TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Actions Were Not Taken to Timely Strengthen Practitioner Priority Service Telephone Line Authentication Controls

October 22, 2024

Report Number: 2025-IE-R001

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: Actions Were Not Taken to Timely Strengthen Practitioner Priority Service Telephone Line Authentication Controls

Final Evaluation Report issued on October 22, 2024 **Report Number 2025-IE-R001**

Why TIGTA Did This Evaluation

This evaluation was initiated because fraudsters have used the Practitioner Priority Service (PPS) telephone line to [redacted]. IRS functional areas and TIGTA's Office of Investigations (OI) brought this fraudulent scheme to IRS management's attention, and the IRS did little to stop this fraud.

Because of this, TIGTA conducted an evaluation to assess the policies and procedures implemented by the IRS to stop fraudsters from exploiting the PPS telephone line by [redacted].

Impact on Tax Administration

The IRS was slow to stop the PPS fraud despite other IRS functional areas identifying this fraud as far back as August 2021. As a result, the IRS did not put an adequate authentication control in place to combat identify theft and protect taxpayers' personal information involving the PPS line until April 8, 2024.

What TIGTA Found

Despite OI issuing a security alert, the IRS's actions were ineffective at stopping a fraud scheme involving fraudsters [redacted]. Because of their limited actions, IRS officials reported that from August 12, 2023, to April 16, 2024, fraudsters were able to [redacted] to fraudulently file 4,828 tax returns and claim nearly $462 million in refunds. Of these fraudulent claims, the IRS was able to detect and stop 4,254 illicit claims; however, the IRS did not stop 574 returns resulting in estimated losses of more than $47 million.

As a result of IRS management's inaction, on February 8, 2024, TIGTA issued an alert to request the IRS's plan to immediately stop the fraud. On April 8, 2024, the IRS implemented additional authentication controls. Specifically, the IRS provided PPS assistors with access to the Secure Access Digital Identity (SADI) dashboard so that [redacted] the assistor would conduct an additional probe to ask the caller to verify the SOR identification number (ID) associated to the mailbox. This additional probe would authenticate that the SOR mailbox belongs to the authorized representative while on the telephone.

Lastly, TIGTA identified 30 out of 376 SOR IDs that were identified by IRS functional groups as fraudulent that the IRS did not restrict access in SADI. The IRS has a manual process in place for restricting access to SOR IDs identified as fraudulent so they cannot be used again.

What TIGTA Recommended

TIGTA recommended that: (1) the IRS provide and train assistors on SADI, (2) establish a Service-wide process where representatives from key functional areas are responsible for expeditiously reviewing and addressing emerging/ongoing fraud schemes where advanced analytics and matching to IRS sourced information proactively identifies a scam, (3) restrict access to all SOR IDs associated with fraudulent activity, and (4) develop processes and procedures to ensure that fraudulent SOR IDs are timely restricted.

IRS management agreed with three of the four recommendations and partially agreed with one recommendation.

TREASURY INSPECTOR GENERAL
for Tax Administration

DATE: October 22, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Russell P. Martin
Deputy Inspector General for Inspections and Evaluations

SUBJECT: Final Report – Actions Were Not Taken to Timely Strengthen Practitioner Priority Service Telephone Line Authentication Controls (Evaluation No.: IE-24-032)

This report presents the results of our evaluation to assess the Internal Revenue Service's actions to address the ongoing fraud scheme involving the Practitioner Priority Service telephone line.

Management's complete response to the draft report is included as Appendix III. If you have any questions, please contact me or Debra Kisler, Director, Inspections and Evaluations.

Table of Contents

Background

Tax practitioners play an important role in our Nation's tax collection system by serving as intermediaries between taxpayers and the Internal Revenue Service (IRS). To perform certain tasks, such as obtaining transcripts, preparing and filing documents, or corresponding and communicating with the IRS regarding tax matter(s), the tax practitioner must have a valid authorization for each taxpayer they represent. Authorizations are generally submitted on Form 2848, *Power of Attorney and Declaration of Representative*, Form 706, *United States Estate (and Generation-Skipping Transfer) Tax Return*, and Form 8821, *Tax Information Authorization.*

Submitted authorizations are worked by IRS employees in the Centralized Authorization File (CAF) unit. Along with reviewing and processing authorizations, the CAF unit is also responsible for assigning tax practitioners a unique nine-digit identifying number the first time a tax practitioner submits an authorization. At the time the CAF number is assigned, the IRS sends the tax practitioner a letter informing them of their assigned CAF number. This CAF number is then to be used by the tax practitioner on all authorizations. The IRS maintains all processed authorization forms in computer database system called the CAF.

The IRS provides tax practitioners with a dedicated Practitioner Priority Service (PSS) telephone line to obtain tax assistance for their clients

Tax practitioners frequently need copies of tax return transcripts for their clients. Tax return transcripts detail sensitive tax data from a taxpayer's filed tax return. One of the primary ways authorized tax practitioners obtain copies of tax return transcripts is by calling the IRS's PPS telephone line. The PPS is a nationwide, toll-free telephone line for tax practitioners to obtain assistance from the IRS with tax account-related issues (including requesting tax return transcripts) for their individual and business clients.

[redacted]. The PPS assistor then validates [redacted]. In addition, the assistor checks the IRS CAF to make sure it is in good standing.

Once the previously mentioned validations are completed, [redacted] which will then be sent to an online Secure Object Repository (SOR) mailbox provided by the caller.[1] The e-Services SOR mailbox is specific to the individual user and may not be accessed by others. Only active registered e-Service's users have access to a SOR mailbox. Tax practitioners can receive up to 30 records per taxpayer for up to five taxpayers per call to the PPS telephone line.

[1] Provides a secure method to send sensitive tax-related information to registered users.

Fraud scheme involving the PPS identified by IRS Cybersecurity Fraud and Analytics (CFAM) group

The IRS has a CFAM group that is dedicated to detecting and preventing identity theft and other tax-related frauds. In May 2023, the CFAM group referred to the Treasury Inspector General for Tax Administration's (TIGTA) Office of Investigations (OI) and IRS Criminal Investigation (CI) an impersonation scheme whereby fraudsters were calling the IRS PPS telephone line and [redacted].

TIGTA's OI issues security alert to IRS Cybersecurity Division

On August 11, 2023, TIGTA's OI issued a security alert to IRS's Director, Cybersecurity Operations. The purpose of this alert was to bring to the IRS's attention the ongoing fraud scheme involving [redacted]. OI's alert noted that from January 2022 through July 2023, OI special agents working with the CFAM group, and the IRS Office of the Research, Applied Analytics, and Statistics (RAAS) identified approximately 112 [redacted] involving at least 22 compromised CAF numbers, with over 6,900 taxpayers [redacted]. The IRS's analysis of the fraudulently filed tax returns related to these taxpayers showed that fraudsters tried to claim approximately $66 million in fraudulent refunds. Deterrence measures were able to prevent nearly 85 percent of the claims from being processed. However, of the $66 million fraudulent refunds, approximately $10 million in refunds were processed and resulted in an actual loss to the Federal Government.

The Security Alert further detailed that the IRS deployed the Tax Professional Online Account (Tax Pro Account) to strengthen security over the process for representatives to access taxpayers' account information. Tax Pro Account is an online system that allows authorized individuals to securely request third-party authorizations for an individual taxpayer, as power of attorney or designee, [redacted]. This service allows the authorized individual, using their CAF number, to initiate authorization requests that route to the taxpayer's IRS Online Account for approval. Using this online method, the authorization will automatically be loaded to the CAF database without tax examiner input or review. OI recommended that the IRS [redacted] promote use of the Tax Pro Account.

We met with the IRS to determine what actions had been taken in response to the OI Security Alert as the CFAM group, RAAS, and OI continued to identify [redacted] fraudulent returns claiming refunds.

Results of Review

Our evaluation identified that the IRS failed to take timely actions to mitigate the fraud scheme outlined in OI's August 2023 Security Alert. Specifically, the IRS failed to [redacted]. As a result, IRS officials reported an additional estimated loss to the Federal Government of more than $47 million. Specifically, from August 12, 2023, to April 16, 2024, the CFAM group, RAAS, and OI [redacted] the fraudsters filed 4,828 tax returns claiming nearly $462 million in refunds. The IRS was able to detect and stop the issuance of a fraudulent refund for 4,254 of these return filings. However, for the remaining 574 tax returns, fraudsters were able to obtain fraudulent refunds totaling more than $47 million.

In addition, our evaluation also identified that fraudsters [redacted]. As of April 16, 2024, RAAS, the CFAM group, and IRS CI identified 376 SOR IDs being used by fraudsters and recommended that steps be taken to restrict access to these repositories. Our verification identified that access for 30 SOR IDs was not restricted.

Activities Related to the Practitioner Priority Service Telephone Lines

On February 8, 2024, we issued an email alert advising IRS management of the continued and ongoing fraud scheme whereby [redacted]. We requested IRS management provide the actions that the Director, Cybersecurity Operations, and/or other IRS operations took to address this ongoing fraud scheme in response to the OI Security Alert.

Although not aware of the specific OI Security Alert that was sent to the Director, Cybersecurity Operations, Accounts Management noted that on September 15, 2023, it issued guidance to advise PPS assistors of the increase of suspicious or potentially fraudulent callers. Assistors were instructed to review internal guidelines on how to report [redacted] activity during their contact with callers. In addition, the assistors were required to check the status of the CAF number to confirm that the tax practitioner was in good standing with the IRS.

During our discussions with IRS management regarding the concerns raised in our February 8, 2024, email alert, we noted that the [redacted]. Management indicated that they would consider adding the additional [redacted].

However, IRS management determined not to add these [redacted] resulting in the continued fraud scheme. In response to our questioning why additional [redacted] IRS management noted that PPS assistors requesting [redacted]

[redacted].

The IRS Management noted that they were working with Privacy, Governmental Liaison, and Disclosure Identity Assurance to [redacted]. This would improve the authentication process by allowing PPS assistors to verify that both the [redacted]. SADI authentication is a higher authentication of the practitioner. According to IRS management, this additional verification will authenticate that the SOR ID belongs to the authorized representative while the representative is on the telephone and [redacted]. However, to finalize its new policies, the IRS had to engage Labor Relations for input and coordinate access and training on the new tool. On April 8, 2024, the SADI dashboard was implemented.

However, because of management inaction to immediately implement the use of [redacted]. For example, fraudsters filed 978 tax returns claiming more than $26 million in refunds from February 9, 2024, to April 16, 2024. Of these fraudulent claims, the IRS was able to detect and stop 931 illicit claims. The remaining 47 fraudulent return filings were not stopped resulting in estimated losses of $480,112 to the Federal Government.

Our Office of Audit will be conducting a review to assess the effectiveness of providing PPS assistors with SADI access to prevent fraudsters [redacted] to gain access to sensitive tax return information and file fraudulent tax returns.

The Deputy Commissioner should:

Recommendation 1: Ensure that PPS assistors have access and are trained on how to use the SADI dashboard.

> **Management's Response:** IRS management agreed with the recommendation. As of April 8, 2024, the IRS has trained all PPS employees on how to use the SADI dashboard.

Recommendation 2: Establish a Service-wide process where representatives from key functional areas including CFAM, RAAS and Accounts Management officials are responsible for expeditiously reviewing and addressing emerging/ongoing fraud schemes where advanced analytics and matching to IRS sourced information proactively identifies a scam.

> **Management's Response:** IRS management agreed with the recommendation. IRS functional areas across the Taxpayer Services Division, Information Technology organization, RAAS organization, and the Privacy, Governmental Liaison, and Disclosure organization contribute specific actions to the current process. The RAAS director will work with these stakeholders, and potentially others to further develop and document the processes and improve communications among the stakeholders.

Some Fraudulent Secure Object Repository Numbers Were Not Restricted

When the IRS identifies [redacted].

The process to restrict access to the SOR ID is manual and once the CFAM group or RAAS identifies a fraudulent SOR ID they send to another IRS functional group notifying them of the SOR ID to be restricted. These groups then take the necessary steps in SADI to restrict access to the fraudster's SOR mailbox, [redacted].

As of April 16, 2024, a total of 376 SOR IDs were requested to be restricted.[2] Our review of IRS records found that 30 (8 percent) of the total 376 SOR IDs were not restricted. We notified the Deputy Director, Accounts Management, of our concern that 25 identified fraudster SOR IDs still were not restricted.[3] IRS officials agreed to restrict access to eight SOR IDs; however, for the remaining 17, the IRS reviewed the accounts and determined they were all identified as having fraudulent use in eAuth (the system used prior to SADI). IRS management decided that eAuth restrictions would not be automatically restricted in SADI but will be restricted if there is new evidence of fraud. We believe management's position to not automatically restrict access to SOR ID previously restricted under eAuth disregards the fact that these SOR IDs were identified and confirmed as being used by fraudsters. As such, we believe the 17 accounts previously restricted in eAuth should also be restricted in SADI.

The Deputy Commissioner should:

Recommendation 3: Ensure that all SOR IDs identified as being used by fraudsters are timely restricted in SADI.

> **Management's Response:** IRS management partially agreed with the recommendation. The Director, Identity and Access Management, Information Technology will work with stakeholders to ensure that the applicable SOR IDs identified as being used by fraudsters are restricted in SADI. For accounts identified as targeted by fraudsters via the former IRS system pre-dating SADI, the IRS found no current fraudulent activities with these accounts in the new more rigorous SADI system. Accordingly, we do not think restricting access is appropriate for these accounts but will continue to monitor for suspicious activities moving forward.
>
> > **Office of Inspections and Evaluations Comment:** We believe management's position to not automatically restrict access to SOR IDs previously restricted under eAuth disregards the fact that these SOR IDs were identified and confirmed as being used by fraudsters. As such, we believe the 17 accounts previously restricted in eAuth should also be restricted in SADI.

Recommendation 4: Develop processes and procedures to ensure that identified fraudulent SOR IDs are timely restricted.

[2] According to the IRS, this fraud goes back as far as August 2021.

[3] At our request, the IRS shut off five of the 30 SORs prior to TIGTA issuing the email alert.

Management's Response: IRS management agreed with the recommendation. Several IRS functional areas across the IRS contribute specific actions to the current process. The Director, Identity and Access Management, Information Technology will work with stakeholders, and potentially others to further develop and document the processes and improve communications among stakeholders.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the actions taken by the IRS to address the ongoing fraud scheme involving the [redacted] telephone line. To accomplish our objective, we:

- Inquired into allegations of waste, fraud, and abuse involving the PPS telephone line.
- Interviewed IRS management to determine the actions taken since TIGTA's OI issued its security alert.
- Determined whether corrective actions were sufficient to prevent the fraud scheme from continuing.
- Obtained CAF numbers, SOR IDs, and TINs that RAAS and CFAM teams identified as being affected by this scheme.
- Coordinated with TIGTA's OI on its efforts to investigate the scheme.

Performance of This Review

This review was performed with information obtained from the IRS Accounts Management, RAAS, and the CFAM group located in Atlanta, Georgia and Carmel, Indiana, during the period February 2024 through July 2024. We conducted this evaluation in accordance with the Council of the Inspectors General for Integrity and Efficiency Quality Standards for Inspection and Evaluation. Those standards require that the work adheres to the professional standards of independence, due professional care, and quality assurance and followed procedures to ensure accuracy of the information presented. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions.

Major contributors to the report were Debra Kisler, Director; Jeff Stieritz, Supervisory Evaluator; and Michael Bibler, Lead Evaluator.

Appendix II

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Funds Put To Better Use – Actual; $47,698,849 in fraudulent refunds paid for 574 tax returns that the IRS did not stop from August 12, 2023, to April 16, 2024 (see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

IRS officials reported that from August 12, 2023, to April 16, 2024, [redacted] 4,828 tax returns and claim nearly $462 million in refunds. Of these fraudulent claims, the IRS was able to detect and stop 4,254 illicit claims; however, the IRS did not stop 574 returns resulting in estimated losses of more than $47 million.[1]

[1] The IRS directly provided us this information; however, we did not validate the numbers.

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

CHIEF
TAXPAYER SERVICES

September 26, 2024

MEMORANDUM FOR RUSSELL P. MARTIN
DEPUTY INSPECTOR GENERAL FOR INSPECTIONS AND EVALUATIONS

FROM: Kenneth C. Corbin /s/ Kenneth C. Corbin
Chief, Taxpayer Services Division

SUBJECT: Draft Evaluation Report – Actions Were Not Taken to Timely Strengthen Practitioner Priority Service Telephone Line Authentication Controls (Evaluation No.: IE-24-032)

Thank you for the opportunity to review and provide comments on the subject draft report. Authorized tax practitioners call the toll-free Practitioner Priority Services (PPS) for assistance with tax matters for their clients, including obtaining account transcripts. In conjunction with the Treasury Inspector General for Tax Administration's Office of Investigations, we identified an [redacted].

The protection of taxpayer information and prevention of fraudulent refunds are top priorities for the IRS. To address this scheme, several IRS functional offices joined forces to share data and expertise and determined that higher levels of authentication for [redacted]. This team is continually working to evaluate suspicious activity with the objective of predicting and preventing future fraudulent schemes. The ever-evolving nature of fraudulent schemes calls for extreme vigilance and we evaluate and implement processes intended to combat and thwart those schemes. Our Customer Service Representatives answering the PPS lines document key data elements in the call record notes that is used in ongoing fraud analytics.

We expanded monitoring of the Secure Object Repository (SOR) to include SOR IDs and Secure Access Digital Identity (SADI) accounts associated with tax professionals. On a daily basis, the PPS phone recordings and return filings from all SOR mailboxes that exhibit a spike in transcript activity, exhibit a spike in suspect return filings, and

contain Taxpayer Identification Numbers associated with other compromised accounts are reviewed.

Additionally, we review all referrals from Cybersecurity Fraud Analytics and Monitoring (CFAM) and either confirm the presence of a scheme or mark the SOR ID as requiring continued monitoring. Between May 30 and August 2, 2024, monitoring has resulted in the identification of 63 [redacted]. We blocked incoming phone numbers associated with the SOR scheme from contacting IRS call centers. Further analysis is being done to determine whether this is an effective strategy.

As mentioned in the report, we updated procedures so that PPS employees, using SADI information, [redacted] and were the true SOR mailbox owners. Although this eliminated most fraudulent attempts, we recognized that additional safeguards were needed since some SOR mailboxes were owned by bad actors rather than by an authorized representative. For those compromised accounts, we monitored to prevent refunds associated with them from being issued.

Fraudsters continue to attempt to access our systems and information, making identity theft and fraud a constant challenge. We recognize the need for additional improvements, and we will remain proactive in addressing evolving schemes. We disagree; however, that 17 accounts authenticated via the former e-Authentication process still need to be disabled. Our cybersecurity function reviewed the accounts and found no fraudulent activity. Any further interactions with IRS from those accounts would require the more rigorous ID.me authentication process.

Our responses to your specific recommendations are enclosed. If you have any questions, please contact me, or a member of your staff may contact Joseph Dianto, Director, Customer Account Services, at 470-639-3504.

Attachment

Attachment

Recommendations

The Deputy Commissioner should:

RECOMMENDATION 1
Ensure that PPS assistors have access and are trained on how to use the SADI dashboard.

CORRECTIVE ACTION
We agree. As of April 8, 2024, we have trained all Practitioner Priority Services employees on how to use Secure Access Digital Identity (SADI) dashboard.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Accounts Management, Customer Account Services, Taxpayer Services Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 2
Establish a Service-wide process where representatives from key functional areas including CFAM, RAAS and Accounts Management officials are responsible for expeditiously reviewing and addressing emerging/ongoing fraud schemes where advanced analytics and matching to IRS sourced information proactively identifies a scam.

CORRECTIVE ACTION
We agree. IRS functional areas across the Taxpayer Services Division, Information Technology organization, Research, Applied Analytics and Statistics organization, and the Privacy, Governmental Liaison, and Disclosure organization contribute specific actions to the current process. We will work with these stakeholders, and potentially others to further develop and document the processes and improve communications among the stakeholders.

IMPLEMENTATION DATE
December 15, 2025

RESPONSIBLE OFFICIAL
Director, Research, Applied Analytics and Statistics

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 3
Ensure that all SOR IDs identified as being used by fraudsters are timely restricted in SADI.

CORRECTIVE ACTION
We partially agree. We will work with stakeholders to ensure the applicable Secure Object Repository IDs identified as being used by fraudsters are restricted in SADI. For accounts identified as targeted by fraudsters via the former IRS system pre-dating SADI, we found no current fraudulent activities with these accounts in the new more rigorous SADI system. Accordingly, we do not think restricting access is appropriate for these accounts but will continue to monitor for suspicious activities moving forward.

IMPLEMENTATION DATE
February 15, 2025

RESPONSIBLE OFFICIAL
Director, Identity and Access Management, Information Technology

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 4
Develop processes and procedures to ensure that identified fraudulent SOR IDs are timely restricted.

CORRECTIVE ACTION
We agree. Several IRS functional areas across IRS contribute specific actions to the current process. We will work with these stakeholders, and potentially others to further develop and document the processes and improve communications among the stakeholders.

IMPLEMENTATION DATE
March 15, 2025

RESPONSIBLE OFFICIAL
Director, Identity and Access Management, Information Technology

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

Appendix IV

Abbreviations

CAF	Centralized Authorization File
CFAM	Cybersecurity Fraud and Analytics
CI	Criminal Investigation
ID	Identification Number
IRS	Internal Revenue Service
OI	Office of Investigations
PPS	Practitioner Priority Service
RAAS	Research, Applied Analytics and Statistics
SADI	Secure Access Digital Identity
SOR	Secure Object Repository
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number

To report fraud, waste, or abuse,
contact our hotline on the web at
https://www.tigta.gov/reportcrime-misconduct.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

Information you provide is confidential, and you may remain anonymous.