

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Authenticating Callers' Identity on Business and Practitioner Telephone Lines Needs to Be Strengthened to Combat Fraud

August 12, 2025

Report Number: 2025-IE-R025

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

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

HIGHLIGHTS: Authenticating Callers' Identity on Business and Practitioner Telephone Lines Needs to Be Strengthened to Combat Fraud

Final Evaluation Report issued on August 12, 2025

Report Number 2025-IE-R025

Why TIGTA Did This Evaluation

We initiated this evaluation in response to a referral that TIGTA's Office of Investigations made involving a scheme related to the filing of fraudulent Forms 941, *Employer's Quarterly Federal Tax Return*.

Specifically, fraudsters contact the IRS, [REDACTED]

Fraudsters then file a fraudulent Form 941 to obtain a refund check.

For this evaluation, we assessed policies and procedures that the IRS has implemented to stop fraudsters from [REDACTED]

to file fraudulent Forms 941 claiming a tax refund.

Impact on Tax Administration

If the IRS does not properly authenticate individuals before providing tax account information, there is a continued risk of unscrupulous individuals taking advantage of the tax system. The federal government is also at risk of losing funds.

What TIGTA Found

The IRS does not always properly authenticate a caller's identity to adequately protect against the release of tax information and safeguard government funds. We found that the IRS did not adequately verify the identity of callers to the Business Specialty Tax and the Practitioner Priority Service telephone lines. This allowed the unauthorized disclosure of tax information, the fraudulent filing of Forms 941, and the issuance of fraudulent tax refund checks.

Based on the information provided in the referral, we issued an alert in October 2024. Our alert advised IRS management about a scheme involving the fraudulent filing of Forms 941. The alert noted that the Office of Investigations identified over \$93 million in fraudulent refund checks issued to 20 different businesses. The Office of Investigations successfully stopped payment on most of these refund checks. However, the federal government incurred at least \$2.7 million in losses.

We used information in the referral to perform further analysis. We identified 150 unique Employer Identification Numbers that were issued approximately \$55.6 million in refund checks from January 2023 through July 2024.

IRS management was aware of the risk of erroneous refunds being issued based on fraudulent Form 941 filings, but did not take action to prevent the scheme. IRS representatives in the Customer Account Services function raised the issue in June 2024 and August 2024.

We found that the IRS has guidance in place to ensure that IRS representatives are aware of possible fraudulent activity on a tax account, including a tool that alerts them when identity theft is suspected or documented. If identity theft is an issue on the tax account, IRS representatives are required to conduct additional research, including reviewing history notes on the account.

Our review of the history notes showed that IRS representatives had documented fraudsters' initial requests for tax information. If subsequent IRS representatives had reviewed those notes, they may not have provided the information needed to further the fraud scheme.

What TIGTA Recommended

In our alert, we recommended that the Chief, Taxpayer Services, educate representatives about the fraud scheme and require them to properly authenticate callers before providing tax account information, including tax deposit and tax transcript information.

IRS management agreed with our recommendation and took appropriate corrective action.



TREASURY INSPECTOR GENERAL

for Tax Administration

DATE: August 12, 2025

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Nancy A. LaManna 
Deputy Inspector General for Inspections and Evaluations

SUBJECT: Final Evaluation Report – Authenticating Callers' Identity on Business and Practitioner Telephone Lines Needs to Be Strengthened to Combat Fraud (Evaluation No.: IE-24-051)

This report presents the results of our review to assess actions taken by the Internal Revenue Service to address schemes involving the fraudulent filing of Form 941, *Employer's Quarterly Federal Tax Return*. This review is part of our Fiscal Year 2025 Annual Program Plan and addresses the major management and performance challenge of *Tax Fraud and Improper Payments*.

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

Table of Contents

<u>Background</u>	Page 1
<u>Results of Review</u>	Page 2
<u>Employees Did Not Follow Existing Authentication Procedures, Which Allowed Individuals to File Fraudulent Forms 941 and Obtain Tax Refund Checks</u>	Page 2
<u>Recommendation 1:</u>	Page 4
 Appendices	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 5
<u>Appendix II – Outcome Measure</u>	Page 6
<u>Appendix III – Management’s Response to the Draft Report</u>	Page 7
<u>Appendix IV – Abbreviations</u>	Page 9

Background

Employers use Form 941, *Employer's Quarterly Federal Tax Return*, to report wages and tips their employees have earned. Form 941 is also used to report employment taxes, including federal income, Social Security, and Medicare taxes withheld from employees. In addition, the form is used to report employer's contribution of Social Security and Medicare taxes. Businesses generally are required to file a Form 941 each quarter.

If a business has tax or refund-related questions, they can contact the Internal Revenue Service's (IRS) Business Specialty Tax or the Practitioner Priority Service telephone lines. The Business Specialty Tax telephone line provides service to businesses, corporations, partnerships, and trusts that need information or assistance with business tax returns or tax accounts. The Practitioner Priority Service telephone line is the first point of contact for tax practitioners who need assistance regarding their client's tax accounts.

IRS internal guidance indicates that when an individual calls the IRS, they will be asked questions to verify the individual's identity prior to discussing or making any changes to a tax account. Return information should not be disclosed until an IRS representative has confirmed that an individual making an inquiry is the taxpayer, the taxpayer's authorized representative, or an authorized representative of the business. When an individual requests changes via the telephone, IRS representatives can only make changes for editorial errors involving spelling, incomplete names, and missing or incorrect suffixes. Non-editorial changes, such as an address change, can be made after the IRS representative verifies the previous address with the caller.

We initiated this evaluation after we received a referral from TIGTA's Office of Investigations (OI) about a scheme related to the filing of fraudulent Forms 941. Specifically, OI identified fraudsters

[REDACTED]

Some fraudsters also [REDACTED]
[REDACTED]. Federal regulations require the IRS to send two notices when an address change is requested. One notice is sent to the current address on file and the other to the new address.¹ Fraudsters—aware of the notification requirements—[REDACTED]

[REDACTED]

An IRS representative releases the refund, and the check is sent to the new address.

¹ The IRS sends [REDACTED] notices to [REDACTED]. The [REDACTED] notice is mailed to the taxpayer's new address. The [REDACTED] notice is mailed to the taxpayer's prior address.

Results of Review

We found that the IRS does not always properly authenticate a caller's identity to adequately protect against the release of tax information or safeguard government funds. The IRS did not adequately verify the identity of callers to the Business Specialty Tax and the Practitioner Priority Service telephone lines. This allowed the unauthorized disclosure of tax information, the fraudulent filing of Forms 941, and the issuance of fraudulent tax refund checks.

Based on information that OI shared in its referral, we identified approximately \$56 million in possible fraudulent refund checks issued from January 2023 through July 2024. The checks were associated with 150 Employer Identification Numbers.

Employees Did Not Follow Existing Authentication Procedures, Which Allowed Individuals to File Fraudulent Forms 941 and Obtain Tax Refund Checks

In October 2024, we used information obtained from the OI referral to issue an alert advising IRS management about a scheme involving the fraudulent filing of Forms 941. The alert noted that OI identified over \$93 million in fraudulent refund checks issued for 20 different businesses. While OI worked with the Bureau of Fiscal Services to stop payment on most of these refund checks, at least \$2.7 million was paid.

IRS management responded to the alert and indicated they were aware of the risk of erroneous refunds being issued based on fraudulent Form 941 filings. In June 2024, the Customer Account Services function referred a case to the Identity Theft Victim Assistance function. The case involved a business experiencing issues with [REDACTED], as well as the fraudulent filing of a Form 941. The Business Master File Identity Theft unit reviewed the case, but the issue was not elevated until August 2024. By then, the Customer Account Services function had referred two additional cases. All three cases had the same individuals involved in the [REDACTED], but the IRS did not take action to prevent the continuation of the scheme.

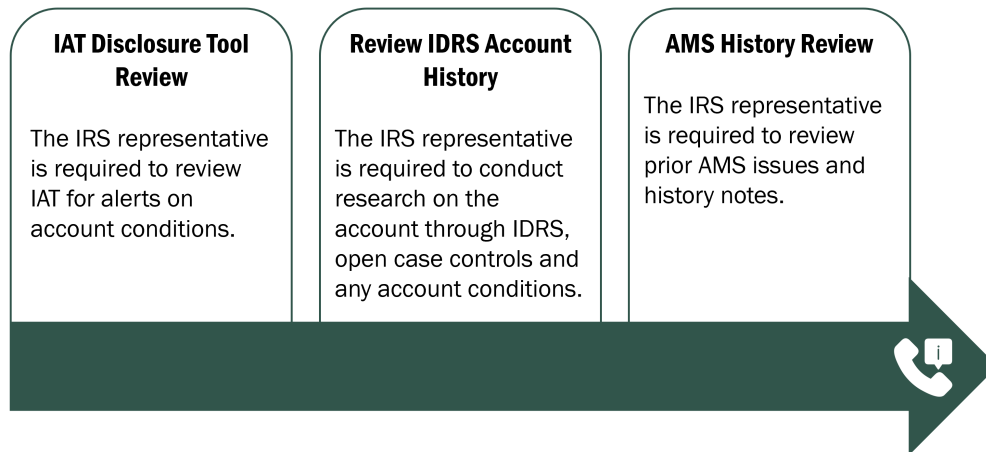
To determine the extent of the scheme, we analyzed all Forms 941 filed from January 2023 through August 2024 that had [REDACTED]. [REDACTED] is an indicator of possible fraud. In addition, we used common names identified in the fraud scheme to determine whether there were other instances where individuals had requested a [REDACTED]. We then compared our results to tax accounts that had refund checks issued from January 2023 through July 2024. We identified 150 unique Employer Identification Numbers that were issued approximately \$56 million in refund checks.

We found that fraudsters repeatedly called the IRS to [REDACTED].

As previously mentioned, the IRS has a process to authenticate and properly identify individuals calling its telephone lines. The IRS also has procedures to inform representatives about possible fraudulent activity on a tax account. The procedures state that prior to releasing any tax account information over the telephone, IRS representatives are required to review the Integrated Automation Technology (IAT) Disclosure tool. This tool alerts IRS representatives to certain tax account conditions when identity theft is suspected or documented.

If the IAT Disclosure tool indicates identity theft is an issue on the tax account, IRS representatives are required to conduct additional research. This includes reviewing the Integrated Data Retrieval System (IDRS) account history and conducting an Accounts Management System (AMS) history review.² Figure 1 outlines the steps IRS representatives are required to take prior to releasing tax information over the telephone.

Figure 1: Requirements for Releasing Tax Information Over the Telephone



Source: IRS internal guidance.

However, the IRS does not always follow this process. For example, IRS representatives are not always reviewing call history notes documented on the tax account before providing tax account information to a caller. We reviewed the call history notes of tax accounts affected by the scheme and found that IRS representatives had documented fraudsters' initial requests for tax account information. If subsequent IRS representatives had reviewed the call history notes, they may not have provided the information needed to further the fraud scheme.

In October 2024, we reported another impersonation scheme that involved fraudsters calling the Practitioner Priority Service telephone line.³ The report noted that fraudsters

[REDACTED]

² The IDRS is an IRS computer system capable of retrieving or updating stored information. The IDRS works in conjunction with taxpayer account records. The AMS allows employees to access multiple IRS systems, including inventory management, case delivery, history narratives, and print-to-fax capabilities to send information to taxpayers.

³ TIGTA, Report No. 2025-IE-R001, [Actions Were Not Taken to Timely Strengthen Practitioner Priority Service Telephone Line Authentication Controls](#) (October 2024).

[REDACTED]

As a result of our review, IRS management implemented additional authentication controls. IRS representatives answering calls on the Practitioner Priority Service telephone line received access to the Secure Access Digital Identity dashboard. This dashboard provides IRS representatives access to an additional tool to verify the identity of an authorized representative while the person is on the telephone. This occurs before any tax return transcripts are released.

The IRS must perform proper authentication. This includes individuals calling to obtain tax return transcripts or other key tax information, such as the dates and amounts of federal tax deposit payments. If the IRS does not properly authenticate individuals before providing tax account information, there is a continued risk of unscrupulous individuals taking advantage of the tax system. The federal government is also at risk of losing funds.

Recommendation 1 (Alert): The Chief, Taxpayer Services, should educate IRS representatives about the fraud scheme and require them to properly authenticate callers before providing tax account information, including tax deposit and tax transcript information.

Management's Response: IRS management agreed with our recommendation. As of April 17, 2025, the IRS provided employees with a training course on Business Master File Authentication and Disclosure as a mandatory topic for the Fiscal Year 2025 Critical Filing Season Readiness Training. IRS management also issued a Service-wide Electronic Research Program Alert to remind employees of disclosure guidelines and procedures for address changes.

Recent executive order to digitize all federal disbursements and payments will likely help prevent similar fraud schemes

In October 2024, we issued an alert to the IRS. We recommended that the IRS delay issuing refund checks from the filing of a Form 941, when the filing or prior contact with the IRS resulted in an address change. At the time, IRS management agreed with our recommendation and planned to request a programming change to delay the refund checks. However, Executive Order 14247, *Modernizing Payments To and From America's Bank Accounts*, was issued in March 2025 to phase out paper checks.

The executive order states that effective September 30, 2025, the Secretary of the Treasury will stop issuing paper checks for all federal disbursements, including tax refunds. There will be limited exceptions where electronic payment and collection methods are not feasible. We believe that the executive order will likely help resolve this particular fraud scheme and make our previous recommendation to the IRS obsolete. However, strengthening the authentication process is still needed to further eliminate the fraudulent issuance of tax refunds.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess actions taken by the IRS to address schemes involving the fraudulent filing of Form 941. To accomplish our objective, we:

- Obtained and analyzed information from TIGTA's OI about fraudulent Forms 941 filings.
- Interviewed IRS management and determined whether the agency took any actions after we issued our October 2024 alert.
- Determined whether proposed corrective actions were sufficient to prevent the fraud scheme.
- Performed an analysis of Form 941 refund data and identified additional cases involving fraudulent filings of the form.

Performance of This Review

This review was performed with information obtained from the IRS's Accounts Management and Submission Processing functions; the Office of Research, Applied Analytics, and Statistics; and the Office of Cybersecurity Fraud Analytics and Monitoring during the period of September 2024 through January 2025.

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Federal Offices of Inspector General*. Those standards require that the work adheres to the professional standards of independence, due professional care, 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.

Data Validation Methodology

We evaluated the data by performing tests to assess the reliability of data obtained from the IRS's Individual Master File system. Specifically, we evaluated the data by performing electronic testing of required data elements. We determined that the data were sufficiently reliable for purpose of this report.

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 (Revenue Protection – Potential; \$55,889,446 in erroneous refund checks were issued to individuals involved in the Form 941 fraudulent scheme (see Recommendation 1).

Methodology Used to Measure the Reported Benefit:

We identified 34,908 Forms 941 filed from January 1, 2023, through August 15, 2024, that requested a refund to be paid and had a transaction code [REDACTED] posted to the business tax account, [REDACTED]. We further analyzed the Forms 941 and determined that 232 of them had [REDACTED]. In addition, notes in the AMS contained key words that indicated possible fraud. We compared these cases to refund checks issued from January 1, 2023, through July 31, 2024. We identified 150 unique Employer Identification Numbers that were potentially issued \$55,889,446 in fraudulent refund checks.

Appendix III

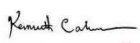
Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

July 3, 2025

MEMORANDUM FOR NANCY A. LAMANNA
DEPUTY INSPECTOR GENERAL FOR INSPECTIONS AND
EVALUATIONS

FROM: Kenneth C. Corbin 
Chief, Taxpayer Services Division

Digitally signed by
Kenneth C. Corbin
Date: 2025.07.03
12:03:02 -04'00'

SUBJECT: Draft Evaluation Report – Authenticating Callers' Identity on
Business and Practitioner Telephone Lines Need to Be
Strengthened to Combat Fraud
(Evaluation No.: IE-24-051)

Thank you for the opportunity to review and provide comments on the subject draft report. The protection of taxpayer information and prevention of fraudulent refunds are top priorities for the IRS. We regularly review our electronic filing systems and recognize the critical need for accuracy and efficiency during form processing and record retrieval, while maintaining database integrity.

We are placing a greater emphasis on the requirements of IRC 6103 to help strengthen supporting guidance and to give telephone assistors the support they need to combat fraud. To reduce the risk of inadvertent disclosure, we modified training plans to reinforce existing caller authentication procedures. These efforts reflect our ongoing commitment to protecting taxpayer information and ensuring consistent application of established protocols.

We agree that disbursing payments electronically will lower the risks associated with paper checks. As an additional mitigation, we are evaluating program changes to delay the issuance of refunds from Form 941 *Employer's Quarterly Federal Tax Return*, for business filers with address and/or name changes.

Our response to the recommendation is enclosed. If you have any questions, please contact me, or a member of your staff may contact Customer Account Services Director, Joseph Dianto, at 470-639-3504.

Attachment

**Authenticating Callers' Identity on Business and Practitioner
Telephone Lines Needs to Be Strengthened to Combat Fraud**

Attachment

Recommendation

RECOMMENDATION 1 (Alert)

Educate IRS representatives about the fraud scheme and require them to properly authenticate callers before providing tax account information, including tax deposit and tax transcript information.

CORRECTIVE ACTION

We agree. As of April 17, 2025, we provided employees with a training course on Business Master File Authentication and Disclosure as a mandatory topic for the Fiscal Year 2025 Critical Filing Season Readiness Training (CFSRT). The training course will remain available for future CFSRTs. We also issued a Servicewide Electronic Research Program (SERP) Alert 24A0237 to remind employees of disclosure guidelines and procedures for address changes.

IMPLEMENTATION DATE

Implemented

RESPONSIBLE OFFICIAL

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

CORRECTIVE ACTION MONITORING PLAN

N/A

Appendix IV

Abbreviations

AMS	Accounts Management System
IAT	Integrated Automation Technology
IDRS	Integrated Data Retrieval System
IRS	Internal Revenue Service
OI	Office of Investigations
TIGTA	Treasury Inspector General for Tax Administration



**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.