TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Internal Revenue Service Did Not Identify and Assist All Individuals Potentially Affected by the Get Transcript Application Data Breach

May 16, 2016

Reference Number: 2016-40-037

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:
2 = Risk Circumvention of Agency Regulation or Statute

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.

THE INTERNAL REVENUE SERVICE DID NOT IDENTIFY AND ASSIST ALL INDIVIDUALS POTENTIALLY AFFECTED BY THE GET TRANSCRIPT APPLICATION DATA BREACH

Highlights

Final Report issued on May 16, 2016

Highlights of Reference Number: 2016-40-037 to the Internal Revenue Service Commissioner for the Wage and Investment Division.

IMPACT ON TAXPAYERS

The IRS Get Transcript application allows taxpayers to view and download their tax information on the IRS public website. On May 21, 2015, the IRS removed this application from its website after discovering it was being used for unauthorized accesses to taxpayer data. The IRS believes that some of this information may have been gathered to file fraudulent tax returns.

WHY TIGTA DID THE AUDIT

This audit was conducted to evaluate IRS identification and assistance to victims of the Get Transcript application breach. Assistance includes sending potential victims a notification letter and marking their accounts with an identity theft incident marker.

WHAT TIGTA FOUND

The IRS did not identify all individuals potentially affected by the Get Transcript application breach. Our analysis of system audit logs created between January 1, 2014, and May 21, 2015, identified 620,931 taxpayers whose tax account information involved a potentially unauthorized access not identified by the IRS. Further analysis of these access attempts found that potentially unauthorized users were successful in obtaining access to 355,262 of the taxpayers' accounts.

TIGTA also identified 2,470 additional taxpayers whose accounts were targeted through the Get Transcript application breach that the IRS did not identify. This resulted from the IRS erroneously excluding three system error codes when identifying accounts of potential victims.

In addition, the IRS did not place identity theft incident markers on the tax accounts of 3,206 taxpayers who the IRS identified as affected by the Get Transcript application breach. After TIGTA questioned the IRS's rationale for not placing the marker on all tax accounts, management agreed that all affected taxpayer accounts need the marker. As a result, IRS officials informed us that they would ensure that all affected taxpayer accounts receive the identity theft marker.

Finally, the IRS did not offer an Identity Protection Personal Identification Number (IP PIN) or free credit monitoring to 79,122 individuals whose tax accounts the IRS identified as being involved in an attempted access.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS:
1) implement additional evaluative methods to identify all individuals affected by the breach;
2) issue notification letters to 620,931 taxpayers whose accounts were potentially targeted and place identity theft incident markers on their accounts; 3) ensure that authentication system error codes are analyzed when responding to future data breaches as well as notify the additional 2,470 taxpayers identified and place identity theft incident markers on their accounts;
4) place identity theft incident markers on the 3,206 taxpayer accounts, as required; and
5) issue IP PINs to the 79,122 individuals whose personal information was used by unauthorized individuals to attempt access to the Get Transcript application.

The IRS agreed with seven of the eight recommendations. The IRS disagreed with the recommendation to issue IP PINs to the 79,122 individuals with attempted accesses to their tax information. Although it disagreed with the recommendation, it acknowledged the potential inconsistency in its IP PIN issuance policy and stated that it would consider this inconsistency in future IP PIN policy decisions. TIGTA is concerned that the lack of prompt action on this issue leaves these taxpayers' accounts at an increased risk of fraud.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

May 16, 2016

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Did Not Identify and Assist All Individuals Potentially Affected by the Get Transcript Application Data Breach (Audit # 201540027)

This report presents the results of our review to evaluate Internal Revenue Service (IRS) identification and assistance provided to victims of the Get Transcript application data breach. This audit addresses the major management challenges of Security for Taxpayer Data and IRS Employees, and Providing Quality Taxpayer Service Operations.

Management's complete response to the draft report is included in 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

CSIRC	Computer Security Incident Response Center
IP PIN	Identity Protection Personal Identification Number
IRS	Internal Revenue Service
OCA	Office of Compliance and Analytics
PII	Personally Identifiable Information
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number

Background

The Internal Revenue Service (IRS) deployed the Get Transcript application on its public website (www.IRS.gov) in January 2014. This application allows taxpayers to view and download their tax information, such as account transactions, line-by-line tax return information, and income reported to the IRS. Taxpayers can download or print five distinct transcript types: tax account, tax return, record of account, wage and income, and verification of nonfiling. From October 1, 2014, through April 15, 2015, the IRS provided 23 million transcripts to individuals using the Get Transcript application. Some transcripts include the taxpayer's personal information and the personal information of other individuals reported on the taxpayer's tax return, including names and Social Security Numbers (SSN) of dependents, a day care provider, or a former spouse receiving alimony.

The Get Transcript application was accessed by unauthorized users

The IRS used a multistep authentication process to verify the identity of Get Transcript application users before they could access their tax information. This process required users to:

- Provide a valid e-mail address to access their transcripts as a guest user or create an online account. The IRS e-mailed a confirmation code to the e-mail address input by the users. The users must receive and use this code to access their transcripts.
- Input five pieces of Personally Identifiable Information (PII)[1] –********2***** **********2**********.
- Answer "out of wallet" questions that only the taxpayers should know, such as **2*** **********2******.

On May 14, 2015, the IRS Computer Security Incident Response Center (CSIRC) identified a significant number of undeliverable e-mails sent by the online authentication system. These e-mails were the confirmation code e-mails that the system sends individuals attempting to establish an online account. The CSIRC reported the backlog of undeliverable e-mails to the Information Technology organization's Cybersecurity function. Cybersecurity function officials reviewed these e-mails and provided the Office of Compliance and Analytics (OCA) information on 59 suspicious domains[2] that generated the e-mails.

The Cybersecurity function deemed the domains suspicious because they met the established criteria for a suspicious domain. For example, multiple domains were registered to the same

[1] Any information that, either alone or in combination with other information, can be used to uniquely identify an individual.
[2] A domain refers to the name assigned to a computer, service, or any resource connected to the Internet.

person using the same foreign name and address, and some domains were registered out of the same data center.[3] The OCA used these 59 suspicious domains to then analyze access attempts to the Get Transcript application. Based on its results, the IRS removed the application from its website on May 21, 2015. The IRS concluded that one or more individuals succeeded in clearing an authentication process that required knowledge of information about the taxpayer, including **********2**********. It appeared that these unauthorized users had access to private personal information that allowed them to correctly answer questions which typically only the taxpayer would know.

In a separate review,[4] we found that when the IRS assessed the risk of the Get Transcript application, it rated the authentication risk associated with the Get Transcript application as low to both the IRS and taxpayers. As a result, the IRS implemented single-factor authentication to access the Get Transcript application. The IRS now knows that the authentication risk was in fact high to both the IRS and taxpayers and it should have required multifactor authentication. The IRS anticipates having the technology in place for multifactor authentication capability in the spring of 2016 to relaunch the Get Transcript application.

Identification of affected taxpayers

To identify taxpayers affected by the Get Transcript application breach, the OCA analyzed a variety of data sources, including system audit logs[5] and data from a credit monitoring agency used to administer the out-of-wallet questions. Using its data sources, the OCA determined that unauthorized individuals used 12 of the 59 suspicious domains to attempt 224,688 accesses to taxpayer data using the Get Transcript application and that the remaining 47 domains were not associated with the unauthorized access attempts. The OCA also reported that 124,870 of the 224,688 accesses were successful. Generally, a successful access involved either an individual creating an online account or an individual signing on as a guest user who provided the five initial pieces of taxpayer PII[6] and correctly answered the out-of-wallet questions.[7] The remaining 99,818 attempts were performed by individuals who were unable to correctly input the taxpayer's PII and/or correctly answer the out-of-wallet questions or who were unable to access the system due to a system error. Figure 1 shows the unauthorized attempts to gain access to the Get Transcript application and taxpayers' accounts.

[3] A virtual location, physical building, or portion of a building whose primary function is to house a computer room and its support areas; data centers typically contain high-end servers and storage products within mission-critical functions.
[4] Treasury Inspector General for Tax Administration, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).
[5] An audit log is a chronological record of system activities that allows for the reconstruction, review, and examination of a transaction from inception to final results.
[6] The IRS refers to the five pieces of PII as Level of Access C, which is a level of assurance known as Single-Factor Identification or Basic Identity (ID) Proofing.
[7] The IRS refers to the out-of-wallet questions as Level of Access D, which is a level of assurance known as Knowledge-Based Authentication.

Figure 1: Attempts to Gain Unauthorized Access to the Get Transcript Application

Access Attempts	Input of Five Pieces of PII		Answering Out of Wallet Questions	
	Pass	Fail	Pass	Fail
224,688	151,943	72,745		
151,943			124,870	27,073

Source: Analysis of data provided by the IRS on June 11, 2015.

After identifying the first group of 224,688 taxpayers on May 17, 2015, the IRS expanded its analysis to include e-mail addresses that individuals used to attempt access to these same taxpayer accounts. For example, if @mouse.com, a suspicious domain, was used to attempt access to an account, the IRS determined if this account had additional attempted accesses by individuals using e-mail addresses, *e.g.*, johnsmith@gmail.com. The IRS then identified other accounts in which the johnsmith@gmail.com e-mail address was used in an attempted access. The IRS believes these e-mail addresses are suspicious because they were used to attempt access to an account targeted by a suspicious domain and another taxpayer's account. Thus, the IRS determined that the accounts accessed by these e-mail addresses were targeted and potentially breached by unauthorized individuals.

On August 17, 2015, the IRS reported that it identified approximately 390,000 taxpayer accounts targeted by suspicious e-mail addresses, and for about 220,000 of these accounts, potentially unauthorized individuals successfully gained access and viewed the taxpayers' personal tax information.

The Office of Management and Budget requires agencies to notify victims after a data loss incident

The Office of Management and Budget requires agencies to implement data loss and incident management procedures to notify individuals after a data loss incident if the incident results in a high risk of harm to the individuals. The Get Transcript application breach can lead to significant harm for taxpayers and other individuals whose PII was accessed by the unauthorized individuals. The IRS believes that some of this information may have been gathered to file fraudulent tax returns. This information can enable an identity thief to file a fraudulent tax return that more closely resembles a legitimate tax return, making it more difficult for the IRS to detect.

To mitigate this burden, the IRS created five distinct letters to notify individuals affected by the Get Transcript application breach. The letters notified them that unauthorized individuals used their PII to attempt or gain access to their tax information. Figure 2 describes the letters that the IRS mailed to taxpayers.

Figure 2: Letters Mailed to Taxpayers Affected by the Get Transcript Application Data Breach

Letter 4281-	Description
A	*Get Transcript Incident - Impacted Taxpayer* – informs taxpayers that the IRS recently learned that fraudsters used their PII (obtained from another source) to view their tax information via the Get Transcript application. The letter also states that the IRS arranged free credit monitoring for the taxpayer from the Equifax credit monitoring agency and that the taxpayer can request an Identity Protection Personal Identification Number (IP PIN).[8] This letter provides the IRS Identity Theft telephone number for taxpayers to call if they have questions.
B	*Get Transcript Incident - Non-Impact Letter* – informs taxpayers that their accounts were targeted but access was not gained, *i.e.*, the criminal was unable to input the taxpayer's PII or correctly answer the out-of-wallet questions. These letters notify taxpayers that third parties appear to have had access to the taxpayer's SSN and additional personal financial information prior to the unauthorized access attempt. This letter also provides the IRS's Identity Theft telephone number for taxpayers to call if they have questions.
E	*Get Transcript Incident - Impacted Minors Letter* – informs the parent of a dependent(s) that the dependent(s) SSN, listed on the parent's tax return, was accessed by unauthorized individuals and subject to misuse. Because credit reporting agencies usually do not maintain credit files on minor children, the letter advises the parent to contact the Equifax credit monitoring agency to determine if a credit report exists for their dependent(s) and suggests actions the parent can take to protect the identity of the minor child. This letter also provides the IRS's Identity Theft telephone number.
F	*Get Transcript Incident - Alimony Spouse-Other* – informs taxpayers that they are eligible to request an IP PIN from the IRS to protect their tax account and that they are eligible for free credit monitoring. This letter is sent to taxpayers whose SSNs were disclosed indirectly via the Get Transcript application incident, such as alimony recipients' SSNs that the primary taxpayer listed on his or her tax return. This letter provides the IRS's Identity Theft telephone number.
G	*Exposed Taxpayer Identification Number,*[9] *Access to Account Data* – informs taxpayers that they are eligible to request an IP PIN from the IRS to protect their tax account and that they are eligible for free tax credit monitoring from the Equifax credit monitoring agency. This letter is sent to taxpayers whose PII was obtained from a source outside the IRS to view their tax information via the Get Transcript application. It also provides the IRS's Identity Theft telephone number.

Source: Treasury Inspector General for Tax Administration's (TIGTA) review of Get Transcript notification letters.

[8] The IP PIN is a six-digit, single-use identification number that the IRS issues to some taxpayers and uses to validate a taxpayer's identity and for security purposes.
[9] The TIN is 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 Taxpayer Identification Number.

IRS officials stated that the letters were mailed to the address maintained in the IRS Individual Master File.[10]

In addition to issuing the notification letters, the IRS marked affected taxpayer tax accounts with an indicator that would alert employees assisting a taxpayer that the taxpayer's account was targeted or breached using the Get Transcript application. The IRS also flagged the accounts to protect them from an identity thief filing a fraudulent tax return using their SSN. For example, the IRS will scrutinize future tax returns received with these SSNs to ensure that the taxpayer, not an identity thief, filed the return, prior to updating the taxpayer's account. These markers also include one of two incident numbers to enable employees to distinguish between the accounts that unauthorized individuals attempted to access and accounts that unauthorized individuals successfully accessed. Employees who answer the IRS's telephones can access the taxpayers' accounts and refer to the markers and incident numbers while assisting taxpayers who call with questions about their letter.

Impact of the Get Transcript application breach on tax administration

The IRS determined that of the 124,870 successful accesses, unauthorized individuals successfully obtained a tax transcript in 113,383 of the access attempts (a tax transcript was not viewed in the remaining 11,487 access attempts). For the 113,383 SSNs used in these accesses, 95,181 tax returns were filed in Processing Year[11] 2015 as of November 30, 2015. The IRS determined that 59,970 of these returns warranted review because they were filed after the account was breached through the Get Transcript application. IRS analysis of these returns identified:

- 34,201 tax returns[12] that were detected and treated as likely identity theft. The IRS prevented a total of $119,026,062 in refunds claimed on these returns.
- 22,318 tax returns that were not treated as identity theft. The IRS paid a total of $62,196,854 in refunds claimed on these returns.
- 2,869 tax returns that were likely filed by the innocent taxpayer because the returns report either a balance due or a zero amount owed, *i.e.*, the returns do not claim a refund.
- 582 tax return filings that the IRS was still examining at the end of our review.

This review focused on the IRS's identification of accounts potentially breached and assessed the assistance provided to the 224,688 taxpayers identified as of May 17, 2015. This review was performed at the OCA in Washington, D.C., and in the Information Technology organization's offices in Atlanta, Georgia; Lanham, Maryland; and Dallas, Texas, during the period June 2015 through January 2016. We conducted this performance audit in accordance with generally

[10] The IRS database that maintains transactions or records of individual tax accounts.
[11] The calendar year in which the tax return or document is processed by the IRS.
[12] For 167 of the 34,201 returns identified, the IRS did not prevent $446,608 in refunds claimed on those returns.

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.

Results of Review

Many Taxpayers Potentially Affected by the Get Transcript Application Data Breach Were Not Identified

Our analysis of system access logs created between January 1, 2014, and May 21, 2015, identified 620,931 taxpayers whose tax account information involved a potentially unauthorized access not identified by the IRS. Further analysis of these access attempts found that potentially unauthorized users successfully obtained access to 355,262 of the taxpayers' accounts[13] and obtained a transcript. It should be noted that the actual number of individuals whose personal information was available to the potentially unauthorized individuals accessing these tax accounts is significantly larger because these tax accounts include information on other individuals listed on a tax return (*e.g.*, spouses and dependents). The 620,931 accounts[14] with a potentially unauthorized access include:

- 609,951 accounts for which the same e-mail address was used in an attempt or successfully to access 10 or more different accounts. We determined that for 351,315 taxpayers, their accounts were successfully accessed by unauthorized individuals.
- 17,077 accounts for which four or more different e-mail addresses were used in an attempt to access the account. We determined that for 6,395 taxpayers, their accounts were successfully accessed.
- 68 accounts for which e-mail addresses used involved questionable characters within the e-mail address. We determined that for 39 taxpayers, their accounts were successfully accessed.

Many of the above 620,931 taxpayers with potentially unauthorized accesses remained unaware that their tax information may have been stolen and that they were at a heightened risk of future identity theft. Our analysis determined that 172,326 (28 percent) of these taxpayers have been further victimized. The IRS placed an identity theft marker on their accounts between January 2, 2014, and January 18, 2016, indicating that they are a confirmed identity theft victim or the taxpayer notified the IRS that they are a victim and provided supporting information.

[13] While the total number of accessed bulleted accounts on this page is 357,749 accounts (351,315+6,395+39), there are 2,487 accounts that are included in both the 351,315 and 6,395 bulleted accounts. Thus, the number of unique accounts successfully accessed is 355,262 (357,749–2,487).

[14] While the total number of bulleted accounts on this page with suspicious characteristics is 627,096 accounts (609,951+17,077+68), there are 6,165 accounts that are included in both the 609,951 and the 17,077 bulleted accounts. Thus, the number of unique accounts with suspicious characteristics is 620,931 (627,096–6,165).

Analysis of system audit logs identified that e-mail addresses used to access multiple taxpayer accounts were not identified by the IRS as suspicious

Our analysis of system audit logs between January 1, 2014, and May 21, 2015, identified 943,094 taxpayer accounts that had suspicious access attempts. We determined that these account access attempts were suspicious because they involved an e-mail address that was used to attempt access to 10 or more different taxpayer accounts. The IRS identified 333,143 of the 943,094 accounts as part of its initial and expanded effort to identify victims. The IRS did not identify the remaining 609,951 accounts. Of these accounts, potentially unauthorized individuals successfully obtained tax transcripts for 351,315 accounts. Figure 3 provides the number of accounts accessed[15] by an individual using an e-mail address that was used to target 10 or more other accounts.

Figure 3: Number of Taxpayer Accounts Accessed by an E-Mail Address That Was Used to Target 10 or More Other Accounts

Taxpayer Accounts Accessed by E-Mail Address	E-Mail Addresses	Taxpayer Accounts Accessed	Accounts Identified by the IRS	Accounts Not Identified by the IRS
10 to 20	13,904	189,489	26,944	162,545
21 to 50	6,889	213,349	39,796	173,553
51 to 100	2,161	149,657	40,667	108,990
101 to 250	1,322	202,718	91,414	111,304
251 to 500	468	165,153	104,512	60,641
501 to 1,000	141	91,847	62,194	29,653
More Than 1,000	28	36,072	30,717	5,355
Unique TINs[16]		**943,094**	**333,143**	**609,951**

Source: TIGTA analysis of authentication system audit logs and OCA analysis of e-mail addresses used to access Get Transcript application audit logs.

[15] For purposes of Figure 3, the term "accessed" refers to access attempts and successful accesses.
[16] Total unique TINs (accounts) for which an e-mail address was used to attempt access and the same e-mail address was used to attempt access to 10 or more accounts. Some accounts had an access attempt by an individual(s) using more than one e-mail address. Thus, the columns in this table cannot be summed.

After we identified the suspicious taxpayer account accesses in Figure 3, IRS officials stated that they would analyze these accounts and take appropriate actions such as placing identity theft incident markers on the taxpayers' accounts and issuing notification letters. The IRS completed its analysis and announced on February 26, 2016, that it would begin taking these actions. In addition, the officials stated they did not previously identify the suspicious access attempts that we found because the accesses, although unusual, were a single-factor characteristic, which they believe is rarely sufficient to distinguish between identity theft and non–identity theft behavior.

IRS officials also informed us that they modified the online authentication system in July 2015 to prevent an e-mail address from being used to access more than one account through the Get Transcript application. In addition, the officials stated that once the Get Transcript application is brought back online, the authentication system will be stronger. For example, guest access will be eliminated.

Analysis of system audit logs identified accounts accessed by multiple individuals, but the accesses were not identified by the IRS as suspicious

Our analysis of Get Transcript application audit logs created between January 1, 2014, and May 21, 2015, identified 208,721 taxpayer accounts that had suspicious access attempts. We determined these account access attempts were suspicious because these accounts had access attempts associated with four or more different e-mail addresses. The IRS identified 191,644 accounts as having been potentially breached. The remaining 17,077 accounts were not identified by the IRS. For 6,395 of the 17,077 accounts, we determined that potentially unauthorized individuals successfully accessed the account and obtained a tax transcript. Figure 4 provides the number of accounts accessed[17] by four or more different e-mail addresses.

Figure 4: Taxpayer Accounts Accessed by Four or More E-Mail Addresses

E-Mail Addresses Used to Access a Single Account	Accounts Accessed	Accounts Identified by the IRS	Accounts Not Identified by the IRS
4	46,584	36,005	10,579
5	31,887	28,975	2,912
More Than 5	130,250	126,664	3,586
Total	**208,721**	**191,644**	**17,077**

Source: TIGTA analysis of authentication system audit logs.

[17] For purposes of Figure 4, the term "accessed" refers to access attempts and successful accesses.

The IRS did not identify the 17,077 accounts as potentially breached because it did not believe that the lone characteristic of accesses to an account by multiple e-mail addresses was sufficient to distinguish between identity theft and non–identity theft behavior. Thus, the IRS did not believe these accesses were suspicious enough to notify the affected taxpayers or place an identity theft incident marker on their tax account. However, as previously stated, the IRS completed additional analysis of the accesses after we identified them and announced that it would issue the affected taxpayers a notification letter and place an identity theft incident marker on their account.

The IRS did not review suspicious e-mail addresses to identify all taxpayers affected by the Get Transcript application data breach

We identified 68 accounts that were targeted using suspicious e-mail addresses that included questionable characters within the e-mail address. Each of these e-mail addresses contained 50 or more characters. For 39 (57 percent) of the 68 accounts, unauthorized individuals successfully accessed and obtained a tax transcript. Figure 5 provides hypothetical examples of e-mail addresses similar to the 50-character e-mail addresses that we identified.

Figure 5: Hypothetical Examples of Suspicious E-Mail Addresses

Unusual E-Mail Addresses of 50 Characters or Greater
P.....777@COOPPER.....MOUNT.....BAS..33MAIL.COM
F.....A....L.L...F.A.T...AK..A.....A..F..IS...B.ABY@P……..COLLEGE.EDU
JOHNB.....WWWWW.....WWW.....BOWEN@OUTLOOK.COM

Source: TIGTA's analysis of unusual e-mail addresses.

Cybersecurity function or OCA officials could have conducted additional reviews of the e-Authentication audit logs to find the suspicious 50-character e-mail addresses and identify more victims. However, they informed us that although the IRS's Enhanced Breach Incident Response Plan[18] was in place, the plan did not require a review to identify the "unusual" e-mail addresses that we identified.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 1: Ensure that additional evaluative methods are implemented to identify all individuals affected by the Get Transcript application breach and that procedures are developed based on this breach to assist the IRS in responding to any future related data breaches.

[18] IRS's blueprint for roles, required notifications, lines of communication, and steps to be taken to respond to a security breach.

Management's Response: The IRS agreed with this recommendation. The IRS has employed both expanded methodologies and incorporated suggestions from TIGTA to identify suspect accesses. The IRS has built these refinements into its current processes for addressing such issues.

Recommendation 2: Once analysis of the 620,931 suspicious account accesses is complete**,** issue notification Letter 4281-G to the taxpayers whose accounts were potentially targeted by unauthorized individuals and place identity theft incident markers on the accounts of taxpayers whose accounts do not have the marker.

Management's Response: The IRS agreed with this recommendation. The IRS indicated that notification letters for the subject population were mailed during March and April 2016. These accounts were placed on the Dynamic Selection List for heightened levels of identity theft protection on any subsequently filed returns, and the Data Loss Indicators were placed on the accounts.

Analysis of Suspicious E-Mail Domains Did Not Identify All Victims

Our evaluation of the 12 suspicious e-mail domains that the OCA analyzed identified 2,470 taxpayer accounts[19] that were targeted by an unauthorized individual through the Get Transcript application but were not identified by IRS. Although these access attempts were unsuccessful, the affected taxpayers should have been issued a Letter 4281-B, and an identity theft incident marker should have been placed on their tax account.

OCA officials stated that they researched the 2,470 accounts and determined these attempted accesses were associated with three authentication system error codes that they had not included in their review. They stated that their original dataset did not contain transactions associated with authentication system failure codes and their research focused on pass and fail rates. As a result, the OCA did not identify these 2,470 potential victims. OCA officials noted that they shared our results with other IRS functions including the Wage and Investment Division; the Office of Privacy, Governmental Liaison, and Disclosure; and the Cybersecurity function to discuss lessons learned from the authentication audit log analysis and potential solutions for ensuring that all unauthorized attempted accesses are identified.

Our review also identified that the OCA inadvertently truncated one legitimate domain, "gmail.com" as "gmail.co" in its analysis, which resulted in the incorrect identification of 32 victims. OCA officials stated that they are working with the Cybersecurity function and other functions to address e-mail truncation problems in the OCA analysis process. After we brought this issue to the IRS's attention, the IRS placed identity theft incident markers on the tax accounts of the 2,470 potential victims, as appropriate.

[19] Of the 2,470 taxpayer accounts, 2,423 were included in the population of 620,931 taxpayers whose tax account information also involved a potentially unauthorized access not identified by the IRS.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 3: Ensure that all appropriate authentication system error codes are included when responding to any future data breaches so that all potentially fraudulent accesses are captured and analyzed to properly identify all individuals affected by the breach.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has included all appropriate authentication system error codes in its analysis methodologies.

Recommendation 4: Ensure that the 2,470 individuals identified by TIGTA are mailed Letter 4281-B.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS indicated that Letter 4281-B, *Non-Impacted Primary Taxpayers Without Offer of Credit Monitoring*, has been mailed to this population of individuals.

Identity Theft Incident Markers Were Not Placed on All Victim Tax Accounts

The IRS did not place an identity theft incident marker on the tax accounts of 3,206 of the 289,843 taxpayers[20] initially identified by the IRS as affected by the Get Transcript application breach. IRS procedures require employees to place an identity theft incident marker on the tax account of all affected taxpayers. This marker would alert IRS employees assisting a taxpayer that the taxpayer's account was affected by the Get Transcript application breach.

IRS management officials stated that the markers were placed only on the accounts of taxpayers who were mailed a notification letter, and 2,690 taxpayers of the 3,206 taxpayers we identified without a marker were ones who were not mailed a letter. The IRS decided to not issue a notification letter to Get Transcript application breach victims if their address on the Master File is an IRS campus address.[21] Letters were also not mailed to victims 18 years and under or to victims whose tax accounts do not show a date of birth.

For the remaining 516 tax accounts without an identity theft incident marker, Accounts Management function officials cited employee error as the reason why the markers were not added to the taxpayers' accounts. The employees inadvertently missed some accounts during the marking process. After we brought this issue to the IRS's attention, the IRS placed identity theft

[20] The affected taxpayers without an identity theft marker on their account who were part of the initially identified group of the 224,688 primary taxpayers plus the associated secondary filers, dependents, day care providers, and alimony recipients listed on the fraudulently accessed tax returns.

[21] The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts. The IRS updates a taxpayer's address on the Master File to a campus address when it cannot determine the taxpayer's correct address.

incident markers on 3,162 of the 3,206 tax accounts. However, 44 tax accounts remain unmarked.

After we questioned the IRS's rationale for not placing the marker on all tax accounts, management agreed that all affected taxpayer accounts need the marker. As a result, IRS officials informed us that they would ensure that all taxpayer accounts receive the identity theft marker.

Recommendation

Recommendation 5: The Commissioner, Wage and Investment Division, should ensure that required identity theft incident markers are placed on the tax accounts of the 44 taxpayers affected by the Get Transcript application breach.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will ensure all accounts are marked appropriately.

Notification Letters Did Not Always Provide Sufficient or Accurate Information

Our review of IRS issuance of notification letters identified that the letters did not always provide sufficient information to identify dependents who may have been listed on accessed transcripts. Other letters did not provide the correct address for the credit bureau to be contacted for free credit monitoring. In addition, duplicate letters were mailed to some taxpayers.

- The IRS mailed Letter 4281-E to 32,133 taxpayers who claimed a dependent(s) on their tax return and their tax account was accessed by a potentially unauthorized individual. However, the letter did not provide the tax transcript year, transcript type, or other personal information to enable the taxpayer to identify the dependent whose PII was accessed. IRS officials stated that they followed their standard practice of only providing the name of the primary/secondary taxpayer on breach notification letters. Their intent is to provide the taxpayer with the information they need to understand the vulnerability while not exposing additional sensitive information (SSN or names of dependents) in the letter. The officials also stated that Letter 4281-E informs the taxpayer that the unauthorized access to their account may include access to other SSNs listed on their tax returns and suggests the taxpayer contact a credit bureau to determine whether a credit file exists for their dependent.
- Letter 4281-B provided an incorrect physical address for the credit bureau that the IRS coordinated with to provide free credit monitoring. The IRS identified this inaccuracy and issued an internal alert in June 2015 advising employees who assist taxpayers that the physical address for a credit bureau on Letter 4281-B was incorrect. The alert provided

the employees with the correct address. The IRS also revised this letter with the correct address in July 2015. The incorrect physical address for the credit bureau was due to an employee obtaining the address from an older notice that contained credit bureau information and not checking the credit bureau web page to verify the current address.

- Letter 4281-B was mailed to 4,579 taxpayers twice. The Office of Privacy, Governmental Liaison, and Disclosure, the Accounts Management function, the National Distribution Center, and the Media and Publication office worked together to create and issue the notification letters. However, the duplicate letters were mailed because the National Distribution Center did not have a procedure to compare the number of recipients on the Letter 4281-B recipient file to the number of letters that were printed for mailing. The IRS identified the duplicate letter error only after the letters were mailed, and the IRS promptly issued another internal alert to employees advising them to apologize to taxpayers for the inconvenience of sending duplicate letters. To avoid similar reoccurrences of mailing taxpayers duplicate letters, the IRS stated that it will implement quality assurance measures to assign a sequential number to each recipient. The final letters will be placed in sequential order within each run and verified against the production plan before mailing.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 6: Revise notification letters to enable taxpayers to more easily identify the individuals whose PII was accessed in any future security breaches.

Management's Response: The IRS agreed with this recommendation. The IRS indicated that they agree with this recommendation as it applies to future incidents. The IRS will continually review and revise their notification letters depending on the circumstances of a particular incident. Their standard will continue to be that they provide sufficient information for the affected individuals to protect themselves while not exposing additional sensitive information. In developing the notifications for the taxpayers affected by the Get Transcript application breach, as noted by the auditors, the IRS alerted letter recipients that "…the unauthorized access to their account may include access to other Social Security Numbers (SSN) listed on their tax returns…" The IRS considers this reasonable because return filers would know those included on their submissions and the variances between tax years is likely to be minimal. IRS acknowledges the concerns about unusual filing situations that could cause confusion on the recipient's part and will ensure that, to the extent possible, future notifications address those concerns while still protecting sensitive information.

Recommendation 7: Ensure that procedures are followed to identify errors in letters and to verify the sequential order of letters against the letter production plan before the letters are mailed.

> ***Management's Response:*** The IRS agreed with this recommendation. Quality assurance controls were implemented in June 2015 that assign sequential numbers to each letter recipient to be used in preventing errors in mailing.

An Identity Protection Personal Identification Number Was Not Offered to All Individuals Affected by the Get Transcript Application Breach

The IRS mailed Letter 4281-B to 79,122 taxpayers whose accounts were targeted but not successfully breached by unauthorized individuals through the Get Transcript application. This letter advised taxpayers that the third party who attempted to access their tax information may have their personal information. However, the letter does not offer the recipient an IP PIN or provide instructions on how to obtain one. In addition, the IRS did not offer free credit monitoring services to the individuals mailed Letter 4281-B. Although the IRS acknowledges in this letter that third parties appear to have the taxpayer's SSN, officials stated that free credit monitoring was not offered because the unauthorized individuals obtained the taxpayers' PII from sources outside the IRS. The officials also stated that the decision to not provide an IP PIN was based on the fact that the unauthorized individuals did not pass the second authentication level, *i.e.*, unauthorized individuals were unable to answer the out-of-wallet questions in the online authentication process to access the taxpayers' accounts.

All individuals whose accounts were targeted through the Get Transcript application should receive the same protection because they are at an increased risk of having an identity thief file a fraudulent tax return using their personal information. In addition, we determined that the IRS placed identity theft incident markers on 4,910 (6 percent) of the 79,122 taxpayer accounts. This marker is a strong indication that these taxpayers became an identity theft victim after their accounts were breached through the Get Transcript application.

Lastly, the IRS's reasons for not offering an IP PIN to Letter 4281-B recipients conflict with its policy to offer at-risk taxpayers an IP PIN. For example, the IRS offers IP PINs to individuals who live in three high-risk locations for identity theft (Florida, Georgia, and the District of Columbia). The IRS also offers IP PINs to taxpayers who report a lost or stolen wallet or purse.

Recommendation

Recommendation 8: The Commissioner, Wage and Investment Division, should issue an IP PIN to all Letter 4281-B recipients whose SSNs were used by unauthorized individuals to attempt to access the Get Transcript application.

Management's Response: The IRS disagreed with this recommendation. The IRS disagreed with this recommendation primarily because they consider the issuance of IP PINs to be just one tool in its efforts to combat identity theft. The IRS has many defenses in place and is constantly exploring new and better ways to address this ever-changing challenge. In this instance, the IRS offered both credit monitoring and an opportunity to opt into an IP PIN to those taxpayers for whom their personal tax information was compromised by thieves accessing the Get Transcript application. The information these thieves used to pass authentication was obtained from sources outside the IRS. When they obtained additional information from an IRS system, the IRS provided the affected taxpayers with the appropriate mitigating protection. However, the population referenced in this recommendation is a different group and did not have any of their personal information exposed from IRS systems. It is not readily apparent that the thieves had any of their information beyond name and SSN since the authentication attempt failed. As a courtesy, the IRS notified these taxpayers that their personal information was apparently being used by fraudsters in a failed attempt to gain more information. These accounts were also added to the Dynamic Selection List, which means they were flagged in IRS systems, allowing the IRS to recognize the SSNs as potentially compromised and offer added protection to any return filed under those numbers. Another factor contributing to the IRS's decision not to offer IP PINs to these taxpayers was that the thieves attempting to access these accounts did so between one and two years ago, and offering IP PINs at this time would be counter-productive. However, the IRS acknowledges TIGTA's concern regarding the potential inconsistency in the IRS's policy regarding the offering of IP PINs to non-tax related identity theft victims and the population for whom there was a failed attempt to access Get Transcript. The IRS agreed to consider this point in future decisions regarding any changes to its IP PIN policy or general response to identity theft.

> ***Office of Audit Comment:*** Although IRS officials disagreed with our recommendation, they acknowledge the potential inconsistency in their policy with regards to issuing IP PINs and note that they agreed to consider this inconsistency in their future policy. Unfortunately, the lack of prompt action on this issue leaves the 79,122 taxpayers whose accounts were targeted at an increased risk of an identity thief filing a fraudulent tax return using their personal information. In fact, as we reported, 4,910 of these taxpayers had an identity theft marker on their tax account.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate IRS identification and assistance provided to victims of the Get Transcript application data breach. To accomplish our objective, we:

I. Evaluated the processes used to identify all victims.

A. Identified the CSIRC process used to identify the data breach.

1. Interviewed CSIRC officials and determined how they identified the undelivered e-mails.

a. Evaluated the number and dates of undelivered e-mails that the CSIRC identified.

b. Determined the criteria used to identify the 59 domains as risky.

c. Assessed supporting documentation that the OCA used to identify risky domains.

2. Determined how the OCA analyzed audit logs and obtained a walk-though demonstration of the process used to identify all domains.

B. Determined if the number of victims affected by the data breach reported by the IRS was accurate.

1. Assessed the domains that the OCA identified.

2. Determined that the OCA did not identify all accounts for which unauthorized individuals attempted access, passed Level of Access C, and passed Level of Access D.[1]

a) Interviewed OCA officials and obtained an explanation of the process used to identify the number of attempted accesses.

b) Matched the list of SSNs affected by the Get Transcript application breach to the e-Authentication audit logs to determine if unauthorized individuals attempted 224,688 accesses.

[1] The IRS refers to the five pieces of PII as Level of Access C, which is a level of assurance known as Single-Factor Identification or Basic Identity (ID) Proofing. The IRS refers to the out-of-wallet questions as Level of Access D, which is a level of assurance known as Knowledge-Based Authentication.

3. Identified the IRS Application Development function's process for identifying SSNs associated with the SSNs of taxpayers whose accounts unauthorized individuals attempted to access via the Get Transcript application.

    a) Obtained the list of associated SSNs produced by the IRS Applications Development function.

II. Evaluated IRS service provided to victims of the Get Transcript application data breach and determined if proper notification letters were mailed to taxpayers and their tax accounts were properly updated.

A. Determined if proper notification letters were mailed to taxpayers.

1. Obtained the list of Letter 4281-B recipients from the Office of Privacy, Governmental Liaison, and Disclosure.

2. Interviewed IRS officials to determine the IRS's rationale for not providing IP PIN instructions to recipients of Letter 4281-B.

3. Verified information presented on some letters was correct while others contained inaccurate information.

B. Determined IRS processes for marking the tax accounts of those taxpayers identified as being affected by the Get Transcript application data breach.

1. Interviewed IRS officials to determine the process to place identity theft incident markers on the tax accounts of those affected by the data breach.

2. Matched the list of 224,688 SSNs to an indicator identifying a taxpayer as being affected by the Get Transcript application breach to determine if all accounts were properly marked and the miscellaneous field includes the correct incident number.

3. Interviewed appropriate IRS personnel and determined the reasons why accounts were not marked with an identity theft indicator as required.

4. Performed validation procedures for the data obtained in Step II.B. Because only the tax accounts associated with 199,741 of the 224,688 SSNs were marked when validation tests were performed, we reconciled a judgmental sample of 10 records from our population of 199,741 SSNs to verify that the accounts were properly marked and the miscellaneous field includes the correct incident number. Based on our sample, we determined that the data were sufficiently reliable for the purposes of this report.

III. Quantified the impact of the Get Transcript application data breach on tax administration.

A. Interviewed Return Integrity and Compliance Services function officials concerning their process for determining the number of fraudulent tax returns filed with an affected SSN.

B. Obtained analytical data completed by the Return Integrity and Compliance Services function concerning tax returns filed after the Get Transcript application breach using the taxpayer's associated SSNs.

IV. Performed analysis of suspicious e-mail addresses by analyzing the relationship between TINs and e-mail addresses that were captured by the e-Authentication application system audit logs.

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: how the Get Transcript application breach was identified; the processes used to identify, notify, and help protect individuals affected by the breach; and the impact of the breach on tax administration. We evaluated these controls by interviewing personnel and reviewing identity theft claims.

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
W. Allen Gray, Director
Jamelle L. Pruden, Audit Manager
Jerry Douglas, Lead Auditor
Lynn Faulkner, Senior Auditor
Gwen Gilboy, Senior Auditor
Tracy Hernandez, Senior Auditor
Arlene Feskanich, Information Technology Specialist
Alberto Garza, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Director, Strategic Data Services
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:

- Taxpayer Privacy and Security – Potential; 620,931 taxpayers whose accounts were potentially targeted by unauthorized individuals using the Get Transcript application (see page 7).

Methodology Used to Measure the Reported Benefit:

We identified 609,951 taxpayer accounts that an individual(s) attempted to access with an e-mail address that was used to attempt access to 10 or more accounts. However, the IRS did not identify these accounts as potentially targeted by identity thieves. In addition, we identified 17,077 taxpayer accounts that an individual(s) attempted to access using four or more different e-mail addresses, but the IRS did not identify these taxpayers as potential victims. A total of 6,165 accounts appeared in both populations of unidentified victims. Lastly, we identified 68 taxpayer accounts targeted using an e-mail address of 50 or more characters. Because the IRS did not identify these potential victims, it did not mail them a notification letter or place an identity theft incident marker on their account (609,951 + 17,077 - 6,165 + 68 = 620,931).

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 2,470 taxpayers whose accounts were targeted by unauthorized individuals, but the IRS did not identify them as potential victims (see page 11).

Methodology Used to Measure the Reported Benefit:

We identified 2,470 taxpayer accounts that an individual, using a suspicious domain,[1] attempted to access. The IRS did not identify these potential victims because its analysis of suspicious e-mail domains that were used to access accounts through the Get Transcript application excluded access attempts that resulted in a systemic error code. Thus, the IRS did not mail these taxpayers a notification letter or place a protective identity theft incident marker on their account as required.

[1] A domain refers to the name assigned to a computer, service, or any resource connected to the Internet.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 3,206 taxpayer accounts were not marked with an identity theft incident marker (see page 12).

Methodology Used to Measure the Reported Benefit:

We identified 3,206 taxpayer accounts that were not updated with the appropriate identity theft incident marker despite the IRS identifying the accounts as targeted by unauthorized individuals in the Get Transcript application breach. We identified these taxpayers by comparing the universe of all SSNs for the individuals affected by the Get Transcript application breach to an extract of the Individual Master File[2] accounts with identity theft incident markers.

Type and Value of Outcome Measure:

- Reduction of Burden on Taxpayers – Potential; 32,133 taxpayers who claimed a dependent(s) on their tax return and their tax account was accessed by a potentially unauthorized individual (see page 13).

Methodology Used to Measure the Reported Benefit:

We identified 32,133 taxpayers who were mailed Letter 4281-E because they claimed a dependent(s) on their tax return and their tax account was accessed by a potentially unauthorized individual. However, the letter did not provide the name or SSN of the dependent whose PII was accessed. Consequently, these individuals will have the burden of having to determine which of their dependents are affected.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 79,122 taxpayers whose accounts were targeted by unauthorized individuals through the Get Transcript application and were not offered an IP PIN or instructions on how to obtain one (see page 15).

Methodology Used to Measure the Reported Benefit:

We identified 79,122 taxpayers whose tax accounts were targeted by unauthorized individuals but not successfully accessed. We identified these individuals by obtaining the population of SSNs from the Office of Privacy, Governmental Liaison, and Disclosure. The IRS did not provide an IP PIN to these individuals although unauthorized individuals possessed their PII**.**

[2] The IRS database that maintains transactions or records of individual tax accounts.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

APR 2 2 2016

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Debra Holland
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – The Internal Revenue Service Did Not Identify and Assist All Individuals Potentially Affected by the Get Transcript Application Data Breach (Audit # 201540027)

Thank you for the opportunity to review and comment on the subject draft report. The theft of taxpayer data from the Get Transcript system was unprecedented in both its scope and the method by which the crime was committed. Criminals are becoming increasingly sophisticated and are gathering vast amounts of personal information as the result of data breaches at sources outside the IRS. They have attempted to use that cache of personal data stolen from other sources to impersonate their victims and either create or access online accounts and to obtain the tax return and account information of the legitimate taxpayer whom they are impersonating. In an age where massive losses of personally identifiable information (PII) of individuals occur regularly, through theft or by loss from public and private entities, the authentication standards that were widely acceptable just a few years ago, when our online systems were designed, are no longer adequate. We are moving to multi-factor authentication which provides a greater level of assurance; however, it will come at a price of additional burden for legitimate taxpayers trying to authenticate. For those unable to authenticate under the strengthened process, we will continue to provide alternative methods of service delivery to meet their needs while protecting against the unauthorized exposure of PII.

The IRS has been improving our system-monitoring capabilities, enabling us to detect suspicious activity before being alerted to it by outside sources such as taxpayers or vendors. We continue working to improve our monitoring capabilities, and enhancing our return processing filters, so that we can thwart criminal activity as quickly as possible. The IRS shut down the Get Transcript application when suspicious transactions were first identified and confirmed. It will not be reactivated until we are confident authentication processes are strong enough to provide reasonable assurance that users of the system are the legitimate owners of the account they are accessing. As

the scope of the crime became apparent, the IRS made the decision to remove the Get Transcript application from IRS.gov on May 21, 2015. At that time, a massive triaging effort was already underway to analyze information provided by system and application log files, and to define the methodology that would be used to identify potential victims. On May 29, 2015, we were contacted by the Treasury Inspector General for Tax Administration (TIGTA), and informed of your intent to conduct this review. Over the course of several months, from June 2015 through January 2016, the TIGTA audit team assisted in the effort to identify the scope of the event and the impacted population. The team expanded the scope of the review by building upon our identification methodologies, exploring alternative methods, and by widening and lengthening the breadth and depth of the analysis. As time was of the essence and our own resources were stretched thin in identifying and assisting the affected taxpayers, we appreciate the assistance the TIGTA provided to us during this time.

When the population of suspected victims was first identified, to ensure their accounts were protected against attempted identity theft through the filing of fraudulent returns by the fraudsters, we immediately placed those Taxpayer Identification Numbers (TIN) on a database against which every processed return is checked. Any tax returns subsequently filed and processed would be matched against the Dynamic Selection List and would be suspended from processing while the return was reviewed and the legitimate taxpayer contacted and asked to authenticate themselves. For the most at-risk population, where stolen information was sufficient to prepare tax returns nearly identical to those of previous years' filings, authentication was done face-to-face, where IRS employees verified the taxpayers' identities with government-issued photo identification.

With the accounts protected from subsequent fraudulent filings, the process of notifying taxpayers began. For those taxpayers whose accounts had been successfully accessed, or whose TINs had been exposed due to their inclusion on the return of a successfully accessed account owner, the IRS offered free credit monitoring and the opportunity to request an Identity Protection Personal Identification Number be placed on their account for continued future protection. For those taxpayers where accesses had been attempted, but were unsuccessful, and there had been no previous determination of identity-theft activity on the account, the IRS notified them of the attempt but did not offer credit monitoring as no PII had been released to the fraudster.

We do not agree with the TIGTA's position that credit monitoring services should have been provided to the population of taxpayers whose accounts were not successfully accessed. Providing an identity theft monitoring product (commonly referred to as credit monitoring) is a standard practice when an incident causes sensitive information in the possession of the IRS to be compromised and the risk of identity theft is high. This is also standard practice in private industry when a data breach occurs. The common principle being that the organization that exposes the sensitive information offers the credit monitoring. Credit monitoring was not offered to the recipients of Letter 4281-B,

Non-Impacted Primary Taxpayers without Offer of Credit Monitoring, as the attempt to access transcripts was unsuccessful and, consequently, IRS held data was not compromised. We therefore disagree with the Outcome Measure associated with this population of 79,122 taxpayers.

A final step in treating the population of taxpayers affected by the Get Transcript incident was to place a reference marker on their account to identify them as a victim of this particular incident. The report refers to these markers as "Identity Theft Incident Markers," however, that is not an accurate description of their purpose or use. The transactions to which the TIGTA refers are actually Data Loss Indicators and are linked to an alpha-numeric indicator that is unique to the Get Transcript event. This particular transaction has no effect on identity theft protection, unlike the inclusion of all affected accounts on the Dynamic Selection List.

Attached are our comments to your recommendations. If you have any questions, please contact me, or a member of your staff may contact Ivy McChesney, Director, Customer Account Services, Wage and Investment Division, at (404) 338-8910.

Attachment

Attachment

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 1
Ensure that additional evaluative methods are implemented to identify all individuals affected by the Get Transcript application breach and that procedures are developed based on this breach to assist the IRS in responding to any future related data breaches.

CORRECTIVE ACTION
We agree with this recommendation and have employed both expanded methodologies and incorporated suggestions from the Treasury Inspector General for Tax Administration to identify suspect accesses. We have built these refinements into our current processes for addressing such issues.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Research, Applied Analytics, and Statistics

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 2
Once analysis of the 620,931 suspicious account accesses is complete, issue notification Letter 4281-G to the taxpayers whose accounts were potentially targeted by unauthorized individuals and place identity theft incident markers on the accounts of taxpayers whose accounts do not have the marker.

CORRECTIVE ACTION
Notification letters for the subject population were mailed during March and April 2016. These accounts were placed on the Dynamic Selection List for heightened levels of identity theft protection on any subsequently filed returns, and the Data Loss Indicators were place on the accounts. .

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Accounts Management, Customer Account Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 3
Ensure that all appropriate authentication system error codes are included when responding to any future data breaches so that all potentially fraudulent accesses are captured and analyzed to properly identify all individuals affected by the breach.

CORRECTIVE ACTION
We have included all appropriate authentication system error codes in our analysis methodologies.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Research, Applied Analytics, and Statistics

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 4
Ensure that the 2,470 individuals that TIGTA identified are mailed Letter 4281-B.

CORRECTIVE ACTION
Letter 4281-B, *Non-Impacted Primary Taxpayers without Offer of Credit Monitoring*, has been mailed to this population of individuals.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Accounts Management, Customer Account Services, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

Recommendation

RECOMMENDATION 5
The Commissioner, Wage and Investment Division, should ensure that required identity theft incident markers are placed on the tax accounts of the 44 taxpayers affected by the Get Transcript application breach.

CORRECTIVE ACTION
We will ensure all accounts are marked appropriately.

IMPLEMENTATION DATE
June 15, 2016

RESPONSIBLE OFFICIAL
Director, Accounts Management, 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.

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 6
Revise notification letters to enable taxpayers to more easily identify the individuals whose PII was accessed in any future security breaches.

CORRECTIVE ACTION
We agree with this recommendation as it applies to future incidents. We continually review and revise our notification letters depending on the circumstances of a particular incident. Our standard will continue to be that we provide sufficient information for the impacted individuals to protect themselves while not exposing additional sensitive information. In developing the notifications for the Get Transcript fraudulent access, as noted by the auditors, we alerted letter recipients, "…the unauthorized access to their account may include access to other Social Security Numbers (SSN) listed on their tax returns…" We consider this reasonable as return filers would know those included on their submissions and the variances between tax years is likely to be minimal. We acknowledge the concerns about unusual filing situations that could cause confusion on the recipient's part and will ensure, to the extent possible, that future notifications address those concerns while still protecting sensitive information.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Privacy, Governmental Liaison and Disclosure

CORRECTIVE ACTION MONITORING PLAN
N/A

RECOMMENDATION 7
Ensure that procedures are followed to identify errors in letters and to verify the sequential order of letters against the letter production plan before the letters are mailed.

CORRECTIVE ACTION
Quality assurance controls were implemented in June 2015, that assign sequential numbers to each letter recipient to be used in preventing errors in mailing.

IMPLEMENTATION DATE
Implemented

RESPONSIBLE OFFICIAL
Director, Media and Publications, Customer Assistance, Relationships, and Education, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
N/A

Recommendation

RECOMMENDATION 8
The Commissioner, Wage and Investment Division, should issue an IP PIN to all Letter 4281-B recipients whose SSNs were used by unauthorized individuals to attempt to access the Get Transcript application.

CORRECTIVE ACTION
We disagree with this recommendation primarily because we consider the issuance of IP PINs to be just one tool in our efforts to combat identity theft. We have many defenses in place, and we are constantly exploring new and better ways to address this ever-changing challenge. In this instance, the IRS offered both credit monitoring and an opportunity to opt into an Identity Protection Personal Identification Number (IP PIN) to those taxpayers for whom their personal tax information was compromised by thieves accessing our Get Transcript application. The information these thieves used to pass authentication was obtained from sources outside of IRS. When they obtained

additional information from an IRS system, we provided the affected taxpayers with the appropriate mitigating protection. However, the population referenced in this recommendation is a different group and did not have any of their personal information exposed from IRS systems. It is not readily apparent that the thieves had any of their information beyond name and SSN since the authentication attempt failed. As a courtesy, IRS notified these taxpayers that their personal information was apparently being used by fraudsters in a failed attempt to gain more information. These accounts were also added to the Dynamic Selection List, which means they were flagged in our systems, allowing us to recognize the SSNs as potentially compromised and offer added protection to any return filed under those numbers. Another factor contributing to our decision not to offer IP PINs to these taxpayers was that the thieves attempting to access these accounts did so between one and two years ago, and offering IP PINs at this time would be counter-productive. However, we note your point with regard to potential inconsistency in IRS policy regarding IP PIN offers to non-tax related identity theft victims and the population for whom there was a failed attempt to access Get Transcript. We agree to consider this point in future decisions regarding any changes to our IP PIN policy or to our response to identity theft in general.

IMPLEMENTATION DATE
N/A

RESPONSIBLE OFFICIAL
N/A

CORRECTIVE ACTION MONITORING PLAN
N/A