TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Actions Were Not Always Taken to Protect Taxpayers Associated With Reported External Data Breaches

November 14, 2018

Reference Number: 2019-40-010

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.

Redaction Legend:
1 = Tax Return/Return Information

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

ACTIONS WERE NOT ALWAYS TAKEN TO PROTECT TAXPAYERS ASSOCIATED WITH REPORTED EXTERNAL DATA BREACHES

Highlights

Final Report issued on November 14, 2018

Highlights of Reference Number: 2019-40-010 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

Identity thieves continue to conduct more sophisticated fraud schemes using stolen tax information from employers and tax return preparers to file fraudulent returns that often mirror the actual taxpayer's return. To assist taxpayers and help protect them from tax-related identity theft, the IRS must distinguish the identity thieves' tax returns from returns filed by the taxpayers.

WHY TIGTA DID THE AUDIT

This audit was initiated to assess the effectiveness of IRS assistance to victims of external data breaches.

WHAT TIGTA FOUND

In response to the increasing number of data breaches, the IRS has taken many actions to inform external stakeholders on how to protect taxpayer information as well as actions to take if a data breach occurs. For example, the IRS developed and released tax tips, alerts, and news releases on its public website to educate stakeholders and the public on safeguarding taxpayer information and actions they should take if their systems have a data breach.

For Calendar Year 2017, the IRS's Return Integrity and Compliance Services (RICS) organization recorded 730 external data breaches on its Incident Management Tracker Matrix. However, our review identified that RICS analysts did not record and monitor 89 data breaches of external entities that were reported to the IRS. For 70 of these incidents, the RICS analysts did not request the external entity to provide the IRS with a list of stolen client Taxpayer Identification Numbers (TIN). The analysts should have also recorded these incidents on the tracker. In another four data breaches, the external entity declined to provide a TIN list. For these breaches, RICS analysts did not attempt to create a list of stolen TINs as required.

In addition, the external entity provided a TIN list for 15 data breaches but the RICS analysts did not record the incidents on the Incident Management Tracker Matrix. As a result, 11,406 Social Security Numbers associated with these breaches were not added to the IRS's Dynamic Selection List (DSL) to protect taxpayers from tax-related identity theft. For 79 of these Social Security Numbers, the taxpayers already experienced the burden of an identity thief using their Social Security Number to file a fraudulent Tax Year 2016 or 2017 return.

Our review also identified that RICS analysts did not add to the DSL, as required, all the TINs associated with 105 external data breach incidents recorded on the Incident Management Tracker Matrix in Calendar Year 2017.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS 1) record the 89 data breaches on the Incident Management Tracker Matrix and apply the appropriate treatment; 2) develop procedures to ensure that all reported data breaches are added to the Incident Management Tracker Matrix and ensure that RICS analysts add reported TINs to the DSL, if appropriate; 3) research the TINs that TIGTA identified as potentially not being on the DSL and add them, as appropriate; and 4) add the missing TINs that TIGTA identified to the DSL to allow detection of potential identity theft returns filed using the TINs.

The IRS agreed with all four recommendations. IRS management completed its review of referred TINs from data breaches and assigned applicable TINs to the appropriate treatment stream and the DSL. Additionally, IRS management is currently developing the Incident Management and Other DSL Treatments Database to replace the current method for updating, monitoring, and tracking incidents referred to the RICS function.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

November 14, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Actions Were Not Always Taken to Protect Taxpayers Associated With Reported External Data Breaches (Audit # 201740036)

This report presents the results of our review to assess the effectiveness of Internal Revenue Service (IRS) assistance to victims of external data breaches. This audit was included in our Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and IRS Employees.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services).

Table of Contents

Abbreviations

CY	Calendar Year
DDb	Dependent Database
DSL	Dynamic Selection List
IMP	Incident Management Plan
IRS	Internal Revenue Service
PII	Personally Identifiable Information
RICS	Return Integrity and Compliance Services
SSN	Social Security Number
TIN	Taxpayer Identification Number

Background

Safeguarding taxpayer data is a top priority for the Internal Revenue Service (IRS). Taxpayer data is defined as any information that is obtained or used in the preparation of a tax return (*e.g.*, income statements, notes taken in a meeting, or recorded conversations). Implementing safeguards to protect taxpayer data can help prevent identity theft as well as enhance confidence and trust in the IRS. Implementing strong safeguards is more important than ever as identity thieves continue to conduct more sophisticated fraud schemes using stolen tax information from employers and tax return preparers. Once the taxpayer's information is stolen, the identity thief uses it to file a fraudulent return that often mirrors the actual taxpayer's return. The IRS must then distinguish the identity thief's return from the returns filed by the legitimate taxpayer.

In Calendar Year (CY) 2015, the IRS brought together major organizations in the tax industry (*i.e.*, tax return preparers, software providers, State tax agencies, payroll providers, financial institutions) for its first annual Security Summit to increase cooperation to fight a common enemy – identity thieves. Tax return preparers are critical to this partnership, and because of the taxpayer information stored in their systems, they are increasingly a target for data theft. A data breach is the intentional or unintentional release or theft of secure taxpayer data. For example, a data breach involving the unauthorized access to tax return preparer tax data can result in refund fraud, taxpayer burden, and lost tax revenue. A data breach can also involve the improper disposal of Personally Identifiable Information (PII)[1] or a sophisticated cyberattack on corporate computers by criminals.

The IRS's Return Integrity and Compliance Services (RICS) organization plays a key role in addressing the risks associated with external data breaches through education, outreach, screening returns for identity theft, and preventing fraudulent refunds. For example, in response to the increased number of data breaches, the IRS established dedicated electronic mailboxes where data breaches can be reported to the IRS from both internal IRS functions and external entities. For example:

- **RICS Internal Mailbox** – Created for use by internal IRS functions to report data breaches received from external entities, including breaches at tax return preparer offices.
- **Dataloss Mailbox** – Created for use by businesses and payroll service providers to report Forms W-2, *Wage and Tax Statement*, data loss incidents. The mailbox address is dataloss@irs.gov, which is listed on the IRS public website.

[1] PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

- **Phishing Mailbox** – Created for use by businesses and individuals receiving unsolicited e-mails posing to be from a legitimate entity such as the IRS, financial institution, or software provider requesting personal and financial information. The mailbox address is phishing@irs.gov, which is listed on the IRS public website.

Stakeholder Liaison function provides assistance to external entities

The IRS's Stakeholder Liaison function field offices provide information about IRS policies, practices, and procedures and are the focal point for tax practitioners to report data breaches. For example, tax practitioners are directed to contact their Stakeholder Liaison function field office where an IRS employee will obtain basic information relating to the data breach they are reporting. The employee will also ask the tax practitioner to send, via encrypted e-mail, the names and Social Security Numbers (SSN) of potentially affected individual taxpayers and dependents as well as the Employer Identification Numbers if the breach includes business taxpayers. Once this information is received, the Stakeholder Liaison function field office will forward information relating to the reported incident to the RICS organization for treatment. Finally, the Stakeholder Liaison function employee will inform the practitioner that their Electronic Filing Identification Number[2] will be deactivated and to contact the IRS's Electronic Products and Services Support help desk to obtain a new one.

This review was performed at the Wage and Investment Division's RICS organization in Horsham, Pennsylvania; and the Stakeholder Liaison function in Little Rock, Arkansas; San Diego, California; Atlanta, Georgia; St. Louis, Missouri; Portland, Oregon; and Dallas, Texas, during the period August 2017 through August 2018. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[2] The Electronic Filing Identification Number is a six-digit number that the IRS assigns to an authorized e-File provider.

Results of Review

The IRS considers data breaches one of the top five risks currently facing tax administration. In response to the increasing number of breaches, the IRS has initiated a number of actions to inform external stakeholders on how to protect taxpayer information as well as actions to take if a data breach occurs. For example, the IRS has:

- Developed and issued Publication 4557, *Safeguarding Taxpayer Data*. This guide seeks to help tax professionals understand basic security steps, recognize the signs of data theft and how to report it, as well as how to respond to and recover from a data loss. The publication also includes steps to be taken to comply with the Federal Trade Commission Safeguards Rule.[3]
- Developed and released tax tips, alerts, and news releases on IRS.gov to educate stakeholders and the public on safeguarding taxpayer information and actions they should take if their systems have a data breach. The information includes tips on identifying phishing scams, methods to prevent data losses or identity theft, how to report incidents to the IRS, and victim assistance information. The IRS also provides specific guidance to tax return preparers to help them safeguard their Electronic Filing Identification Number against suspicious activity, develop a security plan, and educate employees on how to recognize phishing scams.
- Posted information about the Security Summit on IRS.gov. The Security Summit, convened in CY 2015, includes IRS officials, the Chief Executive Officers of leading tax preparation firms, software developers, payroll and tax financial product processors, and representatives from State Departments of Revenue. The purpose is to share information among participating organizations regarding detecting, deterring, and preventing tax-related identity theft. During CYs 2016 and 2017, Security Summit partners held three public awareness campaigns directed at taxpayers and tax professionals to identify steps they can take to protect themselves from identity thieves and cybercriminals.

The IRS also developed the RICS Incident Management Plan (IMP). The IMP includes information that is necessary to assist external entities that had a data breach as well as the steps the RICS organization Incident Management Team will take in response to the reporting of these incidents. For example, the IMP includes a description of how incidents are evaluated based on information gathered to develop the background of the incident and how the incident is scored

[3] Under the Safeguards Rule, financial institutions must protect the consumer information they collect. The Gramm-Leach-Bliley Act (Pub. L. No. 106-102) requires companies defined under the law as "financial institutions" to ensure the security and confidentiality of this type of information. The "financial institutions" definition includes professional tax return preparers.

based on the impact and number of affected taxpayers. The IMP outlines the RICS organization's roles and responsibilities for the incident management process. Figure 1 details these processes.

Figure 1: RICS Incident Management Processes

Incident Step	Process
Incident Identification	The RICS organization receives referrals of reported breaches (referred to as incidents by the RICS organization) from internal IRS functions and external entities. After receipt of the referral, RICS analysts review the incident details to accurately assess the incident risk and assign a treatment.
Control and Monitoring	All incidents referred to the RICS organization are tracked and monitored using the Incident Management Tracker Matrix. Specifically, reported incidents are logged into the matrix and assigned a control number that is used to track and monitor the actions taken by the RICS organization.
Incident Evaluation	The RICS organization uses the information related to the number of taxpayers affected and the impact of the incident to calculate an incident risk assessment score. All incidents referred to the RICS organization must include the following information: – Determination of whether the incident is new or an update to a prior incident. – Identification of the originator who referred the incident to the IRS. – Date of incident. – Date range of incident occurrence. – Impacted business units. – Impacted IRS systems. – Description of the data lost/compromised. – Confirmation of Identity Protection Personal Identification Number[4] status. – Number of known and potential taxpayers affected. – Mitigation actions taken to address the incident.
Assign Treatment	Based on the RICS organization calculated incident risk assessment score, the incident is addressed using one of the following treatment streams: – Ultra High – The IRS places the Taxpayer Identification Numbers (TIN)[5] associated with the incident on the Ultra High Dynamic Selection List (DSL)[6] and

[4] The Identity Protection Personal Identification Number is a single-use, six-digit number that is placed on an e-filed or paper return to allow tax-related identity theft victims from a prior year avoid delays in having their current year Federal tax return processed.
[5] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an Employer Identification Number, an SSN, or an Individual TIN.
[6] The DSL is used as a protective measure to select tax returns with stolen TINs for review by the Taxpayer Protection Program. This program gives the legitimate taxpayers an opportunity to authenticate before processing the returns.

Incident Step	Process
	in the Dependent Database (DDb).[7] The IRS rates the incident as high risk based on details such as taxpayers' Identity Protection Personal Identification Numbers being compromised in conjunction with Federal tax information and/or PII. The IRS defines high profile or sensitive PII as a breach that involves PII or sensitive but unclassified[8] information, and there is a potential impact to tax administration. – High – The IRS places the TINs on the High DSL and in the DDb. The incident risk assessment is rated as high but Identity Protection Personal Identification Numbers were not compromised. – Medium High –The IRS places the TINs on the Medium High DSL and in the DDb. Critical data loss occurred and the risk to tax administration is elevated. – Medium – The IRS places the TINs on the High Risk TIN List and in the Return Review Program.[9] The incident risk assessment is elevated and a more tailored treatment can be applied. – Low – The IRS does not place the TINs in the DDb or the Return Review Program. Instead, Fraud Referral and Evaluation analysts review tax returns with the TINs to identify suspicious patterns and trends that were not identified by the DDb or the Return Review Program. – Very Low – No treatment is needed. Evaluation of the incident indicates no impact to tax administration.

Source: RICS Incident Management Plan, dated September 8, 2017.

For CY 2017, the RICS organization used these processes to calculate an incident risk assessment score for the 730 external data breaches it recorded on its Incident Management Tracker Matrix.[10] However, our review identified that necessary actions were not always taken to protect taxpayers associated with all reported data breaches. For example, the IRS did not record and track all reported external data breaches. In addition, TINs associated with reported data breaches were not consistently placed on the DSL to detect fraudulent tax returns that identity thieves might file using the TINs.

[7] The DDb is a rules based selection application designed to identify potentially ineligible tax returns claiming the Earned Income Tax Credit and other refundable credits.
[8] Information if lost, stolen, misused, accessed, or altered without authorization may adversely affect the national interest or the conduct of Federal programs.
[9] The Return Review Program is the IRS's primary line of defense against tax fraud and noncompliance. This program helps stop identity theft refund fraud and other tax fraud schemes.
[10] The Incident Management Tracker Matrix is a spreadsheet used by the RICS organization to track and monitor incidents referred to it for treatment consideration.

Some Reported Data Breaches Were Not Recorded on the Incident Management Tracker Matrix

Our review identified that RICS analysts did not record and monitor 89 (17 percent) of 527 judgmentally[11] selected external data breaches that the IRS received in its data breach reporting mailboxes in CY 2017. These 527 e-mails each reported a data breach that should have been recorded and monitored on the Incident Management Tracker Matrix. For the 89 data breaches not recorded on the Incident Management Tracker Matrix, we determined that for:

- 70 data breaches – the RICS analyst did not ask the external entity to provide the IRS with a list of stolen TINs. Internal guidelines require RICS analysts to request the stolen TIN list from the external entity and record the data breach on the Incident Management Tracker Matrix. If a TIN list cannot be obtained, an analyst should still document the data breach on the Incident Management Tracker Matrix with the notation, "unable to secure taxpayer data." In addition, internal guidelines state that RICS analysts should attempt to create a list of stolen TINs by using information in the external entity's e-mail that reported the data breach, if appropriate. For example, if the entity is a tax return preparer who reports that his or her clients' TINs were stolen, the employee could create the TIN list by identifying tax returns filed under the tax return preparer's Preparer Tax Identification Number in the prior filing season.[12] None of these actions were taken by the RICS analysts.
- 15 data breaches – external entities provided the IRS with a TIN list but analysts failed to record the incident on the Incident Management Tracker Matrix. As a result, 11,406 SSNs associated with these breaches were not added to the DSL. For 79 of these SSNs, the taxpayers already experienced the burden of an identity thief using their SSN to file a fraudulent tax return. The thieves used the taxpayers' SSNs to file either a Tax Year[13] 2016 or 2017 return.
- 4 data breaches – the analysts *did* request the TIN list but the external entity declined to provide one. However, similar to the first bullet, once the external entity declined to provide the TIN list, RICS analysts did not attempt to create a list of stolen TINs as required.

The omission of the 89 data breaches from the Incident Management Tracker Matrix occurred primarily because RICS organization management did not establish a reconciliation process to

[11] We judgmentally selected the 527 e-mails from the universe of 3,486 e-mails in the IRS mailboxes used to receive reported data breaches from external entities. Many of the external entities' e-mails did not report a data breach; rather, the e-mails reflected back and forth correspondence between an external entity and IRS employees. A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[12] The period from January through mid-April when most individual income tax returns are filed.
[13] The 12-month accounting period for keeping records on income and expenses used as the basis for calculating the annual taxes due. For most individual taxpayers, the tax year is synonymous with the calendar year.

ensure that analysts record all data breaches received. In addition, management does not have a process to monitor the receipt of a TIN list or to ensure that when this list is not received RICS analysts attempt to create a list. Management stated that the Incident Management Tracker Matrix does not track whether a breach involves a TIN list received from the tax return preparer or if a RICS analyst attempted to create the list. As a result, the IRS did not monitor, evaluate, and assign a treatment for these data breaches, as required by the incident management process.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 1: Record the 89 data breaches on the Incident Management Tracker Matrix Record, calculate an incident risk assessment score for each incident, and apply the appropriate treatment for each incident. This includes requesting a list of TINs for those 70 breaches for which a TIN list was not provided.

> ***Management's Response:*** The IRS agreed with this recommendation. IRS management reviewed the 89 data breaches and assigned them to the appropriate treatment stream. The TINs associated with those breaches requiring treatment were added to the DSL based on the type of breach and the year it was reported.

Recommendation 2: Develop processes to ensure that all reported data breaches are added to the Incident Management Tracker Matrix. In addition, ensure that RICS analysts follow internal guidelines for adding reported TINS to the DSL, request the TIN list from external entities when they do not provide one, and attempt to develop a TIN list when an external entity declines to provide it, if appropriate.

> ***Management's Response:*** The IRS agreed with this recommendation. IRS management is reviewing and updating its guidelines as appropriate. Additionally, IRS management is developing the Incident Management and Other DSL Treatments Database, which will replace the current method for updating, monitoring, and tracking incidents referred to the RICS function.

Some Taxpayer Identification Numbers Associated With Reported Data Breaches Were Not Recorded on the Dynamic Selection List

Our review of 728[14] external data breach incidents, recorded on the Incident Management Tracker Matrix in CY 2017, identified that RICS analysts did not add to the DSL, as required, all the TINs associated with 105 (14 percent) of the incidents. RICS management did not implement a process to ensure RICS analysts add all TINs associated with data breach incidents

[14] Two of the 730 external data breaches recorded on the Incident Management Tracker Matrix in CY 2017 were not scored high enough by the IRS to warrant placement on the DSL.

to the DSL. As a result, the IRS will not identify tax returns filed using the TINs not added to the DSL to ensure that the legitimate taxpayer filed the tax return. Specifically, we identified:

- 97 data breaches in which there was a discrepancy between the number of TINs associated with the data breach compared to the number of TINs cited as being added to the DSL. For example, our review of documentation prepared by RICS analysts identified that 147,123 TINs were associated with these 97 breaches but only 119,012 were added to the DSL. Thus, 28,111 TINs may not have been added to the DSL.
- 8 data breaches that RICS analysts scored as Ultra High, High, or Medium High risk but did not add the TINs to the DSL. Consequently, many of the 2,976 TINs affected by these data breaches were not subject to the DDb filters to detect fraudulently filed tax returns during tax return processing.

The process for placing TINs on the DSL involves two manual processes:

- RICS analysts place the TINs for an external data breach on a master spreadsheet for data breaches that are assigned an Ultra High, High, or Medium High treatment.
- Another employee accesses the master spreadsheet, creates a separate file, and initiates a program to load the TINs on the DSL.

When we discussed our results with RICS management they stated that one reason why the number of TINs on the Incident Management Tracker Matrix may differ from the number on the DSL is that some TINs may have previously been added to the DSL. To validate management's claim we examined in-depth **********1**********1**********1**********1********** and identified 185 TINs were in fact not on the DSL. Therefore, an additional 27,270[15] TINs are potentially not on the DSL *******1*******1****** in which the number of TINs on the Incident Management Tracker Matrix differs from the number on the DSL.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 3**:** Research the 27,270 TINs and the 2,976 TINS we identified as potentially not being on the DSL to determine if they were previously added, and for those not added, include them on the DSL.

[15] **********1**********1**********.

Management's Response: The IRS agreed with this recommendation. IRS management completed a 100 percent TIN analysis that identified 15,143 unique TINs that had not been assigned a treatment. Upon completion of the analysis, the untreated TINs were assessed and assigned to a treatment steam. The TINs were also added to the appropriate DSL based on the type of breach and the year reported.

Recommendation 4***:*** Add the 185 TINs that we identified to the DSL to allow detection of potential identity theft returns filed using the TINs.

Management's Response: The IRS agreed with this recommendation. IRS management evaluated the identified TINs and placed them on the appropriate DSL based on the type of breach and the year reported.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness of IRS assistance to victims of external data breaches. To accomplish this objective, we:

I. Determined if the IRS proactively provided outreach and support to prevent external data breaches of taxpayer information.

   A. Assessed IRS actions to proactively educate external stakeholders and the public on safeguarding taxpayer information.

   B. Determined if information provided to internal IRS sources was accurate and distributed effectively to promote the safeguarding of taxpayer information.

   C. Evaluated the sufficiency of the RICS IMP for tracking and evaluating reported external data breaches.

II. Determined if the IRS provided sufficient assistance to victims of reported external data breaches of taxpayer information.

   A. Identified the various sources used to report an external data breach and assessed the IRS's actions to process the incidents.

   B. Evaluated the RICS organization incident scoring and treatment methodology to protect tax revenue and identify future fraudulent tax returns.

   C. Obtained reported external data breach incidents for CY 2017, selected a judgmental[1] sample of 527 e-mails from the universe of 3,486 e-mails[2] located in the IRS's mailboxes reporting a data breach, and determined if the incidents were accurately recorded in the Incident Management Tracker Matrix.

   D. Determined if the RICS organization properly scored and treated incidents recorded in the Incident Management Tracker Matrix.

Data validation methodology

During this review, we relied on the e-mails provided to us by the IRS from the established dedicated electronic mailboxes where external data breaches can be reported to the IRS. The IRS also provided us with the Incident Management Tracker Matrix spreadsheet for CY 2017,

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[2] Many of the external entities' e-mails did not report a data breach; rather, the e-mails reflected back and forth correspondence between an external entity and IRS employees.

which the IRS used to record data breaches, as well as the DSL[3] Access database for CY 2017, which it used to ensure that it placed the TINs[4] affected by the data breach into the DDb[5] for treatment. Before relying on the data, we performed analyses to evaluate the validity and reasonableness of the information found in the data sources. We also traced the data breaches reported via e-mail to the RICS organization, to the Incident Management Tracker Matrix, the DSL, and to the DDb to ensure that each of the data sources were complete. Based on the results of this testing, we believe that the data used in our review were reliable.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: processes to ensure that the IRS provided sufficient outreach to inform the public on how to report data breaches to the IRS and controls over the IRS procedures to record, evaluate, and treat the reported data breaches and associated TINs. We tested these controls by evaluating the IRS' outreach activities and traced the data breaches reported to the IRS via e-mail to the Incident Management Tracker Matrix, the DSL, and the DDb to ensure that the IRS accounted for all incidents and scored and treated each incident according to its guidelines.

[3] The DSL is used as a protective measure to select tax returns with stolen TINs for review by the Taxpayer Protection Program. This program gives legitimate taxpayers an opportunity to authenticate before processing the returns.
[4] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an Employer Identification Number, an SSN, or an Individual TIN.
[5] The DDb is a rules based selection application designed to identify potentially ineligible tax returns claiming the Earned Income Tax Credit and other refundable credits.

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Allen Gray, Director
Van Warmke, Acting Audit Manager
Audrey Graper, Lead Auditor
David Robben, Senior Auditor
Nikole Smith, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Services and Enforcement
Commissioner, Wage and Investment Division
Chief, Communications and Liaison
Director, Return Integrity and Compliance Services, Wage and Investment Division
Director, Return Integrity Operations, Wage and Investment Division
Director, Stakeholder Liaison Field, Communications and Liaison
Director, Office of Audit Coordination

Appendix IV

Outcome Measures

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

Type and Value of Outcome Measure:

Reliability of Information – Potential; 89 external data breaches not recorded on the Incident Management Tracker Matrix (see page 6).

Methodology Used to Measure the Reported Benefit:

We obtained 3,486 e-mails located in the IRS's mailboxes used to receive reported data breaches from external entities. We judgmentally[1] selected a sample of 527 e-mails that reported data breaches from the universe of 3,486 e-mails.[2] We then compared the 527 e-mails associated with a data breach to the RICS Incident Management Tracker Matrix to determine if the RICS organization properly recorded all data breaches. We found that 89 (17 percent) were not recorded and monitored on the Incident Management Tracker Matrix.

Type and Value of Outcome Measure:

Taxpayer Rights and Entitlements – Potential; 11,406 taxpayers' SSNs that were received from an external entity reporting a data breach but were not loaded to the DSL (see page 6).[3]

Methodology Used to Measure the Reported Benefit:

For 15 of the 89 data breaches not recorded and monitored on the Incident Management Tracker Matrix, we determined that the external entity provided the IRS with a TIN[4] list. As a result, 11,406 SSNs associated with these breaches were not added to the DSL to protect taxpayers from tax-related identity theft. For 79 of these SSNs, the taxpayers already experienced the burden of

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[2] Many of the external entities' e-mails did not report a data breach; rather the e-mails reflected back and forth correspondence between an external entity and IRS employees.
[3] The DSL is used as a protective measure to select tax returns with stolen TINs for review by the Taxpayer Protection Program. This program gives legitimate taxpayers the opportunity to authenticate before processing the returns.
[4] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an Employer Identification Number, an SSN, or an Individual TIN.

an identity thief using their SSN to file a fraudulent tax return. The thieves used the taxpayers' SSNs to file either a Tax Year[5] 2016 or 2017 return.

Type and Value of Outcome Measure:

Taxpayer Rights and Entitlements – Potential; 185 taxpayers whose TINs were received from an external entity reporting a data breach but were not loaded to the DSL (see page 7).

Methodology Used to Measure the Reported Benefit:

We determined that RICS analysts did not add to the DSL all TINs associated with 97 reported data breaches. For example, analysts recorded that 147,123 TINs were associated with these 97 breaches but added only 119,012 of the TINs to the DSL. Thus, 28,111 TINs may not have been added to the DSL. RICS organization management stated that one reason the number of TINs on the Incident Management Tracker Matrix may differ from the number on the DSL is because the DSL process bypasses TINs that are already on the DSL. However, this explanation does not explain the missing TINs. **********1**********1**********1**********. Therefore, 185 TINs received from the external entity were not loaded to the DSL.

[5] The 12-month accounting period for keeping records on income and expenses used as the basis for calculating the annual taxes due. For most individual taxpayers, the tax year is synonymous with the calendar year.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

October 26, 2018

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kenneth C. Corbin
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – Actions Were Not Always Taken to Protect Taxpayers Associated With Reported External Data Breaches (Audit # 201740036)

Thank you for the opportunity to review the subject draft report and provide comments. Taxpayers, tax professionals, and businesses are increasingly being targeted for purposes of stealing individuals' personally identifiable information (PII) that can be used to file fraudulent tax returns. As the IRS has enhanced and improved its fraud detection processes, criminals have also improved their level of sophistication in attacking the custodians of PII. Having the ability to thoroughly impersonate legitimate taxpayers is one method by which fraudsters attempt to defeat our detection systems and commit identity theft (IDT)-related refund fraud.

We recognize that IDT tactics are continually evolving and exist in a dynamic environment. To counter these ever-changing schemes, we have taken a number of steps to prevent the victimization of taxpayers, protect their data, and assist those who ultimately are victimized. Some of these actions include:

- Established an Incident Management Plan that documents the actions to be taken when a third-party tax-related data loss occurs or is reported.
- Developed processes for monitoring taxpayer and business accounts that have been identified as being a victim of a tax-related data loss.
- Developed processes to assist tax practitioners who report they are victims of a tax-related data loss, or whose credentials were compromised.

- Established dedicated mailboxes, Dataloss@irs.gov and Phishing@irs.gov, for businesses and individual taxpayers to report they have been victims of email phishing schemes.

Additionally, we increased our outreach efforts to educate taxpayers, tax professionals, and businesses. Some of these communications include:

- Updated, and continue to update, IRS.gov with timely guidance on how individuals may report they have been victims of tax-related data compromises.
- Published IRS Newswire articles and Fact Sheets.
- Launched the "Protect Your Clients, Protect Yourself" campaign and the "Don't Take the Bait" series.
- Provided informational seminars during the annual Nationwide Tax Forums.

We have made great strides in providing awareness and assisting victims of external data breaches, but more opportunities exist. The report findings state there were external data breaches reported to the IRS that were not treated. We agree there were reported breaches that either were not treated or should have been reviewed further for potential treatment; however, we do not agree with the number of untreated breaches cited. For example, the report concludes that in cases where the victimized entity does not provide the data needed to identify all exposed individuals, the IRS should create the list using other information we may have associated with the entity, such as identifying individuals for whom that entity prepared tax returns in the past. We do not agree with that assessment. Creating a list of potentially impacted taxpayers based on data internal to the IRS, such as historical filings, is not always appropriate. When a practitioner reports that several returns were filed using their compromised credentials, and none of the returns filed were for their clients, it would not be beneficial or effective to create a list of clients when there are no indications their actual clients were impacted.

The report also refers to reported Taxpayer Identification Numbers (TINs) that were not assigned to treatment streams. The methodology used to reach this conclusion considered each incident, determined the cumulative count of TINs identified for each incident, and compared that number to the total number of TINs assigned a treatment. The methodology does not consider that some TINs have been involved in multiple incidents and were reported to the IRS more than once. We identified approximately 12,000 TINs involved in multiple incidents. Once protected, there is no additional benefit derived from duplicate protections.

We appreciate the identification of opportunities for improving how we evaluate and treat reported external data breaches. As a result of this review we are automating many of the manual processes that led to the issues identified in this report. We also

note that the Incident Management Processes shown as Figure 1 in the report was revised and updated for 2018.

Attached are our comments and proposed actions to your recommendations. If you have any questions, please contact me or a member of your staff may contact Michael Beebe, Director, Return Integrity and Compliance Services (RICS), Wage and Investment Division at 470-639-3250.

Attachment

Attachment

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1
Record the 89 data breaches on the Incident Management Tracker Matrix Record, calculate an incident risk assessment score for each incident, and apply the appropriate treatment for each incident. This includes requesting a list of TINs for those 70 breaches for which a TIN list was not provided.

CORRECTIVE ACTION
We agree with this recommendation. We have reviewed the 89 data breaches and, when applicable, assigned them to the appropriate treatment stream. The Taxpayer Identification Numbers (TINs) associated with those breaches requiring treatment, and in consideration of the type of breach and the year it was reported, were added to the dynamic selection list (DSL). The review was completed on September 7, 2018.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, Return Integrity and Compliance Services (RICS), Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 2
Develop processes to ensure that all reported data breaches are added to the Incident Management Tracker Matrix. In addition, ensure that RICS analysts follow internal guidelines for adding reported TINS to the DSL, request the TIN list from external entities when they do not provide one, and attempt to develop a TIN list when an external entity declines to provide it, if appropriate.

CORRECTIVE ACTION
We agree with this recommendation. Our guidelines are being reviewed and are being updated as appropriate. Additionally, we are developing the Incident Management and Other DSL Treatments Database, which will replace the current method for updating, monitoring, and tracking incidents referred to the RICS function.

IMPLEMENTATION DATE
April 15, 2019

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, Return Integrity and Compliance 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
Research the 27,270 TINs and the 2,976 TINS we identified as potentially not being on the DSL to determine if they were previously added, and for those not added include them on the DSL.

CORRECTIVE ACTION
We agree with this recommendation. On September 7, 2018, we completed a 100 percent TIN level analysis that identified 15,143 unique TINs that had not been assigned a treatment. Upon completion of the analysis, the untreated TINs were assessed and assigned to a treatment stream. They were also added to the appropriate DSL based on the year the breach was reported and the type of reported data breach.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 4
Add the 185 TINs that we identified to the DSL to allow detection of potential identity theft returns filed using the TINs.

CORRECTIVE ACTION
We agree with this recommendation. The identified TINs were evaluated and, based on the type of breach and the year reported, were placed on the appropriate DSL. This was completed on September 7, 2018.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Return Integrity Operations, Return Integrity and Compliance Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A