
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Office of Inspections and Evaluations



*Revised Procedures Preceded Significant Increases
in Reports of Potential Disclosure of Personally
Identifiable Information*

May 18, 2010 / Revised September 23, 2010

Reference Number: 2010-IE-R005

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.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

May 18, 2010

MEMORANDUM FOR DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT

FROM: R. David Holmgren *R. David Holmgren*
Deputy Inspector General for Inspections and Evaluations

SUBJECT: Final Evaluation Report – Revised Procedures Preceded Significant Increases in Reports of Potential Disclosure of Personally Identifiable Information (# IE-10-003)

This report presents the results of our evaluation to determine why the Internal Revenue Service (IRS) experienced a significant increase in the number of reported potential disclosures of personally identifiable information.

This evaluation focused on the efforts by the IRS Office of Privacy, Information Protection and Data Security to identify and manage potential disclosure of personally identifiable information by the IRS. Inappropriate, unauthorized disclosure of personally identifiable information can place taxpayers at increased risk for identity theft, which remains a serious problem in the United States. Identity theft can create havoc in an individual's life while creating barriers to voluntary compliance for those taxpayers who have been victims of this crime.

Synopsis

This evaluation concentrated on a reported increase in the number of disclosure incidents that began in April 2009. We analyzed data from IRS systems characterizing disclosure incidents, interviewed field employees, and assessed the likely impact of new policy that changed internal IRS procedures on the reporting of potential disclosures. Our analysis leads us to conclude that the increase in disclosure incidents was related to revised reporting guidelines and requirements published by the IRS in March and September 2009.

While we make no recommendations in this report, IRS managers reviewed the draft report and concurred with the facts we developed and reported.



*Revised Procedures Preceded Significant Increases in Reports
of Potential Disclosure of Personally Identifiable Information*

Please contact me at (202) 927-7048 if you have questions or Kevin Riley, Director, Office of Inspections and Evaluations, at (972) 249-8355.



*Revised Procedures Preceded Significant Increases in Reports
of Potential Disclosure of Personally Identifiable Information*

Table of Contents

BackgroundPage 1

Results of ReviewPage 2

 Reporting Procedures Were RevisedPage 3

 Interviewed Employees Were Aware of New Procedures.....Page 5

 ConclusionPage 5

Appendices

 Appendix I – Detailed Objective, Scope, and MethodologyPage 7

 Appendix II – Major Contributors to This ReportPage 8

 Appendix III – Report Distribution ListPage 9



*Revised Procedures Preceded Significant Increases in Reports
of Potential Disclosure of Personally Identifiable Information*

Abbreviations

IRS	Internal Revenue Service
PII	Personally Identifiable Information



Revised Procedures Preceded Significant Increases in Reports of Potential Disclosure of Personally Identifiable Information

Background

During 2009, the Treasury Inspector General for Tax Administration became concerned about an increase in reports of potential disclosure of personally identifiable information (PII).¹ Inappropriate disclosure of PII can place individuals at higher risk of identity theft and may erode public confidence in the Nation's tax system, which is built upon the principle of voluntary compliance with the provisions of the tax code.

The Federal Trade Commission reports that perpetrators of identity theft continue to victimize hundreds of thousands of American citizens. While the overall number of identity theft complaints dropped from 2008 to 2009, identity theft remains the single largest type of complaint submitted to the Federal Trade Commission's Consumer Sentinel Network with over 1.3 million complaints received since 2005.²

In July 2007, the Internal Revenue Service (IRS) established the Office of Privacy, Information Protection and Data Security to protect sensitive data by reducing the risk of inadvertent disclosures by IRS employees. The Office conducts assessments of potential disclosures that might place taxpayers at increased risk for identity theft. In 2009, the Office investigated over 2,900 cases, which was a significant increase from 2008. When taxpayer risk has been identified, the Office notifies taxpayers of potential issues and may offer credit monitoring or related services that are designed to reduce the risk of actual identity theft.

This review was initiated as a limited scope evaluation of the disclosure incident reporting process, with a focus on incidents that were reported during calendar year 2009. The intent was to determine the reason for the increased rate of disclosure incident reporting.

The review was performed at the IRS National Headquarters in Washington, D.C., and supported by field visits to Philadelphia, Pennsylvania, and Austin, Texas, during the period from November 2009 through March 2010. This review was performed in accordance with the Council of the Inspectors General for Integrity and Efficiency Quality Standards for Inspections. Detailed information on our objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

¹ Personally identifiable information (PII) refers to information that can be used to distinguish or trace an individual's identity, alone or when combined with other personal or identifying information. Examples of PII include: names, Social Security Number, biometric records, date of birth, financial or bank account information, and driver's license numbers.

² The complete Consumer Sentinel Network Data Book for January – December 2009 (released February 2010) is available on the Federal Trade Commission website at <http://ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf>.

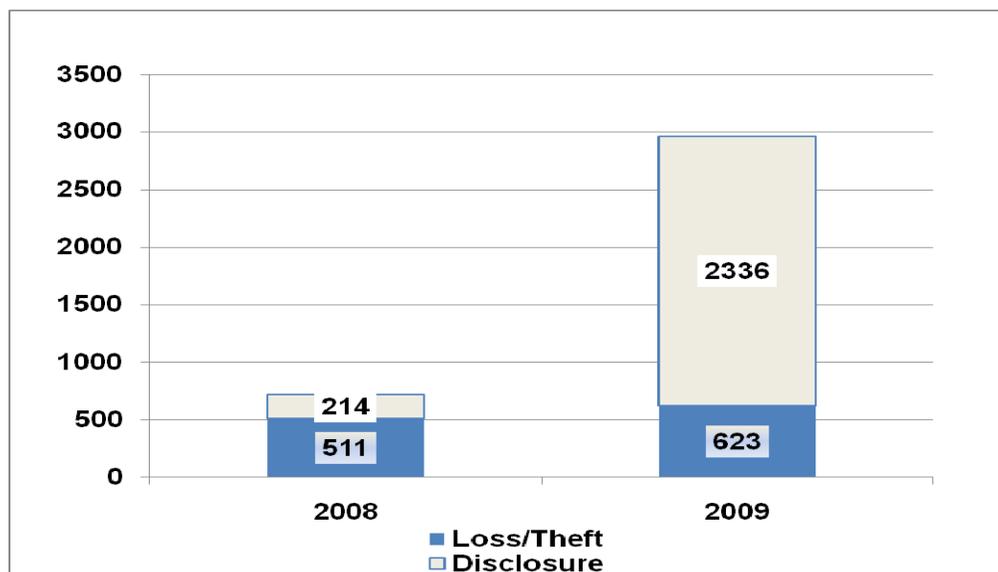


Revised Procedures Preceded Significant Increases in Reports of Potential Disclosure of Personally Identifiable Information

Results of Review

During 2009, the IRS took several steps to improve its ability to report and assess potential breaches of PII. Revisions to incident reporting procedures were followed by significant increases in the number of disclosure incidents (2,336 of 2,959 for all incident types recorded in 2009), exceeding the number of all incident types from the prior year (725 recorded in 2008).

Figure 1: Potential Disclosures Investigated



Source: Treasury Inspector General for Tax Administration derived from IRS PII Tools Database.

IRS categorizes incidents involving the potential breach of PII as a Loss, Theft, or Disclosure.

- **Loss:** PII is lost during handling and/or shipment of paper-based records or computer media containing PII in electronic format.
- **Theft:** PII is stolen from IRS facilities or while in custody of IRS employees. Examples include the theft of computers and or related media, mobile devices, and paper files containing PII.
- **Disclosure:** PII is disclosed to unauthorized parties during routine business activity. Examples include: a person calling the IRS on a toll-free assistance number, purporting to be a taxpayer they are not and obtaining that taxpayer's information; IRS employees failing to follow disclosure procedures and not properly authenticating the caller's



Revised Procedures Preceded Significant Increases in Reports of Potential Disclosure of Personally Identifiable Information

identity through a series of challenge questions for which only the taxpayer should have correct responses; or erroneous correspondence, where a notice, letter or other form of correspondence inappropriately contains another taxpayer's information or is somehow misdirected to an incorrect address and opened by a recipient who is not the taxpayer.

Reporting Procedures Were Revised

In March 2009, the IRS Office of Privacy, Information Protection and Data Security implemented revisions to how IRS personnel were required to report on these types of incidents.

The IRS uses its Computer Security Incident Response Center as a centralized reporting facility for all computer security and privacy incidents. As part of the revised process, Privacy, Information Protection and Data Security, and Computer Security Incident Response Center staff modified reporting mechanisms to better integrate the reporting of disclosure incidents with other security items. This action provided front-line employees and managers with a single mechanism to report on all disclosure incidents not involving taxpayer correspondence.

Due to the volume and complexity of taxpayer correspondence (in excess of 190 million notices and letters in calendar year 2009), the Privacy, Information Protection and Data Security staff clarified that all taxpayer correspondence issues should first be reviewed by the IRS Notice Gatekeeper. The Notice Gatekeeper is responsible for conducting an initial assessment of all erroneous correspondence issues to determine the cause of the problem and to coordinate operational steps to mitigate any taxpayer impact that may result. As part of the assessment, the Notice Gatekeeper is responsible for verifying and reporting all disclosures of personally identifiable information resulting from erroneous taxpayer correspondence to the centralized reporting facility at the Computer Security Incident Response Center.

On March 29, 2009, the revised guidance was published for all front-line employees and their managers. In the following months, the number of reported incidents spiked (see Figure 2).

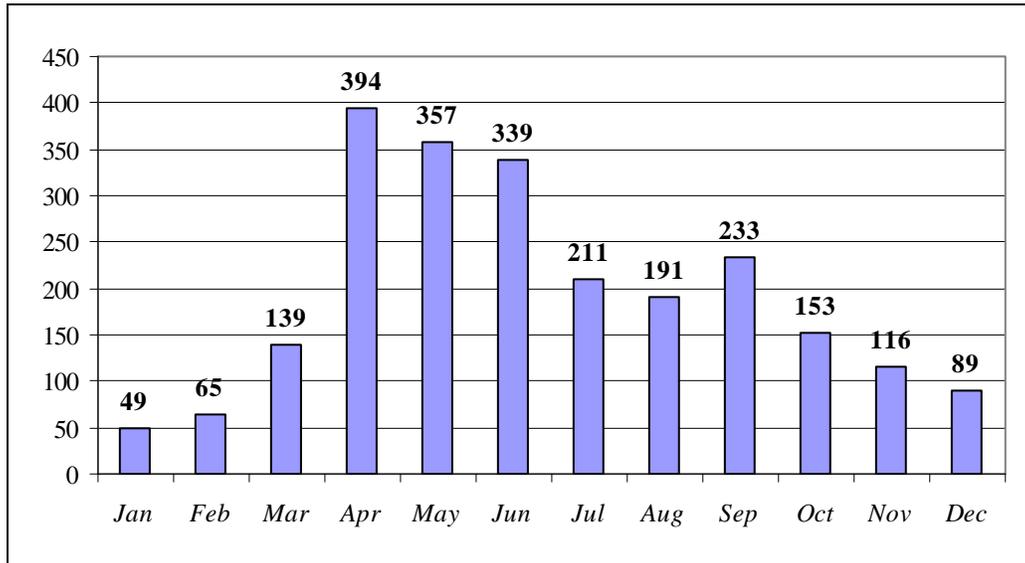
In September 2009, subsequent policy was issued by the IRS Wage and Investment Division that further clarified the types of erroneous correspondence that should be reported first to the Notice Gatekeeper. This guidance formalized the expansion of erroneous correspondence to include notices, letters, transcripts, faxes and other electronic transmissions containing taxpayer information where these communications containing incorrect information were delivered to a wrong party or were created by mistake. Previously, erroneous correspondence was narrowly limited to notices.

Review of the IRS PII Tools Database reflects a second, much smaller increase in incidents reported during September 2009, the majority of which were associated with Notice Gatekeeper issues.



Revised Procedures Preceded Significant Increases in Reports of Potential Disclosure of Personally Identifiable Information

Figure 2: Disclosure Incidents – 2009



Source: Treasury Inspector General for Tax Administration derived from IRS PII Tools Database (based on Date of Incident; excludes Loss/Theft Incidents.)

The increase in disclosure incidents, which include both telephone and correspondence disclosures, contrasts with taxpayer telephone call volumes for the same period. For calendar year 2009, IRS reported 2,336 disclosure incidents compared to total call volumes in excess of 38 million calls and notice/letter volumes exceeding 190 million. During the time of the identified increase in disclosure incidents, IRS experienced call volumes in the range of five million calls per month each for February, March, and April 2009. Call volume dropped to just over three million calls in May 2009. This suggests that the increase in the number of incidents was unrelated to call volumes, which remained relatively steady from February through April, while the increase in disclosures began immediately following the issuance of revised procedures at the end of March.



Revised Procedures Preceded Significant Increases in Reports of Potential Disclosure of Personally Identifiable Information

Interviewed Employees Were Aware of New Procedures

In November 2009, we interviewed employees from a field office where data showed disclosure incidents had occurred. In each interview, employees expressed high awareness of revised IRS disclosure procedures and the associated reporting process should a potential disclosure occur. We were provided examples where employees had self-reported suspected disclosures and were provided evidence where IRS disclosure procedures are reviewed as a normal part of quality review processes conducted at the supervisory and at the program level.

We also observed locally implemented procedures that were adopted to prevent inadvertent disclosures. For example, the IRS Income Verification Expedite Service is a fee-based program that, with taxpayer consent, transmits taxpayer information to participating mortgage and financial companies. The program facilitates income verification for taxpayers seeking to borrow money from those companies. Many mortgage and financial companies submit Income Verification Expedite Service requests in bulk and IRS processes these requests in batches of up to 50 taxpayers per batch.

The secure transmission of Income Verification Expedite Service information is dependent upon an IRS employee correctly entering a unique routing code into an information system. The system provides no validation of that code and sporadic transcription errors caused taxpayer information to be delivered to the wrong party. These incidents were identified and reported in accordance with disclosure incident procedures.

IRS management worked with Income Verification Expedite Service employees to implement a second-level review intended to ensure the routing code has been entered correctly. The process requires that a lead clerk or supervisor review the input screen to verify the correct routing code is input and to record his/her validation of the code by signing a form that is maintained with the batched requests.

Finally, we identified no deviation from IRS incident reporting procedures, nor any other individual causal factor that may have accounted for the overall increase in potential disclosure incidents.

Conclusion

Between March and June 2009, the IRS experienced a sharp increase in the number of reported PII disclosure incidents. An additional spike occurred in September 2009. Our review was conducted to determine the cause of the increase and to determine if taxpayer personally identifiable information was being put at risk by the IRS. Our analysis of reported incident data, policy changes, and interviews with front-line personnel lead us to conclude that the increase in disclosure incidents was related to revised reporting guidelines and requirements published by the IRS in March and September 2009. These guidelines formalized the expansion of erroneous correspondence to include notices, letters, transcripts, faxes and other electronic transmissions



Revised Procedures Preceded Significant Increases in Reports of Potential Disclosure of Personally Identifiable Information

containing taxpayer information where these communications contained incorrect information, were delivered to a wrong party, or were created by mistake. Improved reporting procedures better integrated the reporting of disclosure incidents with other security items and provided front-line IRS employees and managers with a single mechanism to report all disclosure incidents. As a result, the IRS is in a better position to prevent potential disclosures of sensitive taxpayer information.



*Revised Procedures Preceded Significant Increases in Reports
of Potential Disclosure of Personally Identifiable Information*

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine why the IRS experienced an increase during the summer 2009 timeframe in the number of reported incidents where PII may have been inappropriately disclosed to third parties.

To accomplish our objective, we:

- I. Interviewed Privacy, Information Protection and Data Security, and Wage and Investment Division senior staff and field staff.
- II. Determined the IRS efforts to identify and report on potential disclosure of PII.
- III. Determined the changes in policy or workload that may have contributed to the increased number of incidents.
- IV. Determined the number and type of incidents that occurred during calendar year 2009.
- V. Determined other factors that may have contributed to the increased number of incidents.



*Revised Procedures Preceded Significant Increases in Reports
of Potential Disclosure of Personally Identifiable Information*

Appendix II

Major Contributors to This Report

Kevin Riley, Director
Damon Plummer, Program Evaluator



*Revised Procedures Preceded Significant Increases in Reports
of Potential Disclosure of Personally Identifiable Information*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attention: Chief of Staff C
Deputy Commissioner for Services and Enforcement SE
Commissioner, Wage and Investment Division SE:W
Director, Office of Privacy, Information Protection and Data Security OS:PIPDS
Director, Privacy and Information Protection OS:PIPDS:PIP
Director, Customer Accounts Services SE:W:CAS
Director, Accounts Management SE:W:CAS:AM
Director, Submission Processing SE:W:CAS:SP
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC