of Fraud; However, System Security Needs Improvement* (July 2, 2015).

IRS fraud detection systems have a high false positive rate (FPR). For calendar year 2016 through September, IRS filters and business rules used for detecting fraudulent returns and identity theft had many FPRs over 50 percent. These improper selections delayed approximately 1.2 million tax returns associated with about $9 billion in legitimate refunds for more than an additional 30 days on average. Notably, one IRS process for reviewing returns for identity theft had an FPR of roughly 91 percent.

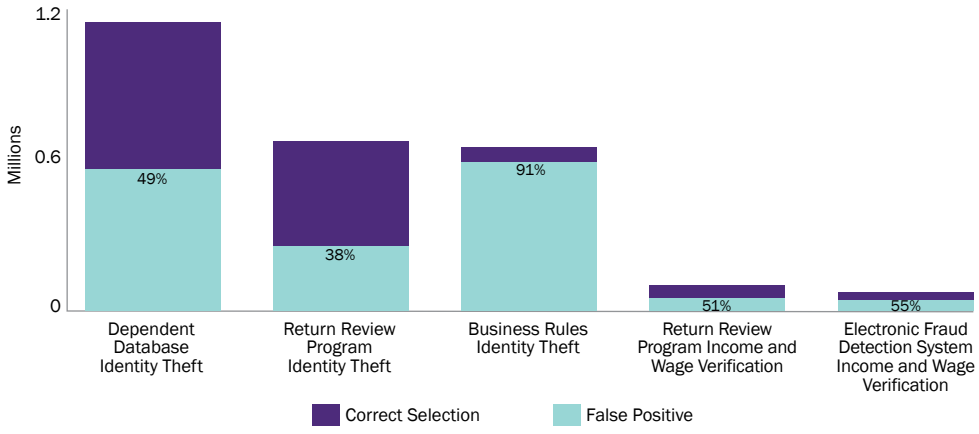
September, RRP has selected 698,960 returns for potential identity theft with an FPR of 37.9 percent, and the affected returns took an average of 57 days to be processed (*i.e.*, this system scrutinizes returns for both identity theft or fraud).[21] Likewise, RRP selected 103,520 returns for potential refund fraud during the same period. The FPR for improperly selected refund fraud returns was 50.6 percent.[22]

The EFDS program will run simultaneously with the RRP program. EFDS uses data mining models to score each Form W-2 and 1099 on refund returns for fraud potential based on business rules that consider return and filing characteristics.[23] For CY 2016 through September, EFDS has selected 77,810 returns with an FPR of 54.5 percent, and the affected returns took an average of 55 days to be processed.[24]

Figure 1.9.2 shows the volume and false positive rates for the above-mentioned IRS identity theft and fraud detection systems.[25]

FIGURE 1.9.2

Program Volumes and False Positives 2016 (through September)



21 IRS response to TAS information request (Nov. 3, 2016).

22 *Id.*

23 IRS response to TAS information request (Aug. 20, 2015). IRM 25.25.2.1 (Aug. 20, 2015).

24 IRS response to TAS information request (Nov. 3, 2016).

25 *Id.*

It appears that the IRS has accepted these FPRs as a necessary byproduct of risk detection, viewing the harm to legitimate taxpayers as a minor inconvenience. However, other government agencies, such as the U.S. Citizenship and Immigration Service (USCIS), are making efforts to improve error rates to as little as three percent.[26] The National Taxpayer Advocate realizes that identifying fraud and identity theft in tax administration is likely much different from the processes established by USCIS, but it illustrates the point that other government agencies are interested and motivated to reduce FPRs.

IRS Systems Are Antiquated and Lack the Nimbleness Necessary to Function in an Ever Changing World of Fraud and Identity Theft

The high false positive rates set out above result in thousands of taxpayers with legitimate returns being subjected to a frustrating and often elusive process. If the IRS is scrutinizing the return for possible identity theft, the taxpayer will likely be instructed to contact the IRS's dedicated Taxpayer Protection Program line, which had a Level of Service of 31.7 percent for fiscal year 2016 and a wait time of almost 11 minutes.

The IRS's EFDS system is incapable of having its filters adjusted regularly.[27] However, the DDb and RRP systems are capable of having their filters adjusted.[28] DDb filters are able to be changed, if needed, on a weekly basis, and RRP has set aside programming dates to make that kind of change during the filing season.[29] Despite the systems' abilities to have their filters changed to address emerging circumstances, the IRS has established a cumbersome and laborious process for such changes to occur. For instance, any changes to the RRP must receive approval from the Business Rules and Requirements Management (BRRM) office, and any changes to the DDb are subject to a different process.[30] BRRM does not meet regularly; therefore, any change request that needs immediate attention must go through a time-consuming approval process resulting in more refund delays. Creating a sub-approval group authorized to implement real-time modifications to screening rules and filters would allow for faster resolution of systemic issues and minimization of taxpayer harm. Such an approach would better align the IRS with accepted private industry practices to detect and prevent fraud. Specifically, experts in this area advise that designing an organizational structure that allows sharing of information in real time enables all necessary stakeholders to evaluate and adjust an organization's fraud detection systems and filters based on this information.[31] In fact, for identity theft and fraud detection systems to be effective, the organization's leaders must accept that some traditional implementation and support processes are too slow to react to actions of fraud groups.[32]

Furthermore, having a large number of stakeholders involved in the decision-making process runs a "risk of over-governance resulting in duplication, inefficiencies, and uncertainty relating to ownership of fraud

26 *E-Verify Progressing, but Still Needs Work, GAO Finds*, CQ HOMELAND SECURITY (Congressional Quarterly, Washington, DC) (Jan. 20, 2011).

27 TIGTA, Ref. No. 2015-20-093, *Review of the Electronic Fraud Detection System* (Sept. 2015) (stating that EFDS is modified annually).

28 IRS response to TAS information request (Nov. 3, 2016).

29 *Id.*

30 IRM 1.1.13.6.3.4 (Oct. 7, 2013). The office is responsible for the coordination and execution of the activities required to define, develop, maintain, and control business requirements and rules.

31 Deloitte, *The Latest Tools and Tactics for Battling Bank Fraud* 3 (May 1, 2014), http://deloitte.wsj.com/cio/2014/05/01/the-latest-tools-tactics-for-battling-bank-fraud/ (Dec. 31, 2016).

32 *Id.*

detection issues needing resolution."[33] The heart of an efficient fraud prevention solution is a strong analytics engine, which can use the available data intelligently, recognize and identify patterns, provide real time visibility into threats, and signal discrepancies.[34] It should enable the solution to detect and respond swiftly to suspicious or fraudulent transactions.[35] It appears that while the IRS's DDb and RRP systems have the analytic capabilities necessary for a successful fraud and identity theft detection system, the IRS is not taking full advantage of these capabilities. Instead, the IRS adheres to a cumbersome process for changing system filters, thereby limiting the system abilities to respond to changing circumstances in real time.

In addition to IRS systems lacking the capability to adjust in real-time, another significant drawback is system limitations towards analyzing information simultaneously. As described above, IRS systems work independently from one another, thereby extending the time for a return to be analyzed, resulting in additional refund delays and frustrated taxpayers.

Continuing and Enhancing Collaboration in the Form of Public-Private Partnerships Can Leverage the IRS's Ability to Fight Identity Theft and Refund Fraud

The literature[36] has shown that in the financial sector, a system developed to detect fraud normally contains the following four elements:

- Detect: predict fraud before it happens;
- Respond: apply new fraud insights;
- Investigate: turn fraud intelligence into action; and
- Discover: leverage existing historical data.[37]

Any successful fraud detection system should also contain a combination of the following types of analytics:

- *Advanced Analytics:* Critical data drawn from across the enterprise can be centralized in a flexible framework that, unlike more limiting relational databases, can accommodate multiple data formats in a production environment.[38]
- *Behavioral Analytics:* Behavioral analytics solutions are designed to understand the normal behavior of each individual consisting of a detailed, multi-faceted combination of timing, sequence, devices, locations, channels, and the financial and non-financial activities performed via those channels.[39]

33 Australian Government, Inspector-General of Taxation, *Review into the Australian Taxation Office's Compliance Approach to Individual Taxpayers Income Tax Refund Integrity Program* 13 (Sept. 2013), http://igt.gov.au/files/2014/11/income-tax-refund-integrity-program.pdf.

34 Vasudevan Easwaran, *The Combination to a Safe Future for Banking Using Technology in the Banking Industry to Prevent Fraud*, WIPRO (2015).

35 *Id.*

36 *See, e.g.* IBM Software, *Fighting Fraud in Banking with Big Data and Analytics* (Oct. 2014), discussed in Literature Review: *Reducing "False Positive" Determinations in Fraud Detection*, vol. 3, *infra*.

37 IBM Software, *Fighting Fraud in Banking with Big Data and Analytics* (Oct. 2014).

38 Deloitte, Chief Information Officer (CIO) News, CIO Insight and Analysis, Wall Street Journal, *The Latest Tools and Tactics for Battling Bank Fraud* 2 (May 1, 2014), http://deloitte.wsj.com/cio/2014/05/01/the-latest-tools-tactics-for-battling-bank-fraud/.

39 Craig Priess, *Behavioral Analytics for Detecting Fraud* 2 (Mar. 18, 2015), https://www.bai.org/banking-strategies/article-detail/behavioral-analytics-for-detecting-fraud.

- *Transaction Analytics:* This technique allows financial institutions to analyze their customers' detailed transaction data over time to gain an understanding of purchasing patterns and behaviors.[40]
- *Anomaly Analytics:* This analytical technique is focused on detecting inconsistencies with previously demonstrated "normal" patterns of behavior.[41]

Although the IRS uses some of these analytic techniques in its fraud detection systems, its systems still have limitations, such as their inability to share information with one another, essentially only allowing these systems to operate in a vacuum. Therefore, the IRS should continue and enhance its collaboration with experts in the financial industry, including the Federal Financial Institutions Examination Council (FFIEC),[42] to identify necessary elements of a robust fraud detection system and learn from private sector and other tax administration experiences to establish best practices for its fraud detection programs. A good example of IRS's collaboration with states and industry partners is the IRS Security Summit.[43]

The National Taxpayer Advocate commends the IRS for its involvement in the Security Summit, but encourages the IRS to leverage private partnerships to a greater extent, to identify industry standards for designing and implementing fraud detection systems that are modern and effective. Additionally, the IRS should establish partnerships with other government agencies, such as the Defense Intelligence Agency, that use data mining and risk detection in an effort to learn more about successful government systems and processes.

IRS's Outdated Systems That Generate High FPRs Result in a High Price for Both Taxpayers and the IRS

IRS Systems with High FPRs Harm Legitimate Taxpayers by Significantly Delaying Their Refunds and Entangling Them in an IRS System That Is Challenging to Navigate

The high FPRs set out above result in thousands of taxpayers with legitimate returns being subjected to a frustrating and often elusive process. If the IRS is scrutinizing the return for possible identity theft, the taxpayer will likely be instructed to contact the IRS's dedicated TPP line, which had a Level of Service (LOS) of 31.7 percent for fiscal year (FY) 2016 and a wait time of almost 11 minutes.[44] If the taxpayer's return was being scrutinized for refund fraud, the taxpayer would call into Accounts Management, which had a LOS of 53.4 percent for FY 2016 and a wait time of almost 18 minutes.[45] If a taxpayer tries to get

40 Dean Nolan, *Combating Fraud with Transaction Analytics* (Apr. 2, 2014), https://www.bai.org/banking-strategies/article-detail/combating-fraud-with-transaction-analytics.

41 The power of anomaly detection lies in the fact that it doesn't matter how the account is compromised - whether it's a Trojan or other malware, stolen credentials, or social engineering through customer service — the suspicious behavior relative to established norms is what provides a clue or signals that something is amiss. Guardian Analytics, *Best Practices for Detecting Banking Fraud*, 2013, http://www.cbai.com/news/Best_Practices_for_Detecting_Fraud_white_paper.pdf. For a more in depth discussion about how private industry has leveraged modern technology to detect and prevent identity theft and fraud, see Literature Review: *Reducing "False Positive" Determinations in Fraud Detection*, vol. 3, *infra*.

42 The Federal Financial Institutions Examination Council, https://www.ffiec.gov/.

43 *See* IRS, *Security Summit Partners Update Identity Theft Initiatives for 2017*, FS-2016-21, June 2016, https://www.irs.gov/uac/security-summit-partners-update-identity-theft-initiatives-for-2017 (last visited Dec. 31, 2016). The IRS Security Summit allows partners to identify possible identity theft (IDT) schemes and report them to the IRS and state partners to help them stay on top of emerging schemes; increases public awareness about the need for computer security and to provide people with tips on how to protect their personal information; and it also established seven workgroups for 2017, including authentication, financial services, lead reporting & information sharing, supporting the filing season 2017, tax professional, Strategic Threat Assessment & Response, and Communications subgroups.

44 IRS, Joint Operations Center (JOC), *TPP Snapshot Reports* (FY 2016).

45 IRS, JOC, *Snapshot Reports: Enterprise Snapshot* (week ending Sept. 30, 2016; report generated Nov. 30, 2016).

Private sector research shows customers who are subjected to false positives are likely to take their business and go elsewhere … Unlike customers making a purchase, taxpayers have little choice other than interacting with the IRS. However, taxpayers may be discouraged by the experience of having their returns improperly delayed, increasing the likelihood that they will disengage from their dealings with the IRS in the future.

information from the "Where's My Refund" application, he or she will receive a generic message prompting a call to the IRS.

Even if the taxpayer does reach a customer service representative (CSR), he or she will find the CSR does not have access to the EFDS histories and cannot give specific responses to taxpayer inquiries.[46] CSRs take down information and refer it to the IWV group in IVO. IVO, however, does not call back or correspond with a taxpayer based on the referral from a CSR. If the information forwarded by the CSR is not verifiable, IVO will simply close out the referral on an Account Management Services application, without contacting the taxpayer.[47]

Not only can scrutinizing a legitimate return unnecessarily subject taxpayers to a frustrating process, but it may also create a significant financial strain. For example, a delay of more than a month could pose severe consequences for a taxpayer who was relying on the refund to assist with medical expenses, rent, heating, or other necessary living expenses.

High FPRs Also Increase Direct and Indirect Costs for the IRS

High FPRs also come at a cost to the IRS and are a drain on the IRS's limited resources.[48] Commentators believe that in the private sector false positives cost businesses more than the actual fraud.[49] For example, when a taxpayer's return is incorrectly identified by one of its fraud detection or identity theft systems, the IRS may have to send letters and notices to the taxpayer, have IRS employees authenticate a taxpayer's identity at a Taxpayer Assistance Center, or consider taxpayer correspondence. Additionally, when a taxpayer's issue still cannot be resolved, the taxpayer may decide to come to TAS, incurring yet another downstream cost that could be mitigated by reducing FPRs.[50]

High FPRs not only come with a significant monetary cost, but they also have a detrimental impact on employee engagement. For example, research shows that the second problem with high FPRs is how it

46 IRM 21.5.6.4.35.3 (Oct. 1, 2016).

47 Integrity and Verification Operation (IVO) does not correspond with a taxpayer based on a referral from a customer service representative. To the contrary, if it is just a refund status inquiry not associated with any verifiable information, IVO employees will just close out the referral on Account Management Services. IRM 25.25.5.2 (July 15, 2016); IRM 25.25.5.4 (Dec. 10, 2015); IRM 25.25.5.4.1 (May 17, 2016).

48 Financial industry experts see a direct correlation between high FPRs and the increased cost of fraud prevention. "As rates rise, fraud prevention requires more labor and becomes more expensive. Indeed, at very high rates, prevention becomes so costly that — from a purely economic view — it could be cheaper simply to let fraud occur." *See* Gregg S. Henzel *et al.*, *Using Model Calibration and Optimization to Reduce Fraud Risk: How Financial Institutions Can Identify Fraud More Effectively While Reducing Costs* 3-4 (Crowe Horwath 2015), https://www.crowehorwath.com/folio-pdf/Using-Model-Calibration-and-Optimization-to-Reduce-Fraud-Risk-Article-RISK-16007-008A.pdf.

49 *See, e.g.*, Steven Overly, *Artificial Intelligence in Credit Cards Saves You From Faux-Fraud Stupidity*, WASH. POST, A9, Dec. 12, 2016 ("MasterCard estimates that $118 billion in sales were declined due to falsely identified fraud in the United States in 2014 — well more than the $9 billion lost to actual instances of fraud."); SecuredTouch, *Fraud Losses and False Positives: The Numbers* 7 (Dec. 2015), http://securedtouch.com/fraud-losses-and-false-positives-the-numbers. ("For example, sales that were blocked by the credit card companies' fraud detection systems amounted to $118 billion in 2014, while the cost of real card fraud only amounted to $9 billion for the same year.").

50 For FY 2016, TAS received 7,160 cases with TPP issues which had a relief rate of 78.7 percent; 41,819 cases with identity theft issues which had a relief rate of 69 percent; and 29,174 cases with Pre-Refund Wage Verification issues with a relief rate of 80.8 percent. Data obtained from the Taxpayer Advocate Management Information System (TAMIS) (Oct. 1, 2016).

affects the engagement level of those analyzing the company's data for evidence of fraud. Research has shown that when FPRs start to climb above the ratio 25:1, employees know their next alert is unlikely to reveal fraud. Employee incentive to stay engaged lessens and morale erodes. In contrast, when false positives run 5:1, employees know that they are likely to potentially uncover another instance of fraud, thereby encouraging an engaged, focused, and efficient workforce.[51]

In addition to increased costs and eroding employee morale, high FPRs also threaten to negatively impact voluntary compliance. In fact, private sector research shows customers who are subjected to false positives are likely to take their business and go elsewhere. For instance, two-thirds of cardholders who were declined during an e-commerce (electronic) transaction or m-commerce (mobile) transaction reduced or stopped their patronage of the merchant following a false-positive decline, versus 54 percent for all declined cardholders.[52] Unlike customers making a purchase, taxpayers have little choice other than interacting with the IRS. However, taxpayers may be discouraged by the experience of having their returns improperly delayed, increasing the likelihood that they will disengage from their dealings with the IRS in the future. A choice to stop engaging could be met with penalties, but it also means a loss of a compliant taxpayer for the IRS.

CONCLUSION

The National Taxpayer Advocate recognizes the need to detect and prevent refunds resulting from fraud or identity theft from being issued. However, this objective must be accomplished while respecting and protecting the taxpayer's *right to a fair and just tax system,* meaning the IRS is obligated to design and implement systems that impact as few legitimate taxpayers as possible. Currently, the IRS systems and processes are largely out of step with private industry's accepted fraud and identity theft detection, and prevention systems and processes because real time adjustments to IRS systems are bogged down by established processes. This creates high FPRs, which compromises a taxpayer's *right to be informed,* and *to finality,* and also drains IRS resources, erodes employee morale, while damaging voluntary compliance.

RECOMMENDATIONS

The National Taxpayer Advocate recommends that the IRS:

1. Establish aspirational FPR goals and a schedule to meet them.
2. Continue to build, maintain, and improve private-public partnerships to implement techniques to fight fraud.
3. Establish relationships with other government agencies that use data mining and risk detection systems to learn better techniques for lowering false positive rates.
4. Create a real time governance board to adjust filters and include TAS on this board.

51 Gregg S. Henzel *et al.*, *Using Model Calibration and Optimization to Reduce Fraud Risk: How Financial Institutions Can Identify Fraud More Effectively While Reducing Costs* 3-4 (Crowe Horwath 2015), https://www.crowehorwath.com/folio-pdf/Using-Model-Calibration-and-Optimization-to-Reduce-Fraud-Risk-Article-RISK-16007-008A.pdf.

52 Riskified and Javelin, *Overcoming False Positives: Saving the Sale and the Customer Relationship* 4 (Sept. 2015).