

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



Sensitive Tax Information Is Not Being Controlled Adequately When Shipping to and From Tax Processing Centers

August 1, 2023

Report Number: 2023-IE-R007

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.

HIGHLIGHTS: Sensitive Tax Information Is Not Being Controlled Adequately When Shipping to and From Tax Processing Centers

Final Evaluation Report issued on August 1, 2023

Report Number 2023-IE-R007

Why TIGTA Did This Study

IRS employees who work in the various operating division functional areas have an ongoing need to obtain and review tax documents as part of the duties they perform. Internal guidelines state that IRS employee requests for paper tax records are sent to the Tax Processing Center where the tax information is stored. When IRS personnel request tax documents located outside of the particular Tax Processing Center that services the request, the IRS ships the requested information to these employees using a private delivery carrier. TIGTA initiated this review to assess the IRS's compliance with policies and procedures when mailing Federal tax information via private delivery carrier.

Impact on Tax Administration

TIGTA is concerned that the IRS is not taking actions to properly account for and control sensitive tax information. Therefore, the IRS is unable to identify, notify, and offer protection to some taxpayers when their sensitive tax information is lost in the mail.

What TIGTA Found

The IRS is not adhering to its own internal guidelines when sending large volumes of sensitive taxpayer information to and from its Tax Processing Centers. Specifically, required tracking documents, *i.e.*, Forms 3210, *Document Transmittal*, are not included with these shipments and/or not prepared properly. For example, during the period August to November 2022, TIGTA conducted on-site inspections of 31 incoming packages with large quantities of sensitive taxpayer information received via private delivery carrier at the Tax Processing Centers. Twenty-two of the 31 packages did not include copies of the completed Forms 3210. Further, TIGTA conducted inspections of 40 packages with large volumes of sensitive taxpayer information that were ready for shipment from the Tax Processing Centers via private delivery carrier. Thirty-nine of the 40 packages did not include copies of the completed Forms 3210. Further, Submission Processing Files function managers at the three Tax Processing Centers are not completing the required quarterly audits of the Forms 3210 Acknowledgment process to ensure compliance with internal guidelines.

Also, the Privacy, Governmental Liaison, and Disclosure Office does not notify businesses or place a data breach indicator on business tax accounts when packages with sensitive business tax information are lost.

What TIGTA Recommended

TIGTA made five recommendations including that the Commissioner, Wage and Investment Division, should ensure that the Form 3210 is completed and included in all packages so actions can be taken to protect taxpayers when a shipment is lost; and ensure that Submission Processing Files function managers conduct quarterly audits of the Forms 3210 Acknowledgment process. Further, the Chief Privacy Officer, Privacy, Governmental Liaison, and Disclosure, should revise internal guidelines to reflect that losses associated with a business are not categorized as low risk automatically and provide notification for business data losses categorized as high risk.

IRS management agreed with four of our recommendations and partially agreed with one recommendation. The IRS plans to issue a notice to remind employees to include a Form 3210 with shipments of large volumes of tax information. In addition, the IRS plans to issue a notice to remind employees to include the taxpayers whose information is shipped on the Form 3210. The IRS also plans to send periodic email communications to the Submission Processing Files functions to ensure Form 3210 reviews are being performed. Further, the IRS plans to develop a process for conducting quarterly reviews in the Files functions. The IRS also updated its Data Breach Response Plan to reflect that losses associated with a business are not automatically categorized as low risk.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

August 1, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

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

SUBJECT: Final Report – Sensitive Tax Information Is Not Being Controlled Adequately When Shipping to and From Tax Processing Centers (Evaluation # IE-22-010)

This report presents the results of our review to assess the Internal Revenue Service's (IRS) compliance with policies and procedures when mailing Federal tax information via private delivery carrier. This review is part of our Fiscal Year 2023 Annual Program Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS Resources*.

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

Table of Contents

Background	Page 1
Results of Review	Page 3
<u>Actions Are Not Taken to Properly Account for and/or Control Sensitive Taxpayer Information Sent by Private Delivery Carriers</u>	Page 4
<u>Recommendations 1 and 2:</u>	Page 6
<u>Quarterly Audits of the Forms 3210 Acknowledgement Process Are Not Performed As Required</u>	Page 6
<u>Recommendations 3 and 4:</u>	Page 7
<u>Inadequate Documentation Resulted in the Inability to Identify, Notify, and Offer Protection to Some Taxpayers When Their Sensitive Tax Information Was Lost</u>	Page 8
<u>Data Breach Indicators Are Not Placed on Business Tax Accounts Associated With Sensitive Business Tax Information Lost by the IRS</u>	Page 9
<u>Recommendation 5:</u>	Page 9
Appendices	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 11
<u>Appendix II – Management’s Response to the Draft Report</u>	Page 13
<u>Appendix III – Abbreviations</u>	Page 18

Background

Internal Revenue Service (IRS) employees who work in the various operating division functional areas have an ongoing need to obtain and review tax documents as part of the duties they perform. Internal guidelines state that IRS employee requests for paper tax records are sent to the Tax Processing Center where the tax information is stored. The IRS's Submission Processing Files functions within the Wage and Investment Division at the Tax Processing Centers are responsible for processing requests for tax records.¹ Specifically, the Files functions are responsible for receiving, filing, refiling, and servicing requests for tax documents.

Process to send sensitive tax documents to requesters located outside of a Tax Processing Center

When IRS personnel request tax documents located outside of the particular Tax Processing Center that services the request, the IRS ships the requested information to these employees using a private delivery carrier.² All IRS personnel should use Form 3210, *Document Transmittal*, to account for and control the shipping of this sensitive tax information. For requests that include a large number of taxpayer documents, IRS internal guidelines require employees shipping these documents to:

- List the total number of documents contained in the package and include identifying information, *i.e.*, taxpayer name, Employer Identification Number,³ *etc.*, for at least the first four documents and the last document in the package.⁴
- Include two copies of the Form 3210, the 'Acknowledgement Copy' and the 'Recipient's Copy,' to be placed inside the secure package with its contents while the sender of the package keeps the 'Originator's Copy.'

Once the requesting functional area receives the shipment, the recipient of the package must:

- Verify receipt of the package by signing and returning the Form 3210 'Acknowledgment Copy' to the sender. This can be returned to the sender via e-mail (electronic or scanned copy), fax, or mail.

After receipt, the sender must store the 'Acknowledgment Copy' with the 'Originator's Copy.' If the 'Acknowledgment Copy' is not received, the sender must access the United Parcel Service website to track the shipment to determine if it was delivered successfully, confirm receipt of the package, and request the recipient complete and return the 'Acknowledgment Copy.' Figure 1 provides an example of the Form 3210.

¹ Internal Revenue Manual (IRM) 3.5.61.1.10 (Jan. 1, 2023). A Form 4251, *Return Charge-Out*, is generated from an IRS computer system request and printed in the Submission Processing Center according to the Document Locator Number. IRM 3.5.61.1 (Jan. 1, 2023). The Tax Processing Centers are located in Kansas City, Missouri; Austin, Texas; and Ogden, Utah.

² IRM 10.5.1.6.9.3 (Dec. 31, 2020). Packages with Personally Identifiable Information (PII) that weigh 13 ounces or more must be shipped through a private delivery carrier.

³ The Employer Identification Number is a unique, nine-digit number used to identify a taxpayer's business account.

⁴ IRM 3.5.61.1.7.3 (Jan. 1, 2023).

Final Report - Sensitive Tax Information Is Not Being Controlled Adequately When Shipping to and From Tax Processing Centers

Figure 1: Form 3210

Document Transmittal	To (Show complete and correct address)		Release Date	Page <input type="text"/> of <input type="text"/>
			Transmittal Code (From-Serial no.-To)	
			Numbered	Unnumbered
Document Identification			Remarks	
Quantity	Code or Type	Instructions: When transmitting reports, please show the type of report and the period covered. For other items, show identifying information such as blocks, DLN, EIN, the last four digits of the SSN, etc.	Shipment Information	
			Container No.	Rec'd (✓)

Part 1 – Recipient's copy	Part 2 – For Facilities Management	Part 3 – Acknowledgement copy	Part 4 – To be retained by originator
----------------------------------	---	--------------------------------------	--

Form 3210 (Rev. 4-2010) Catalog Number 22150T Department of the Treasury Internal Revenue Service

Source: IRS Product Catalog revision dated April 2010.

Reporting lost packages with sensitive taxpayer information to the IRS's Office of Privacy, Governmental Liaison, and Disclosure/Incident Management (PGLD/IM) Office is required

Internal guidelines require IRS employees to immediately report, upon discovery, all instances of lost mailed packages to the IRS PGLD/IM Office as well as the Treasury Inspector General for Tax Administration (TIGTA). In addition, if a data breach involves the loss, theft, or unauthorized destruction of documents containing sensitive taxpayer information, IRS employees must report it to their manager and to the PGLD/IM Office using the online Form 14164-A, *Personally Identifiable Information (PII) Breach Reporting Form*, (Rev. 11-2022).

Once the reported information is received, the PGLD/IM Office will review the information and perform its required risk analysis. The risk analysis is performed to evaluate the likely risk of harm for all reported IRS data breaches, based on standardized factors and ratings criteria. The result of the analysis is a categorization⁵ of the data breach into one of four levels:

- **No Impact** – The loss of confidentiality, integrity, or availability could be expected to have no adverse effect on organizational operations, organizational assets, or individuals. The IRS does not offer identity protection or monitoring services when the risk analysis determines no impact.

⁵ Categorization into levels dictates a recommended level of response and determines when, what, how, and to whom notification of a data breach must be given.

- *Low Impact* – The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. The IRS does not offer identity protection or monitoring services when the risk analysis determines low impact.
- *Moderate Impact* – The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The IRS does not offer identity protection or monitoring services when the risk analysis determines moderate impact.
- *High Impact* – The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. The IRS offers individual identity protection and monitoring services.

The reporting employee and the employee's manager will receive an *Impacted Individuals and/or Business Excel Spreadsheet* from the PGLD/IM Office that requires them to input the Taxpayer Identification Numbers of the taxpayers and/or businesses potentially impacted by the data breach. Once completed, the reporting employee e-mails the spreadsheet via secure e-mail to the **PII mailbox* within two business days of receipt. After the PGLD/IM Office has completed its risk analysis and developed a recommendation regarding the appropriate response, if the recommendation is to notify, the PGLD/IM Office will:

- Notify the potentially impacted taxpayers of an IRS data breach involving their sensitive information via Letter 4281C, *Incident Management Breach Notification Letter*. This letter includes a brief description of the data breach, the type of PII disclosed, actions the taxpayers should take, contact information, taxpayer rights, and a statement that the IRS has provided or will provide potentially impacted taxpayers with identity protection and identity monitoring service at no cost.
- Update the taxpayer's tax account with an indicator denoting they are a potentially impacted individual of an IRS data breach. This indicator is placed on a taxpayer's account because of an unauthorized access or disclosure and if the taxpayer is offered identity protections, such as identity protection and identity monitoring services.

Results of Review

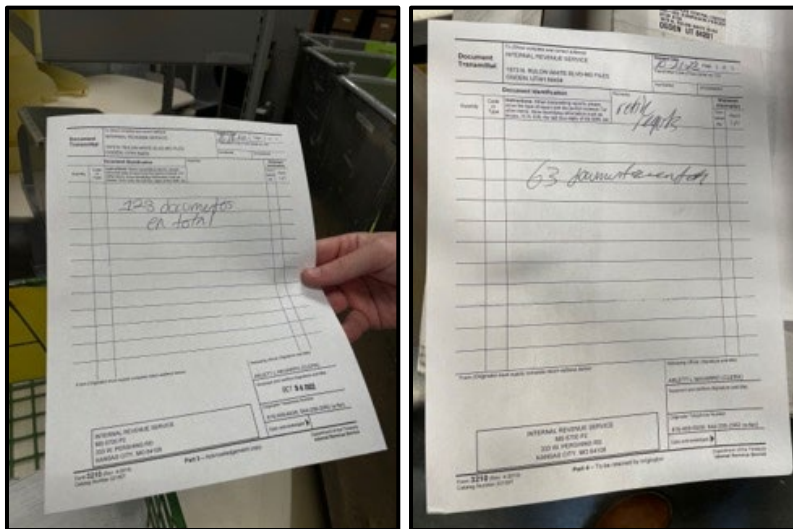
Our review identified that the IRS is not adhering to its own internal guidelines when sending large volumes of sensitive taxpayer information to and from its Tax Processing Centers. Specifically, required tracking documents, *i.e.*, Forms 3210, are not included with these shipments and/or not prepared properly. In addition, steps are not taken to ensure that the Form 3210 tracking acknowledgement is obtained to confirm requester receipt of this sensitive tax information. Furthermore, management is not performing required quarterly audits of its Forms 3210 processes and procedures to ensure compliance with internal guidelines. As a result, the IRS is unable to identify, notify, and/or offer protection to taxpayers when sensitive tax information is lost in the mail and at risk for potential identity theft.

Actions Are Not Taken to Properly Account for and/or Control Sensitive Taxpayer Information Sent by Private Delivery Carriers

During the period August to November 2022, we conducted on-site inspections of 31 incoming packages with large quantities of sensitive taxpayer information received via private delivery carrier at the Kansas City, Missouri; Austin, Texas; and Ogden, Utah Tax Processing Centers. Twenty-two of the 31 packages did not include copies of the completed Forms 3210. Our review of these 31 incoming packages identified:

- 8 packages that did not include the required two copies of the Forms 3210, *i.e.*, the Acknowledgement Copy and the Recipient's Copy, that provide details as to the total number of documents contained in the package as well as the required identifying information, *i.e.*, taxpayer name, Taxpayer Identification Number, *etc.*, for at least the first four documents and the last document in the package.
- 14 packages with incomplete Forms 3210. Specifically, the Forms 3210 did not contain the required identifying information for at least the first four documents and the last document in the package. Figure 2 shows two examples of the incomplete Forms 3210 included with these shipments of sensitive taxpayer information.

Figure 2: Examples of Forms 3210 Observed in Incoming Mailing Packages



Source: Photos taken during TIGTA site visits at the Tax Processing Centers.

In addition, during the same period, we conducted on-site inspections of 40 packages with large volumes of sensitive taxpayer information that were ready for shipment from the Tax Processing Centers via private delivery carrier and identified that only one of the packages included the required properly prepared Form 3210. For the remaining 39 of the 40 packages, we identified the following:

- 26 packages did not include the required Forms 3210.

Final Report - Sensitive Tax Information Is Not Being Controlled Adequately When Shipping to and From Tax Processing Centers

- 13 packages had incomplete Forms 3210. Specifically, the Forms 3210 did not contain the required identifying information for at least the first four documents and the last document in the package.

Finally, for each of three Tax Processing Centers, Files function employees were using an incomplete Form 3210 that included only statements such as "Total boxes of refiles," "Consolidated Mail," and "REQUESTS, FILLED REQUESTS, AND REFILES." These incomplete Forms 3210 were to be used when shipping large volumes of sensitive taxpayer information. The incomplete Forms 3210 did not comply with the IRS's own internal guidelines as to the specific information to be included on the Forms 3210. Figure 3 provides examples of these incomplete Forms 3210.

Figure 3: Examples of Prefilled Forms 3210 Used in Shipping Large Volumes of Sensitive Taxpayer Information

The image shows two examples of Form 3210 (Rev. 4-21-10) used for shipping sensitive taxpayer information. The left form is a 'Part 1 - Recipient's Copy' and the right form is a 'Part 2 - For Facilities Management Use'. Both forms are filled with minimal information, including 'Consolidated Mail' and 'TOTAL BOXES OF REFILES: 87', but missing recipient information.

Source: Photos taken during TIGTA site visits at the Tax Processing Centers.

Inability to identify taxpayers associated with lost shipments containing their sensitive taxpayer information

In our discussions with the Files function, employees indicated that when shipments of large volumes of sensitive taxpayer information are lost, there would be no way to identify specific taxpayers whose information was compromised. This results from the fact that no information is maintained to support which specific taxpayer was associated with the sensitive information in the lost shipment. For example, the IRS could not always determine specific taxpayer(s) associated with some lost shipments during the period January 2021 through August 2022.

Our review of the lost packages tracked by the Tax Processing Centers identified 11 lost packages during the period January 2021 through August 2022.⁶ However, two of the packages were subsequently recovered and therefore, only nine of the 11 packages were lost at the time

⁶ Tax Processing Centers only began tracking lost packages in 2021.

we conducted our analysis. IRS documentation indicated that seven of the nine lost packages contained sensitive taxpayer information. The IRS was unable to provide Forms 3210 for two (29 percent) of these seven lost packages. These two lost packages included:

- A whistleblower case file.
- [REDACTED]

Further, the IRS did not offer identity protection and monitoring services or place the data breach indicator on the tax accounts related to the taxpayers impacted for six (67 percent) of the nine lost packages. Management explained that these actions were not taken because:

- Three packages were related to a business.
- Two packages included an information technology asset and most likely did not contain PII.
- One package did not contain PII (pocket commission).

The IRS did offer identity protection and monitoring services and placed the data breach indicator on the four taxpayers' accounts who were impacted by the remaining three lost packages.

The Commissioner, Wage and Investment Division, should:

Recommendation 1: Remind employees to include required documentation that identifies specific taxpayers whose information is included in shipments of large volumes of sensitive tax information so actions can be taken to protect taxpayers when a shipment is lost.

Management's Response: IRS management agreed with the recommendation and plans to issue a Service-wide Electronic Research Program Alert to remind employees to include required documentation.

Recommendation 2: Remind employees to include the required Forms 3210 with all shipments of large volumes of sensitive taxpayer information.

Management's Response: IRS management agreed with the recommendation and plans to issue a Service-wide Electronic Research Program Alert to remind employees to include Form 3210 with all large volume shipments of taxpayer information.

Quarterly Audits of the Forms 3210 Acknowledgement Process Are Not Performed As Required

Managers at the Submission Processing Files function at the three Tax Processing Centers indicated that the required quarterly audits of the Forms 3210 Acknowledgment process were not completed to ensure compliance with internal guidelines. As a result, there is no assurance that appropriate follow-up and confirmation of receipt of sensitive taxpayer information is occurring nor whether senders of sensitive taxpayer information are following up on Form 3210 acknowledgments so that lost packages are identified quickly. Specifically:

- One manager stated that they were unaware of the internal requirement to perform quarterly audits of Forms 3210.
- One manager stated that audits were being conducted occasionally, but only to verify a signature and date on the form, rather than completeness, accuracy, and acknowledgement of receipt.

Internal guidelines state that all IRS managers must perform, at a minimum, quarterly audits of the Form 3210 Acknowledgment process for packages sent with sensitive taxpayer information to ensure that appropriate follow-up and confirmation of receipt of this sensitive taxpayer information is occurring.⁷ This requirement is to ensure that managers validate that senders of sensitive taxpayer information are following up on Form 3210 acknowledgments within defined time frames so that lost packages are identified quickly. This reduces the likelihood that the sensitive taxpayer information could be exposed to an unauthorized user. Local Files function management must determine the proper follow-up time frame as part of the manager's operational review. Further, employees are to maintain the Form 3210 following the existing record retention schedule for each business unit, which is approximately one year.⁸

Submission Processing Files function personnel stated that they do not receive the majority of the Forms 3210 Acknowledgement copies associated with mailed packages containing sensitive taxpayer documents, which impacts the IRS's ability to perform the required verifications. As a result, Files function management did not know how many Forms 3210 Acknowledgement copies were returned to the sender and matched with the original copy of the Form 3210, making it difficult for managers to even perform the required quarterly audits.

The Commissioner, Wage and Investment Division, should:

Recommendation 3: Ensure that Submission Processing Files function managers are informed of the requirement to perform quarterly audits of the Forms 3210 Acknowledgement process.

Management's Response: IRS management agreed with the recommendation and plans to send periodic e-mail communications to the Submission Processing Files functions to ensure reviews are being performed and require proof of review documentation.

Recommendation 4: Develop processes and procedures to ensure that the required quarterly audits of the Forms 3210 Acknowledgment process are performed in the Submission Processing Files function.

Management's Response: IRS management agreed with the recommendation and plans to develop a process for conducting quarterly reviews in the Submission Processing Files functions.

⁷ IRM 10.5.1.6.9.3 (Dec. 31, 2020).

⁸ Document 12990, *Records and Information Management Records Control Schedules*.

Inadequate Documentation Resulted in the Inability to Identify, Notify, and Offer Protection to Some Taxpayers When Their Sensitive Tax Information Was Lost

When an IRS data breach or incident occurs, depending on what was lost, stolen, or disclosed, employees must report the data breach or incident to the PGLD/IM Office using the *PII Breach Reporting Form*, the Computer Security Incident Response Center using the *Computer Security Incident Reporting Form*, or to the Situational Awareness Management Center using the *Incident Reporting Link*.⁹ During the period October 2019 to August 2022, IRS personnel notified the PGLD/IM Office of 599 instances where packages containing sensitive taxpayer information and/or information technology assets were lost.¹⁰ We selected a random sample of 50 of the lost packages to determine whether the IRS identified specific taxpayers whose tax information was lost, offered these taxpayers identity protection and monitoring services, and updated the associated taxpayer's tax account with an indicator denoting a possible breach of their sensitive tax information. Our review of the 50 packages identified:

- 18 packages (36 percent) for which the IRS identified, notified, and offered identity protection and monitoring services to 49 taxpayers associated with these lost packages. In addition, for all 49 taxpayers, their associated tax accounts were updated to include the data breach indicator.
- 12 packages (24 percent) for which the IRS explained that identity protection and monitoring services were not offered to the taxpayers associated with these losses as the packages were subsequently recovered.
- 10 packages (20 percent) for which the IRS indicated that identity protection and monitoring services were not offered to taxpayers because the packages contained an electronic device that was encrypted and therefore, no taxpayer information was compromised in the lost packages.
- 10 packages (20 percent) for which the IRS did not offer taxpayers identity protection and monitoring services or update their tax account as required. These included:
 - 7 packages in which the PGLD/IM Office reported that identity protection and monitoring services were not offered because the functional area that reported the lost packages could not identify the specific taxpayers associated with the lost tax information.
 - 3 packages in which the PGLD/IM Office reported that identity protection and monitoring services were not offered because the packages contained business tax information.

The lack of documentation identifying the specific taxpayers whose tax information is included in a lost package has impacted the IRS's ability to notify and protect taxpayers. Due to increasing occurrences of data breaches and identity theft, it is critical that the IRS maintain

⁹ IRM 10.5.4.4.1 (Mar. 2, 2023).

¹⁰ An information technology asset is property or equipment that is part of the information technology infrastructure, including hardware and software for information technology and telecommunications data and voice that is in use, in reserve storage, or is awaiting disposal.

adequate documentation to timely identify taxpayers whose information may have been compromised in a lost shipment and offer affected taxpayers identity protection and identity monitoring services.

Data Breach Indicators Are Not Placed on Business Tax Accounts Associated With Sensitive Business Tax Information Lost by the IRS

The PGLD/IM Office does not notify businesses or place a data breach indicator on business tax accounts when packages with sensitive business tax information are lost. The PGLD/IM Office indicated that the data breach indicators are not added to business tax accounts as it considers business identity theft low risk because business information, such as the name, address, and Employer Identification Number, is often public information and made available to large numbers of individuals.

The risk of potential identity theft not only affects individuals, but it can also affect businesses. The IRS defines business identity theft as creating, using, or attempting to use businesses' information without authority to obtain tax benefits. For example, an identity thief files a business tax return using the Employer Identification Number of an active or inactive business without the permission or knowledge of the owner to obtain a fraudulent refund.

The PGLD/IM Office's position as it relates to the protection of business taxpayers whose sensitive tax information is lost is inconsistent with the significant and ongoing business identity theft return filings the IRS identifies each year. For example, in July 2022, TIGTA's Office of Audit reported that during Processing Year 2021, IRS business identity theft fraud filters identified and selected for review 60,296 business returns as potentially fraudulent.¹¹ On December 12, 2021, the IRS published its first Business Taxonomy Report and reported that the IRS's efforts protected almost \$3.8 billion in fraudulent tax refunds from being issued since Tax Year 2016. However, the IRS also reported that identity thieves were successful in receiving between about \$6 million and \$3.2 billion in fraudulent refunds since Tax Year 2016.

In addition, the PGLD/IM Office is not offering the same protection and assistance to business taxpayers that it provides to individual taxpayers whose sensitive tax information the IRS has lost. For example, if individual tax information is lost in the mail, without suspected identity theft, the IRS places the data breach indicator on the account, not an identity theft indicator. The data breach indicator that is placed on the individual tax account identifies that the taxpayer is a potentially impacted individual of a data breach and was notified of their lost tax information.

The Chief Privacy Officer, PGLD, should:

Recommendation 5: Discontinue the practice of categorizing all business data breaches as low risk. In addition, for data breaches categorized as high risk, issue a notification letter to the business and place the data breach indicator on the business tax account.

Management's Response: IRS management partially agreed with the recommendation and indicated that its Data Breach Response Plan was revised to reflect that losses

¹¹ TIGTA, Report No. 2022-40-041, *Successful Detection and Assistance Processes Used to Combat Individual Identity Theft Should Be Implemented for Business Identity Theft* (July 2022).

associated with a business are not automatically categorized as low risk. In addition, the IRS plans to consider notification for business data losses categorized as high risk, depending on the circumstance. However, the IRS stated that placing a data breach indicator on business tax accounts would cause confusion as the indicator is tied to the loss of PII, which is not the case in a business loss. Further, if a business-related loss is categorized as high risk and a notification letter is sent, the IRS plans to place a history item on the business tax account.

Office of Inspections and Evaluations Comment: TIGTA confirmed that the Data Breach Response Plan was updated to reflect that losses associated with a business are not automatically categorized as low risk. In addition, TIGTA agrees with the IRS's approach to addressing this recommendation.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this project was to assess the IRS's compliance with policies and procedures when mailing Federal tax information via private delivery carrier. To accomplish our objective, we:

- Obtained an understanding of the relevant policies and procedures related to the IRS's processes for tracking mailed Federal tax information.
- Determined the population of lost mail from IRS Tax Processing Centers and the PGLD/IM Office for Fiscal Years 2020, 2021, and 2022.
 - During the period October 2019 to August 2022, IRS personnel notified the PGLD/IM Office of 599 instances where packages containing sensitive taxpayer information and/or information technology assets were lost using the *Impacted Individuals and/or Business Excel Spreadsheet*. We selected a random sample of 50 of the lost packages to determine whether the IRS identified specific taxpayers whose tax information was lost, offered these taxpayers identity protection and monitoring services, and updated the associated taxpayer's tax account with an indicator denoting a possible breach of their sensitive tax information. Our random sample of 50 was generated in Excel from a seed number of 10 and a uniform distribution between 1 and 599 and sorting in ascending order. This sampling method was used due to time constraints and the unique circumstances surrounding the population of 599 lost packages.
 - During the period January 2021 to August 2022, IRS Tax Processing Centers identified 11 instances where packages containing sensitive taxpayer information were lost.
- Evaluated the IRS Tax Processing Centers' processes for tracking taxpayer information sent via private delivery carrier. We reviewed outgoing and incoming mail sent via private delivery carrier for Forms 3210 at IRS Tax Processing Centers in Kansas City, Missouri; Austin, Texas; and Ogden, Utah.
- Assessed the IRS's ability to leverage existing systems to track taxpayer information sent via private delivery carrier more effectively and efficiently.

Performance of This Review



This review was performed at the Tax Processing Centers in Kansas City, Missouri; Austin, Texas; and Ogden, Utah. In addition, we obtained information from the PGLD/IM Office and the Wage and Investment Division located in Washington, D.C., during the period September 2022 through May 2023. We conducted this evaluation in accordance with the Council of the Inspectors General for Integrity and Efficiency Quality Standards for Inspection and Evaluation.

Major contributors to the report were James A. Douglas, Director; Brandon Crowder, Supervisory Evaluator; Meghann Noon-Miller, Lead Evaluator; Morgan Little, Lead Auditor; and Audrey Graper, Senior Auditor.

Validity and Reliability of Data From Computer-Based Systems

We performed tests to assess the reliability of data from the *Impacted Individuals and/or Business Excel Spreadsheet* from the PGLD/IM Office. We evaluated the data by performing electronic testing of a sample of 18 cases using select data elements against an IRS computer system. We also reviewed the data to determine if there were any repeat or incomplete data elements. In addition, we performed tests to assess the reliability of data from the *Lost Packages Excel Spreadsheet* from the Tax Processing Centers. We evaluated the data by performing electronic testing of select data elements against an IRS computer system and the *Impacted Individuals and/or Business Excel Spreadsheet*. We also reviewed the data to determine if there were any repeat or incomplete data elements. We determined that the data were sufficiently reliable for purposes of this report.

Management's Response to the Draft Report

 COMMISSIONER WAGE AND INVESTMENT DIVISION	DEPARTMENT OF THE TREASURY INTERNAL REVENUE SERVICE ATLANTA, GA 30308
July 6, 2023	
MEMORANDUM FOR RUSSELL P. MARTIN DEPUTY INSPECTOR GENERAL FOR INSPECTIONS AND EVALUATIONS	
FROM:	Kenneth C. Corbin  Commissioner, Wage and Investment Division
	Digitally signed by TZQCB Date: 2023.07.06 14:35:40 -04'00'
SUBJECT:	Draft Report – Sensitive Tax Information Is Not Being Controlled Adequately When Shipping to and From Tax Processing Centers (Evaluation # IE-22-010)
<p>Thank you for the opportunity to review and provide comments on the subject draft report. This evaluation addresses a significant operational challenge faced by the IRS in that, as an organization, we are reliant on the need to move massive amounts of paper documents between our Submission Processing Centers, satellite offices, other campus locations, and multiple Federal Records Center locations. Without an enterprise-level tracking system, we rely on the use of Form 3210, <i>Document Transmittal</i>, the purpose of which is to serve as a packing list of contents contained in each shipment. The completion of Form 3210 is a manual process that is reliant on both the sender and the recipient completing their required actions. With additional funding appropriated through the Inflation Reduction Act of 2022¹, we are striving to update our systems and processes to a digital environment that will substantially reduce or eliminate the need to continue shipping paper documents.</p> <p>We recognize the risk associated with shipping documents containing sensitive information from one location to another and take steps to mitigate it. Sensitive information is protected during shipment through double packaging and labeling. The shipment contents are held in a sealed container that is labeled with the delivery information and that container is in turn enclosed in a separate sealed container that is also labeled for delivery. This practice provides an added degree of protection if a parcel becomes damaged during shipment and the outer container or envelope is breached. Additional protection is provided by tracking all shipments. In the event an acknowledgement of receipt is not returned to the sender, packages are trackable to determine if they arrived at the intended destination.</p>	
<p>¹ Pub. L. 117-169</p>	

Final Report - Sensitive Tax Information Is Not Being Controlled Adequately When Shipping to and From Tax Processing Centers

2

If it is discovered that a package containing sensitive taxpayer information was lost, procedures are in place to report the incident via Form 14164-A, *Personally Identifiable Information (PII) Breach Reporting* to the IRS Privacy, Government Liaison and Disclosure (PGLD) Incident Management Office as well as to the Treasury Inspector General for Tax Administration. The PGLD organization further investigates the incident, categorizes its level of impact, and informs the potentially impacted taxpayers via Letter 4281C, *Incident Management Breach Notification Letter*. It also updates the taxpayer's account with a data breach indicator and offer free remediation services such as identity protection and credit monitoring services to the impacted taxpayer.

We agree with your recommendations and the corrective actions we are taking are discussed in the attachment. If you have any questions, please contact me, or a member of your staff may contact Dietra D. Grant, Director, Customer Account Services, at 470-639-3504.

Attachment

Attachment

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1

Remind employees to include required documentation that identifies specific taxpayers whose information is included in shipments of large volumes of sensitive tax information so actions can be taken to protect taxpayers when a shipment is lost.

CORRECTIVE ACTION

We will issue a Servicewide Electronic Research Program (SERP) Alert for Internal Revenue Manual (IRM) 3.5.61.1.7.5, *Form 3210, Document Transmittal*, to remind employees to include required documentation.

IMPLEMENTATION DATE

October 15, 2023

RESPONSIBLE OFFICIAL

Director, Submission Processing, Customer Account Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN

We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 2

Remind employees to include the required Forms 3210 with all shipments of large volumes of sensitive taxpayer information.

CORRECTIVE ACTION

We will issue a Servicewide Electronic Research Program (SERP) Alert for IRM 3.5.61.1.7.5, to remind employees to include Form 3210, *Document Transmittal*, with all large volume shipments of taxpayer information.

IMPLEMENTATION DATE

October 15, 2023

RESPONSIBLE OFFICIAL

Director, Submission Processing, Customer Account Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN

We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 3

Ensure that Submission Processing Files function managers are informed of the requirement to perform quarterly audits of the Forms 3210 Acknowledgement process.

CORRECTIVE ACTION

We will send periodic email communications to the Submission Processing Files functions to ensure reviews are being performed and require proof of review documentation.

IMPLEMENTATION DATE

March 15, 2024

RESPONSIBLE OFFICIAL

Director, Submission Processing, Customer Account Services, Wage and Investment Division

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 the required quarterly audits of the Forms 3210 Acknowledgment process are performed in the Submission Processing Files function.

CORRECTIVE ACTION

We will develop a process for conducting quarterly reviews in the Files functions, consistent with IRM 3.5.61.1.7.5.

IMPLEMENTATION DATE

November 15, 2023

RESPONSIBLE OFFICIAL

Director, Submission Processing, Customer Account Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN

We will monitor this corrective action as part of our internal management control system.

Recommendation

The Chief Privacy Officer, PGLD, should:

RECOMMENDATION 5

Discontinue the practice of categorizing all business data breaches as low risk. In addition, for data breaches categorized as high risk, issue a notification letter to the business and place the data breach indicator on the business tax account.

CORRECTIVE ACTION

We revised the Data Breach Response Plan to reflect that losses associated with a business are not automatically categorized as low risk. Additionally, since breach notification laws are specific to individuals at both the federal and state level, business notification is not required by the Office of Management and Budget, not done in private industry, and is not currently being done by other agencies. Nevertheless, depending on the circumstance, we will consider notification for business data losses categorized as high risk. However, placing a data breach indicator on business tax accounts would cause confusion as the indicator is tied to the loss of PII, which is not the case in a business loss. If a business-related loss is categorized as high risk and a notification letter is sent, a history item will be placed on the business account.

IMPLEMENTATION DATE

Implemented

RESPONSIBLE OFFICIAL

Chief Privacy Officer, Privacy Policy and Compliance, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN

N/A

Appendix III

Abbreviations

IRM	Internal Revenue Manual
IRS	Internal Revenue Service
PGLD/IM	Privacy, Governmental Liaison, and Disclosure/Incident Management
PII	Personally Identifiable Information
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number



**To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at
oi.govreports@tigta.treas.gov.**

**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.