

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Thousands of Notifications to Taxpayers Affected by the Large-Scale Data Breach Were Returned Undeliverable

May 27, 2025

Report Number: 2025-IE-R019

HIGHLIGHTS: Thousands of Notifications to Taxpayers Affected by the Large-Scale Data Breach Were Returned Undeliverable

Final Evaluation Report issued on May 27, 2025

Report Number: 2025-IE-R019

Why TIGTA Did This Evaluation

In 2023, TIGTA's Office of Investigations reported that Charles Littlejohn, an IRS contractor, accessed and stole tax returns and return information of a high-ranking government official and thousands of the nation's wealthiest taxpayers between August 2019 and August 2020. In January 2024, Littlejohn was sentenced to five years in prison for disclosing thousands of tax returns and return information without authorization.

As a result of this data breach, the IRS sent notification letters to individuals and businesses that were affected by the data breach. These letters provided taxpayers with information on the data breach, the risk of identity theft, and actions available to taxpayers.

The overall objective of this evaluation was to assess the IRS's processes and procedures to notify individual and business taxpayers affected by a large-scale data breach.

Impact on Tax Administration

Internal Revenue Code (I.R.C.) § 6103 requires safeguarding the confidentiality of tax returns and return information. Disclosing information to third parties is only permitted when authorized by a specific exception within the statute or when it becomes public record during a tax administration proceeding. The IRS has a legal responsibility to notify all taxpayers affected by this large-scale data breach.

What TIGTA Found

From January through May 2024, TIGTA's Office of Investigations identified and shared information with the IRS on 8,418 individual and 70,343 business taxpayers affected by this large-scale data breach.

The IRS informed us that thousands of taxpayers did not receive the initial letters that the IRS mailed to notify individuals and businesses affected by the large-scale data breach. The IRS did not initially know the total number of undeliverable mailings (*e.g.*, returned letters due to incomplete addresses) related to the data breach and which affected taxpayers did not receive the notification letter.

In July 2024, we recommended that the IRS take immediate action to develop a solution to sort the undeliverable mail and determine how many of the mailings were related to the data breach. The IRS ultimately determined that it had approximately 12,200 undeliverable mailings related to the data breach, which were returned to the IRS from the U.S. Postal Service. The IRS also developed a plan to identify the correct mailing address for the business and individual taxpayers with notifications returned as undeliverable.

Additionally, we found that the IRS placed data breach indicators on most of the tax accounts of affected taxpayers. However, we identified 1,334 affected individual taxpayer accounts with no indicators. The IRS may not need to place indicators on taxpayer accounts in certain instances, such as taxpayers who are deceased or taxpayers with no active accounts. Based on our recommendation, the IRS reviewed the 1,334 accounts and stated it will add the data breach indicator and mail out notifications to 20 accounts for individuals who were incorrectly classified as deceased.

In August 2024, the U.S. Department of the Treasury (Treasury) sent a letter to the Chair and Ranking Member of the Senate Finance Committee to report the data breach as a major incident since personally identifiable information for more than 100,000 taxpayers was exfiltrated. As of November 2024, the IRS determined that the data breach affected approximately 406,000 taxpayers.

What TIGTA Recommended

We recommended that the Chief Privacy Officer review the 1,334 affected individual taxpayer accounts, and, if warranted, take appropriate actions to place the data breach indicator on tax accounts and mail notification letters to additional taxpayers affected by the data breach. We also recommended that the Chief Privacy Officer continue working to identify all individual and business taxpayers impacted by the large-scale data breach.

IRS management agreed with our recommendations.



TREASURY INSPECTOR GENERAL

for Tax Administration

DATE: May 27, 2025

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM:

Nancy LaManna

A handwritten signature in cursive script that reads "Nancy LaManna".

Deputy Inspector General for Inspections and Evaluations

SUBJECT:

Final Evaluation Report – Thousands of Notifications to Taxpayers
Affected by the Large-Scale Data Breach Were Returned Undeliverable
(Evaluation No.: IE-24-041)

This report presents the results of our evaluation to assess the Internal Revenue Service's processes and procedures to notify individual and business taxpayers affected by a large-scale data breach. This evaluation is part of our Fiscal Year 2025 Annual Program Plan and addresses the major management and performance challenge of *Protection of Taxpayer Data and IRS Resources*.

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>The IRS Did Not Have a Process to Identify and Resend Undelivered Mailings to Thousands of Affected Taxpayers</u>	Page 2
--	--------

<u>The IRS Placed Data Breach Indicators on Most of the Affected Taxpayer Accounts</u>	Page 4
--	--------

<u>Recommendation 1:</u>	Page 6
--------------------------------	--------

<u>The IRS Continues to Identify Taxpayers Affected by the Large-Scale Data Breach</u>	Page 6
--	--------

<u>Recommendation 2:</u>	Page 6
--------------------------------	--------

Appendices

<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 7
--	--------

<u>Appendix II – Sample Notification Letters Mailed to Taxpayers Affected by the Large-Scale Data Breach</u>	Page 8
--	--------

<u>Appendix III – Management’s Response to the Draft Report</u>	Page 13
---	---------

<u>Appendix IV – Abbreviations</u>	Page 15
--	---------

Background

In June 2021, an independent newsroom began publishing a series of news articles from information it described as a vast trove of Internal Revenue Service (IRS) tax data on thousands of the wealthiest people in the United States. The tax data covered more than 15 years. The newsroom claimed the information came from an anonymous source. Some of the tax data cited included information on income, taxes, profits from stock trades, and the results of audits.

TIGTA's Office of Investigations (OI) has law enforcement responsibility and investigated the data breach. In 2023, TIGTA's OI reported that Charles Littlejohn, an IRS contractor, accessed and stole tax returns and return information of a high-ranking government official and related entities and individuals. Between August and October 2019, Littlejohn disclosed the official's tax return information to the news organization. TIGTA's OI also reported that in Spring 2020, Littlejohn stole additional tax return information associated with the official and provided it to the news organization. Further, TIGTA's OI reported that in July and August 2020, Littlejohn separately stole tax returns and return information associated with thousands of the nation's wealthiest individuals. In November 2020, Littlejohn disclosed this tax return information to a second news organization.

In September 2023, the Department of Justice charged Littlejohn with disclosing tax return information without authorization to two news organizations. In January 2024, Littlejohn was sentenced to five years in prison for disclosing thousands of tax returns without authorization.

As a result of this data breach, the IRS's Privacy, Governmental Liaison and Disclosure (PGLD) office sent notification letters to the individuals and businesses affected by the data breach in accordance with I.R.C. § 7431.¹ These letters informed individuals and businesses that an IRS contractor was charged with the unauthorized inspection or disclosure of the taxpayers' return or return information between Calendar Years 2018 and 2020. Taxpayers were also provided information on the risks of identity theft, a link to more information about the data breach, and how to protect themselves.

The IRS gave these taxpayers the opportunity to request additional information, which the IRS provided in a supplemental letter that described the agency's efforts to address the breach incident. The letter also stated that the IRS has not seen any indication that the taxpayer's information was used for identity theft or any related fraud. Further, the letter stated that the IRS continues to contact additional impacted taxpayers identified as having their information disclosed and provide these taxpayers with information about how to contact the IRS.

The IRS developed a data breach indicator to mark on the Master File of all individual and business taxpayers affected by this unauthorized disclosure.²

¹ In 26 U.S.C. § 7431, as amended by the Taxpayer Browsing Protection Act of 1997, it states that any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of 26 U.S.C. § 6103, such a taxpayer may bring a civil action for damages against the United States in a district court of the United States. See Appendix II for a sample of Letters 6613, 6613-A and the supplemental letter sent to affected taxpayers.

² The Master File is the IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.

Results of Review

From January through May 2024, TIGTA's OI identified and shared information with the IRS on 8,418 individual and 70,343 business taxpayers affected by the large-scale data breach. The IRS informed us that thousands of affected taxpayers did not receive the initial letters the agency mailed to notify individuals and businesses impacted by the data breach. We also identified some affected taxpayer accounts did not have the data breach indicator. We found that:

- The IRS did not initially know the total number of undeliverable mailings (*e.g.*, returned letters due to incomplete addresses) related to the data breach and which affected taxpayers did not receive the notification letters. The IRS ultimately determined that approximately 12,200 notification letters were undeliverable.
- The IRS did not place the data breach indicator on some affected taxpayer accounts that TIGTA's OI identified. For instance, we identified 1,334 affected individual taxpayer accounts with no indicators. The IRS may not need to place indicators on taxpayer accounts in certain instances, such as taxpayers who are deceased or taxpayers with no active accounts. Based on our recommendation, the IRS reviewed the 1,334 accounts and stated it will add the data breach indicator and mail out notifications to 20 accounts for individuals who were incorrectly classified as deceased.

In June 2024, TIGTA's OI provided the IRS with additional criteria that could be considered when identifying taxpayers affected by the data breach. As of November 2024, the IRS determined there were approximately 406,000 taxpayers affected by the data breach.

The I.R.C. § 6103 requires safeguarding the confidentiality of tax returns and return information. Disclosing such information to third parties is only permitted when authorized by a specific exception within the statute or when it becomes public record during a tax administration proceeding. When large-scale data breaches occur, the IRS has a legal responsibility to notify all taxpayers. In addition, providing notification letters to taxpayers helps to inform them of their rights of recourse.

The IRS Did Not Have a Process to Identify and Resend Undelivered Mailings to Thousands of Affected Taxpayers

The IRS informed us that thousands of taxpayers did not receive the initial letters that the IRS mailed. As a result, these taxpayers were not notified about this unauthorized disclosure. Undeliverable mailings were stored at the IRS's campus in Philadelphia, Pennsylvania. Initially, the IRS did not know the total number of undeliverable mailings related to the data breach because they were comingled with undelivered mailings at the Philadelphia campus.



Undeliverable letters stored at the IRS's campus in Philadelphia, Pennsylvania. TIGTA photo.

On July 26, 2024, we issued an alert that recommended the IRS take immediate action to develop a solution for sorting the undeliverable mail and determine how many of the mailings are related to the unauthorized disclosure. In addition, we recommended that the IRS develop a plan to identify the correct mailing addresses for individual and business taxpayers with undeliverable notifications. The IRS agreed with our recommendations and developed a plan to address our concerns.

According to the IRS, approximately 12,200 undelivered mailings were related to the data breach, which had been returned to the IRS by the U.S. Postal Service. The IRS stated it would resend notices where the address of record was incomplete, the taxpayer was temporarily unavailable, or the U.S. Postal Service noted an alternative address on a return label.

We reviewed a judgmental sample of 50 individual and 50 business taxpayer notifications from the batches of undeliverable mailings we found at the IRS's Philadelphia campus.³ We also verified that the address of record on the IRS's Master File matched the address of record on the undeliverable mailing for all business taxpayers.

For the sample of individual taxpayers, we identified seven taxpayers with international addresses on the undelivered mailings that did not match the address of record on the Master File. The IRS confirmed that the complete address of record for international addresses did not transfer to the notification letter. The PGLD worked with the IRS's Research, Applied Analytics and Statistics (RAAS) to identify the address for international taxpayers who were sent notification letters. Those addresses were rechecked to ensure that they included the complete address from the Master File for delivery. According to the IRS, in September 2024 it resent notices to 515 taxpayers with international addresses.

Although the IRS developed a plan to identify correct mailing addresses and resend the notifications, it will be limited because some individual and business taxpayers do not have an

³ A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

updated address of record on the Master File. For example, some businesses did not file taxes in recent years. In addition, some individuals may have moved but did not have updated addresses on file with the IRS. In these cases, the IRS stated it would not have a way to resend the data breach notices to the taxpayers.

In our July alert, we recommended that the IRS:

Recommendation (Alert): Develop a solution on how to sort the undeliverable mail and determine how many of the mailings are related to the data breach, including establishing a time frame for completion.

Management's Response to the Alert: The IRS agreed with this recommendation and PGLD developed a solution to sort the undeliverable mail related to the unauthorized disclosure. According to the IRS, they reviewed all undelivered mail related to this incident received to date as of August 9, 2024, and expected there to be more returned to the IRS. For future mailings related to this incident, PGLD will include a postal stop in the return address directing the mail to a specific office. This should eliminate the need to sort undeliverable mail related to this incident. Also, PGLD is coordinating with existing scanning operations at the IRS's Philadelphia Campus to record undeliverable mail.

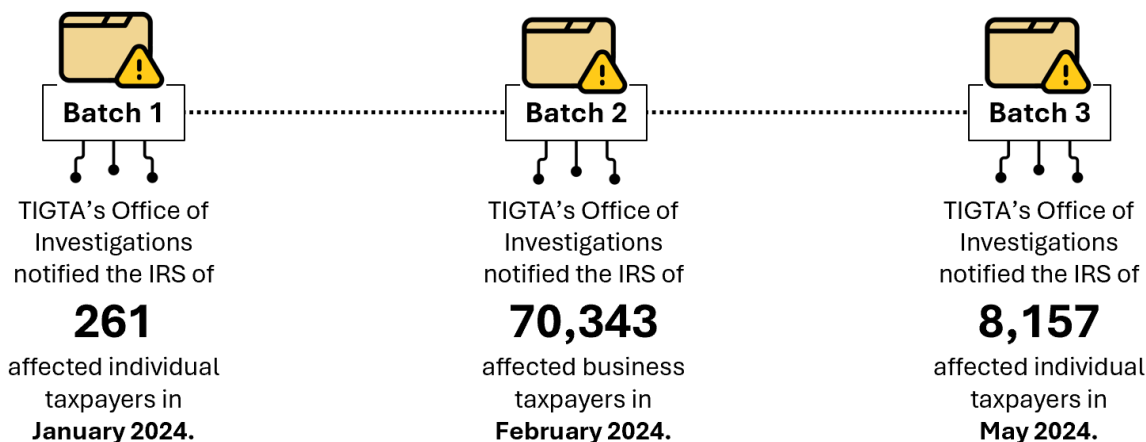
Recommendation (Alert): Develop a plan to identify correct mailing addresses for individual and business taxpayers with undeliverable notifications.

Management's Response to the Alert: The IRS agreed with this recommendation and developed a plan to identify correct mailing addresses for individual and business taxpayers with notifications returned as undeliverable. According to the IRS, the plan is consistent with current IRS policy and ensures that there are protections against potential unauthorized disclosures. In accordance with this policy, PGLD will correct mailing addresses and coordinate remailing the notifications where the address of record was illegible or incomplete, the taxpayer was temporarily unavailable, or an alternative address was noted by the U.S. Postal Service.

The IRS Placed Data Breach Indicators on Most of the Affected Taxpayer Accounts


From January through May 2024, TIGTA's OI shared information with the IRS on 8,418 individual and 70,343 business taxpayers affected by the data breach. Figure 1 highlights the incremental batches of information that TIGTA's OI provided to the IRS.


Figure 1: Batches of Information That TIGTA's OI Provided to the IRS About the Large-Scale Data Breach




Source: TIGTA's correspondence and lists of taxpayers affected by the data breach.

We found that the IRS did not place the data breach indicator on some individual and business taxpayer accounts that TIGTA's OI identified as of July 2024. For instance, we found that:

- 

For Batch 1, the IRS did not place the indicator on the tax accounts of 11 of 261 individual taxpayers. However, we checked the Master File and determined that these taxpayers were deceased, so indicators should not be placed on their tax accounts.⁴
- 

For Batch 2, the IRS did not place the indicator on the tax accounts of 1,076 of 70,343 business taxpayers. The RAAS officials stated that 22 of the 1,076 Employer Identification Numbers were inactive, so the data breach indicator could not be added to their accounts. The IRS could not locate an account on the Master File for the remaining 1,054 business taxpayers. We reviewed a judgmental sample of 30 businesses without the data breach indicator on their tax accounts and confirmed that all 30 of the businesses were not identified in the Master File, so indicators could not be placed on their tax accounts.
- 

For Batch 3, the IRS did not place the indicator on the tax accounts of 1,334 of 8,157 individual taxpayers. Based on our review of the two previous batches and limited research into some taxpayer accounts in this batch, we believe indicators may not be needed on some taxpayer accounts due to various circumstances, such as the taxpayers being deceased or not having active accounts on the Master File.

Based on the results of our analysis, we determined that the IRS placed the data breach indicator on most of the taxpayer accounts identified by TIGTA OI as being impacted by the data breach. Although there are instances where the IRS may not need to place data breach indicators (*e.g.*, deceased individuals), it is important that the IRS take action to determine which of the 1,334 taxpayer accounts should have the indicator and receive the notification.

⁴ The IRS informed us that judicial courts have held that the right to bring a cause of action under § 7431(a) is a personal privacy right. As such, personal privacy rights do not survive the death of the injured party, in this case, the taxpayer. Since a deceased taxpayer had no right to bring a cause of action under § 7431(a), there is no reason to add the indicator on their accounts or to notify them of rights that do not pertain to them.

Recommendation 1: The Chief Privacy Officer should review the 1,334 individual taxpayer accounts and if warranted, take appropriate actions to place the data breach indicator on tax accounts and mail notification letters to additional taxpayers affected by the data breach.

Management's Response: IRS management agreed with this recommendation and stated that it completed its review of the 1,334 taxpayer accounts. The IRS found 1,067 were related to taxpayer accounts of deceased taxpayers, 25 did not have an account or valid mailing address, 222 had a data breach indicator placed on the taxpayer account, and 20 were incorrectly classified as deceased taxpayers. The IRS stated that it will add the data breach indicators to these 20 accounts and mail out notifications.

The IRS Continues to Identify Taxpayers Affected by the Large-Scale Data Breach

TIGTA's OI identified and provided the IRS with Taxpayer Identification Numbers (TIN) for 8,148 individual and 70,343 business taxpayers affected by the data breach.⁵ According to PGLD officials, when it received the impacted taxpayer TINs from TIGTA, PGLD worked with RAAS stakeholders to match the TINs to the IRS's address of record. The PGLD and RAAS also worked to identify secondary taxpayers associated with the primary taxpayers.

In June 2024, TIGTA's OI provided the IRS with additional criteria that could be considered to identify taxpayers affected by the data breach. The RAAS stated that it used this criteria and some of its own criteria to analyze the TINs that OI provided to identify additional taxpayers affected by the data breach.

In August 2024, the Treasury notified TIGTA that the IRS's ongoing review of taxpayer records impacted by the data breach exceeded the 100,000 threshold for declaring a major incident. A week later, Treasury sent a letter to the Chair and Ranking Member of the Senate Finance Committee to report the data breach as a major incident since personally identifiable information for more than 100,000 taxpayers was exfiltrated. As of November 2024, the IRS determined that the data breach affected approximately 406,000 taxpayers.

According to the IRS, after RAAS completes its analysis, the agency will begin placing the data breach indicator on impacted accounts and mailing unauthorized disclosure notification letters to affected taxpayers.

Recommendation 2: The Chief Privacy Officer should continue working to identify all individual and business taxpayers impacted by the unauthorized disclosure. If warranted, take appropriate actions to place the data breach indicator on tax accounts and mail notification letters to additional taxpayers affected by the data breach.

Management's Response: IRS management agreed with this recommendation and stated that it completed its analysis of the data. The IRS identified an additional 22 individual and 412 business taxpayers affected by the data breach. The IRS will place the data breach indicator on the taxpayer accounts and mail notifications.

⁵The TIN is a nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, it can be an Employer Identification Number, a Social Security Number, or an Individual Taxpayer Identification Number.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this project was to assess the IRS's processes and procedures to notify individual and business taxpayers affected by a large-scale data breach. To accomplish our objective, we:

- Assessed whether all individual and business taxpayers affected by the data breach received notification letters.
- Assessed whether all individual and business taxpayers affected by the data breach had the data breach indicator placed on their tax accounts.
- Evaluated whether the address information for approximately 12,200 undeliverable mailings matched the address of record on the IRS's Master File. We obtained a judgmental sample of undeliverable mailings for 50 individual and 50 business taxpayers.
- Evaluated whether the 1,076 business taxpayers without the data breach indicator on their account were identified on the Master File. We used a judgmental sample of 30 business taxpayers to determine whether they were identified on the Master File.
- Evaluated whether the 1,334 individual taxpayers without the data breach indicator on their account were identified on the Master File. We used a judgmental sample of 30 individual taxpayers to determine whether they were identified on the Master File.

Performance of This Review

We performed this review at IRS locations in Bloomington, Illinois, and Philadelphia, Pennsylvania. We also obtained information from the PGLD and RAAS from June 2024 through December 2024. We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *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.

Data Validation Methodology

We performed tests to assess the reliability of data from the Individual Master File and the Business Master File stored in the Data Center Warehouse. We used a random sample of TINs from the Data Center Warehouse and compared the sample to data in the Integrated Data Retrieval System. In addition, we found that the Individual Master File and the Business Master File data contained in the Data Center Warehouse were in the expected ranges. The data did not have any unexpected values, and we determined the data to be sufficiently reliable for the purposes of this report. Further, we performed tests to assess the reliability of data from the batches that TIGTA's OI provided. We determined the data to be sufficiently reliable for the purposes of this report.

Appendix II

Sample Notification Letters Mailed to Taxpayers Affected by the Large-Scale Data Breach



Department of the Treasury
Internal Revenue Service
Washington, DC 20224

Date: XXXXX

XXXXXX
XXXXXX
XXXXXX

Dear XXXX:

We're providing you this letter to notify you that an Internal Revenue Service (IRS) contractor has been charged with the unauthorized inspection or disclosure of your tax return or return information, between 2018 and 2020.¹

When personal information is improperly handled, there may be a risk of identity theft. You can find additional information about identity theft and how you can protect yourself at **FTC.gov/IDTheft**.

We've enclosed copies of Internal Revenue Code (IRC) Section 7431 and the criminal charge with this letter. IRC 7431(a) provides for civil claims for unauthorized disclosure of return information.

The Department of Justice is prosecuting this matter and has provided information about the Crime Victims' Rights Act and the status of this criminal case at **Justice.gov/criminal-vns/case/united-states-v-charles-littlejohn**. If you have any questions about your rights under the Crime Victims' Rights Act, please email the Department of Justice at **CRM-PIN.Victims@usdoj.gov**.

If you have questions about the law or any private right of action you may have, you should consult an attorney.

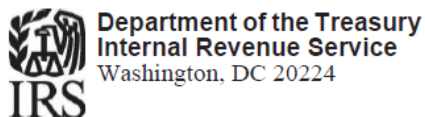
If you have questions for IRS about this matter, you can email us at **Notification.7431@irs.gov**, and we'll respond to you. Please do not email sensitive information (e.g., Social Security numbers, home addresses, bank routing and account numbers or other sensitive Personally Identifiable Information). To expedite a response to your inquiry, you can provide us a personal contact phone number so we can discuss matters directly, if necessary, to provide a full response.

Enclosures:

IRC Section 7431

Copy of criminal information, U.S. v. Littlejohn

¹ See 26 USC Sec. 7431, as amended by the Taxpayer Browsing Protection Act of 1997.



Date: XXXXX

XXXXXX
XXXXXX
XXXXXX

Dear XXXXX :

We are providing you this letter to notify you that an Internal Revenue Service (IRS) contractor has been charged with the unauthorized inspection or disclosure of your tax return or return information, between 2018 and 2020.¹

We have enclosed copies of Internal Revenue Code (IRC) Section 7431 and the criminal charge with this letter. IRC 7431(a) provides for civil claims for unauthorized disclosure of return information.

The Department of Justice is prosecuting this matter and has provided information about the Crime Victims' Rights Act and the status of this criminal case at Justice.gov/criminal-vns/case/united-states-v-charles-littlejohn. If you have any questions about your rights under the Crime Victims' Rights Act, please email the Department of Justice at CRM-PIN.Victims@usdoj.gov.

If you have questions about the law or any private right of action you may have, you should consult an attorney.

If you have questions for IRS about this matter, you can email us at Notification.7431@irs.gov, and we'll respond to you. Please do not email sensitive information (e.g., Employee Identification numbers, business addresses, bank routing and account numbers or other sensitive Business or Personally Identifiable Information).

Enclosures:

IRC Section 7431

Copy of criminal information, U.S. v. Littlejohn

1. See 26 USC Sec. 7431, as amended by the Taxpayer Browsing Protection Act of 1997.



PRIVACY, GOVERNMENTAL
LIAISON AND DISCLOSURE

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

This is a supplement to the 7431 Notification (Letter 6613) that you received from the Internal Revenue Service, which alerted you to the unauthorized disclosure of your tax return information by an IRS contractor. As you may know, the IRS contractor, Charles Edward Littlejohn, pled guilty to the unauthorized disclosure of return information in October 2023 and was sentenced to five years in prison earlier this year.

To begin with, it should be stressed that this incident was unacceptable. Any improper access or disclosure of confidential taxpayer information is unacceptable, and it is completely at odds with the IRS's values and the agency's commitment to taxpayers.

We recognize that this incident has created a difficult situation for many taxpayers, including individuals as well as business entities. We also recognize that it is incumbent on the IRS not only to protect confidential taxpayer information, but also to address matters to the fullest extent possible when any such information is unlawfully disclosed.

We write to you today to update you on our efforts in this regard, and to provide to you what information we can regarding this incident, within the confines of the law. We will update you periodically as additional information becomes available. As noted in our initial letter, you can always contact us with specific inquiries via our dedicated email address for this incident (Notification.7431@irs.gov).¹

We note that responding to this incident presents a number of challenges for the IRS. First, because much of the relevant information was uncovered in a criminal investigation, there are legal limitations on what the IRS can disclose. The criminal investigation was conducted by the Treasury Inspector General for Tax Administration (TIGTA) and resulted in Mr. Littlejohn being charged by DOJ with unauthorized disclosure of tax information, pleading guilty, and being sentenced to a prison term. In deference to these criminal proceedings, it was only after Mr. Littlejohn was sentenced, in February 2024, that the IRS was able to access information regarding all affected taxpayers. The data set that the IRS received at that point is voluminous and complex, and the IRS has been working with TIGTA to process and analyze this data, including to more fully understand what information, pertaining to what taxpayers, was unlawfully disclosed by Mr. Littlejohn. We are doing this so that we can provide taxpayers with notice of the incident as Section 7431 of the Internal Revenue Code requires, and so that we can take whatever additional steps are warranted to address taxpayer inquiries.

¹ As noted in our prior letter, please do not include sensitive personal or financial information in your email.

interests, and concerns. This has taken some time, which is why we may need to follow up with you through additional correspondence. But there is some factual information that we can provide to you at this stage, which may help you to better assess and manage any risks presented to you by this incident:

- First, you should note that this incident occurred several years ago. In particular, Mr. Littlejohn admitted that he collected taxpayer information between 2018 and 2020, which he subsequently unlawfully disclosed to two news organizations. Mr. Littlejohn has stated details regarding these disclosures in the court filings in his criminal case.
- If you are receiving this letter, it is our understanding that Mr. Littlejohn unlawfully disclosed information corresponding to your taxpayer identification number maintained on an IRS database. We do not know – at least not at this point – the full scope of the specific information that Mr. Littlejohn unlawfully disclosed. However, a broad set of taxpayer information is maintained in this database.
- We have seen no indication thus far that any of this information has been disclosed by Mr. Littlejohn to any persons outside of the two news organizations referenced above, or that these news organizations have disclosed this information to any additional persons (beyond the information that they publicly reported). As may be of particular concern to individual taxpayers, we have not seen any indication that this taxpayer information was used in any way for identity theft or any related type of fraud.
- We understand from TIGTA and DOJ that the government has recovered the taxpayer information that was in Mr. Littlejohn's possession.

As noted above, the IRS is continuing to work with TIGTA to better understand this incident, analyze the relevant data, and take appropriate next steps. Among other things, we are continuing to contact any additional impacted taxpayers that we identify, including Form K-1 recipients that may have had their information disclosed. Of particular relevance for individual taxpayers, the IRS has in place screening and review procedures to identify and address potential identity theft and/or tax refund fraud. We also encourage taxpayers and/or their tax professional to review the resources regarding identity theft referenced in our prior letter, and to check IRS transcripts to ensure that taxpayer IRS account(s) do not reflect any unusual activity.²

Apart from the measures specific to this incident discussed above, it bears noting that the IRS has taken aggressive action more generally to enhance data security – to ensure, to the fullest extent feasible, that nothing like the Littlejohn incident can happen

² For information on how to request tax account records, please refer to: [Get Transcript | Internal Revenue Service \(irs.gov\)](#).

in the future. We recognize that this does not address the most immediate concerns of taxpayers whose information has already been unlawfully disclosed. Still, in the hope that this conveys to you our commitment to safeguard tax and financial information and to protect taxpayers' rights, we note that we have developed a number of the protocols and protections that the IRS has put in place in recent years using Inflation Reduction Act (IRA) funding resources and industry and government best practices to better protect taxpayers. These include further restricting user access for the most sensitive taxpayer data sets; more robust protective security controls; more frequent data reviews; improved firewalls; stronger around the clock data monitoring; new security tools; less use of removable media; tighter email controls; new printer controls and improved retention of data access logs.

As discussed above, please contact us with specific questions or concerns. We are working to respond to taxpayer inquiries, and we will provide further updates on this matter. Please be assured that this matter in particular – and safeguarding taxpayer information in general – are among the highest priorities of the Internal Revenue Service.

Appendix III

Management's Response to the Draft Report



CHIEF PRIVACY OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

May 15, 2025

MEMORANDUM FOR NANCY LAMANNA
DEPUTY INSPECTOR GENERAL FOR INSPECTION AND EVALUATIONS

FROM: John J. Walker
Acting Chief Privacy Officer John J. Walker

Draft Evaluation Report – Thousands of Notifications to
Taxpayers Affected by the Large-Scale Data Breach Were
Returned Undeliverable (Evaluation No.: IE-24-041)

Digitally signed by John J.
Walker
Date: 2025.05.14 16:08:47
-04'00'

Thank you for the opportunity to respond to the above referenced draft evaluation report. We appreciate your recognition of the positive steps taken by the IRS to fulfill our statutory obligation to notify all taxpayers affected by this large-scale breach including our development of solutions to sort and identify correct mailing addresses for undeliverable mail in alignment with your recommended (alerts) shared with us earlier in your evaluation.

We agree with the recommendations. We value the Treasury Inspector General for Tax Administration assessment of IRS processes and procedures used to notify individual and business taxpayers affected by this breach.

Attached is a detailed response outlining our corrective actions.

We will continue to ensure that the requirements of Internal Revenue Code Section 7431(e) and 6103 are followed in our response effort. If you have any questions, please contact me at 215-301-5030, or a member of your staff may contact Paul Graves, Associate Director, Information Protection Projects at 240-613-5753.

Attachment

Attachment
TIGTA Draft Evaluation # IE: 24-041

Recommendation 1: The Chief Privacy Officer should review the 1,334 individual taxpayer accounts and if warranted, take appropriate actions to place the data breach indicator on tax accounts and mail notification letters to additional taxpayers affected by the data breach.

Corrective Action: The IRS agrees with this recommendation. IRS received from TIGTA, the Taxpayer Identification Numbers (TINs) for 1,334 individual taxpayers. IRS completed its review of the TINs to determine that data breach indicators ("indicator") are placed on the taxpayer accounts where notifications were appropriately mailed.

IRS analysis of the TINs indicated the following: 1,067 related to taxpayer accounts of deceased taxpayers; 25 did not have an account or valid mailing address on the Individual Master File (IMF); and 222 had a data breach indicator placed on the taxpayer account. IRS noted 20 taxpayer accounts where an indicator was not applied, and notifications were not mailed. This discrepancy was due to taxpayers that had "DECD" indicated in the spouse's name line and were incorrectly classified as deceased taxpayers. IRS is adding the indicators to these accounts, mailing the notifications and will complete this process by May 31st.

Implementation Date: May 31, 2025

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Identity and Records, Director (Information Protection Projects).

Recommendation 2: The Chief Privacy Officer should continue working to identify all individual and business taxpayers impacted by the unauthorized disclosure. If warranted, take appropriate actions to place the data breach indicator on tax accounts and mail notification letters to additional taxpayers affected by the data breach.

Corrective Action: The IRS agrees with this recommendation. IRS completed its analysis of the data to identify individuals and business taxpayers impacted by the unauthorized disclosure and will take action to place the data breach indicators on the taxpayer accounts and mail notifications for the additional taxpayers identified. IRS identified an additional 412 business entities and 22 individuals that will be mailed notifications by May 31, 2025. Breach indicators will be placed on the taxpayer accounts as appropriate, except for taxpayers with locked accounts by May 31, 2025. The purpose of the indicator is to alert IRS Customer Service Representatives that taxpayers were involved in the breach incident and to direct the taxpayers to the 7431 mailboxes should they have any inquiries. Inquiries from the taxpayers with locked accounts would likely go through different channels and the benefit of placing the indicators on the accounts to manage any inquiries would not warrant the risk associated with unlocking the accounts due to the sensitivity of the information.

Implementation Date: May 31, 2025

Responsible Official(s): Chief Privacy Officer (Privacy, Governmental Liaison & Disclosure); Identity and Records, Director (Information Protection Projects).

Appendix IV

Abbreviations

IRS	Internal Revenue Service
OI	Office of Investigations
PGLD	Privacy, Governmental Liaison and Disclosure
RAAS	Research, Applied, Analytics & Statistics
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number
Treasury	U.S. Department of the Treasury



**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.