The Internal Revenue Service Needs to Improve Telephone Authentication Practices to Better Prevent Unauthorized Tax Account Disclosures

February 2000

Reference Number: 2000-10-026

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 29, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Needs to Improve Telephone Authentication Practices to Better Prevent Unauthorized Tax Account Disclosures

This report presents the results of our follow-up review of the effectiveness of corrective actions to strengthen controls for authenticating the identity of taxpayers who telephone the Internal Revenue Service (IRS). These control weaknesses had been previously identified in an IRS Inspection Service (now Treasury Inspector General for Tax Administration) report titled, *Review of Protecting the Privacy of Tax Account Information* (Reference Number 075202, dated September 30, 1997).

In summary, we found Customer Service management adequately addressed one previously reported control weakness of not having clear policies and guidelines for dealing with suspended and/or disbarred practitioners. However, the unauthorized disclosure of taxpayer information remains at risk because Customer Service Representatives (CSRs) did not always comply with revised procedures for authenticating taxpayers' identities. We recommended that Customer Service management strengthen authentication procedures by providing CSRs with training on authenticating identities and revising national guidelines to include authentication verifiers that would be known to only the IRS and the taxpayer.

IRS management's response to the draft report discusses several corrective actions that will improve the reported conditions. Management's comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6500 if you have questions, or your staff may call Maurice S. Moody, Associate Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs), at (202) 622-8500.

Table of Contents

Executive Summary

A significant risk for unauthorized disclosure of taxpayer information occurs when Internal Revenue Service (IRS) Customer Service Representatives (CSR) respond to telephone inquiries from taxpayers. Accordingly, the procedures for effectively authenticating a caller's identity prior to disclosing taxpayer information are critical in protecting taxpayer privacy.

An IRS Inspection Service (now Treasury Inspector General for Tax Administration) report titled, *Review of Protecting the Privacy of Tax Account Information* (Reference Number 075202, dated September 30, 1997), noted weaknesses in the IRS' procedures for authenticating the identity of callers. This current review was performed as a follow-up to the 1997 report to determine if management effectively implemented corrective actions to reduce the risk of unauthorized disclosure to taxpayers and suspended and disbarred practitioners.

Results

The IRS' Customer Service management effectively implemented corrective actions related to establishing clear policies and guidelines for dealing with suspended and disbarred tax practitioners. Customer Service management revised its national guidelines and prepared a job aid for use by the IRS' field personnel. However, the unauthorized disclosure of taxpayer information remains at risk despite the corrective actions that were implemented to strengthen procedures for verifying the identities of taxpayers who telephone the IRS.

Unauthorized Disclosure of Taxpayer Information Over the Telephone Remains at Risk

In response to the prior audit report, Customer Service management expanded the minimum number of items CSRs must request to authenticate the callers' identities and defined high-risk situations that require additional verification. However, the risk of unauthorized disclosure of taxpayer information remains because CSRs have not complied with the revised procedures. Also, CSRs were not required, under the revised procedures, to use any of the items of authentication that would be confidential to only the caller and the IRS. In 65 of the 100 test calls we made, the CSRs either requested none (31 calls) or only 1 (34 calls) of the 2 additional verification items required for high-risk situations. Additionally, most of the identifying information that the CSRs asked for was available commercially from on-line Internet sources.

Summary of Recommendations

Customer Service management can strengthen authentication procedures by (1) providing CSRs with training on authenticating taxpayer identities, and (2) revising national guidelines to include authentication verifiers that would be known to only the IRS and the taxpayer.

Management's Response: Customer Service management agreed with the first recommendation and will emphasize to CSRs the need to comply with existing authentication requirements when high-risk situations are encountered. This increased emphasis will involve providing additional training and reference material on disclosure/authentication requirements for all CSRs. In response to the second recommendation, IRS management stated that it believes adding more probes to authenticate call-in taxpayers will be burdensome to the taxpayers and CSRs. Therefore, IRS management proposed an alternative approach that focuses on mandatory requirements, improved job aids, and training.

Office of Audit Comment: While we understand management's concern about the additional burden discouraging callers, IRS management needs to be prepared to step-up its controls if the proposed alternative enhancements do not work.

Objective and Scope

Our primary objective was to determine the effectiveness of authentication controls by testing the level of Customer Service Representative compliance with revised authentication requirements.

Our overall objective was to determine the effectiveness of corrective actions to strengthen controls for authenticating the identity of taxpayers who telephone the Internal Revenue Service (IRS). Control weaknesses had been identified in the IRS Inspection Service (now Treasury Inspector General for Tax Administration) report titled, *Review of Protecting the Privacy of Tax Account Information* (Reference Number 075202, dated September 30, 1997). We also determined whether alternative authentication methods existed and if the IRS was considering them.

To accomplish our objective, we:

- Interviewed managerial and operational personnel in the Customer Service - Telephone Operations Division on current and proposed alternative authentication practices/methods. We also examined and discussed with Customer Service management the revised procedures governing the disclosure of information to suspended and disbarred practitioners.
- Made test calls and on-site observations to evaluate compliance with revised telephone authentication requirements.

We performed our audit work between November 1998 and June 1999, in accordance with *Government Auditing Standards*.

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

Taxpayer information is protected by various laws and regulations, such as the Privacy Act of 1974[1] and disclosure provisions under the Internal Revenue Code.[2] The potential for unauthorized disclosure of tax information exists when employees with access to the IRS' sensitive computerized information handle telephone inquiries from taxpayers.

The prior audit report recommended strengthening controls over authenticating the identity of callers.

The prior audit report identified control weaknesses in the way the IRS disclosed taxpayer information over the telephone. The report recommended strengthening controls to ensure that Customer Service Representatives (CSR) use the IRS' sensitive computerized information more effectively to authenticate the identity of callers and establishing clear policy and guidelines to address the disclosure of account information to suspended and disbarred practitioners.

As part of the nationwide corrective action, Customer Service management (hereafter referred to as Customer Service) revised its guidelines to require that CSRs ask for the caller's date of birth (DOB) in addition to the name, address, and social security number (SSN). The revised guidelines also defined several high-risk situations in which at least two additional items of authentication must be verified. These additional items include filing status, spouse's SSN, spouse's DOB, income, employer, financial institutions, number of exemptions, paid preparer, or any other items from the last return filed that can be verified.

Examples of high-risk situations include instances in which the caller: asks for tax account information over the telephone; has not received a notice or other IRS correspondence or is not inquiring about a refund; wants tax account information mailed to an address different

[1] Privacy Act of 1974, 5 U.S.C. § 552a (1994)
[2] 26 U.S.C. § 6103(a) (1986)

from that on record; or is requesting a change of address along with a request for tax account information.

Customer Service took further corrective action and clarified its policies and guidelines for the disclosure of information to suspended and disbarred practitioners.

Results

Customer Service had adequately addressed the previously reported control weakness of not having clear policies and guidelines for dealing with suspended and disbarred practitioners. Customer Service revised its national guidelines and clarified and emphasized procedural changes by preparing a job aid on this topic for field personnel. The offices of the Director of Practice and the Director of Government Liaison and Disclosure confirmed a similar and consistent approach in dealing with suspended and disbarred practitioners.

However, despite Customer Service's corrective actions to strengthen procedures for verifying the identities of taxpayers who telephone the IRS, the unauthorized disclosure of taxpayer information remains at risk. Specifically, CSRs did not always comply with the revised authentication procedures. Additionally, the effectiveness of the revised procedures was impaired because CSRs were not required to use any of the items of authentication that would be confidential to only the caller and the IRS.

Unauthorized Disclosure of Taxpayer Information Over the Telephone Remains at Risk

The problem of authenticating taxpayers' identities during telephone contacts continues to exist.

Despite management's corrective action, weaknesses still exist in the authentication of taxpayers' identities during telephone contacts. Specifically, CSRs did not always ask for the required additional authentication items in high-risk situations.

We made 100 test calls to CSRs using the IRS toll-free telephone number to determine the level of CSR compliance with current authentication procedures. These calls included high-risk scenarios and were made from November 2, 1998 to January 19, 1999. Our callers requested tax information on their own and family members' accounts. The distribution of the calls was widespread, covering call sites nationwide that were answering the toll-free number.

The CSRs did verify the four basic authentication requirements: name, address, SSN, and DOB. However, the CSRs did not follow the high-risk authentication criteria in 65 of the 100 calls we made. In high-risk situations, CSRs are required to verify a minimum of two additional information items. But the CSRs did not request any additional items in 31 of the 65 calls we made and requested only 1 additional item in 34 calls.

High-Risk Verifiers Requested By Customer Service Representatives

None	31
One – filing status	21
One – employer	12
One – secondary SSN	1
Total	65

Source: Results of 100 test calls made to call sites nationwide using the IRS' toll-free number: (800) 829-1040.

Our Internet search found that the personal identity information used by CSRs is available commercially from Internet sources. The commercially available identity information included such items as name, address, primary and spousal SSN and DOB, current employer, and bank accounts. This covers 8 of the verifiers listed in the revised national guidelines. 12

The CSRs asked for an item not available from the Internet in only 49 of the 100 test calls. In 34 of the calls, the only item requested by the CSRs that was not available on the Internet was filing status, an item that may not be a particularly reliable authenticator because of the limited number of potential answers. 49

Customer Service had identified that authentication was one of the quality review issues with the highest error rate. According to Customer Service Division Quality Review data, telephone disclosure errors consistently ranked among the three highest errors and constituted nearly one-third of the total errors in each of the past two years.

To authenticate all callers, CSRs must ask for the caller's name, address, SSN, and DOB. In high-risk situations, at least two additional items of authentication must be verified. These items include filing status, spouse's DOB, income, employer, financial institutions, number of exemptions, paid preparer, or any other items from the last return filed that can be verified.

CSRs did not always adhere to authentication procedures.

CSRs did not always adhere to the revised authentication procedures requiring the verification of a minimum of two additional information items in high-risk situations. Additionally, revised procedures did not require that CSRs use items of authentication that would be confidential to only the caller and the IRS.

The likelihood of improper disclosure of taxpayer information greatly increases when CSRs do not follow established procedures or use more confidential authenticators. Customer Service has recently taken aggressive steps to better detect and monitor CSRs' compliance with authentication requirements. This

includes implementing the changes described below to the Quality Assurance/Review process that monitors, measures, and improves the quality of work.

Actions Taken to Improve Authentication

The IRS is aware of the problem and has implemented actions to improve telephone authentication of taxpayers.

In January 1999, Customer Service implemented a new computer screen for CSRs to use in authenticating callers. This screen contains information that should be used to verify the caller's identity, including the caller's name, address, SSN, DOB, filing status, secondary SSN, and secondary DOB. Customer Service will need more time to evaluate whether this new screen is improving authentication. While the screen may focus greater attention on completing required authentication, the items are similar to those noted during our test calls, and most are commercially available.

Customer Service will also be placing greater focus on authentication. As part of the Quality Assurance/Review process, the newly developed Centralized Quality Review System will better measure the accuracy of on-line calls answered by CSRs at the call sites and identify existing problems. IRS officials hope that the new system will help to identify root causes of authentication deficiencies.

From a long-term strategic outlook, the IRS sees electronic filing as a way to reduce the cost of processing tax returns and has taken initiatives to strengthen and simplify the authentication process. The IRS' Office of Electronic Tax Administration (ETA) is taking the lead in designing a new authentication method for use by the IRS in the future. The ETA's paper titled, "Draft Internal Revenue Service Electronic Authentication Principles and Strategy," indicated that the use of Personal Identification Numbers (PIN) is the main method under consideration to authenticate call-in taxpayers.

Several interactive applications on the Customer Service telephone system allow callers to access account information using a PIN. While these approaches appear

to offer a better and simpler way to authenticate callers, the ETA does not expect widespread expansion to the telephone system for several years.

Recommendations

Until the IRS establishes more reliable ways to authenticate callers, Customer Service should take the following steps to strengthen the current authentication process and reduce the risk of unauthorized disclosure.

1. Provide refresher training for CSRs, emphasizing the need for compliance with authentication requirements when high-risk situations are encountered. After the training is completed, CSR managers should monitor the CSRs to ensure compliance.

   Management's Response: Management agreed and has implemented corrective action primarily focusing on the compliance aspect. This includes providing refresher training that stresses the importance of complying with previously revised authentication procedures when high-risk situations are encountered. Additionally, Customer Service Quality Assurance will monitor CSRs for unauthorized disclosure and local managers will be held responsible for employee compliance with authentication requirements.

2. Consider identifying those verifiers, confidential to both the caller and the IRS, that are not available on the Internet and revising national guidelines so that CSRs are required to use them to authenticate call-in taxpayers. Additionally, consider revising the new computer screen used by CSRs to authenticate identities by highlighting the additional confidential items.

   Management's Response: Customer Service management, concerned with balancing disclosure requirements with service to taxpayers and avoiding possible burdensome authentication requirements for

both taxpayers and CSRs, has decided not to identify and require the use of those selected authentication verifiers that would be known to only the IRS and the taxpayer. To further emphasize authentication requirements, Customer Service management will issue a job aid to CSRs that will serve as a ready reference and will periodically address disclosure/authentication on the Servicewide Electronic Research Project during the filing season. Customer Service believes that revising the computer screen to highlight the confidential items will not be necessary if training is successful.

Office of Audit Comment: While we understand management's concern about the additional burden discouraging callers, IRS management needs to be prepared to step-up its controls if the proposed alternative enhancements do not work.

Conclusion

Customer Service implemented corrective actions related to establishing clear policies and guidelines for dealing with suspended and disbarred tax practitioners. However, its corrective actions did not effectively address control weaknesses regarding the disclosure of information over the telephone. The revised procedures did not require that CSRs use items of authentication that would be confidential to only the caller and the IRS. As a result, CSRs are at risk of releasing sensitive account data to telephone callers without first properly verifying their identities. This jeopardizes taxpayer privacy as well as the integrity of, and public confidence in, the IRS.

Management recently implemented improvements in its quality review process to monitor CSR activity, which should increase its ability to detect CSR errors. However, detection alone may not be sufficient to reduce the problem. Without increased management commitment in providing the necessary training and

enforcing compliance with procedures, the risk of unauthorized disclosure of taxpayer data will remain at an unacceptable level.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine the effectiveness of corrective actions to strengthen controls for authenticating the identity of taxpayers who telephone the Internal Revenue Service (IRS). Control weaknesses had been identified in the IRS Inspection Service (now Treasury Inspector General for Tax Administration) report titled, *Review of Protecting the Privacy of Tax Account Information* (Reference Number 075202, dated September 30, 1997). We also determined whether alternative authentication methods existed and if the IRS was considering them. To accomplish our objective, we:

I. Evaluated the effectiveness of the procedural changes implemented by management to strengthen controls for authenticating callers. To accomplish this, we:

   A. Obtained relevant national guidelines (Internal Revenue Manual and related handbook sections) that the IRS revised in response to the previous report's recommendations.

      1. Identified the revised identification criteria that Customer Service Representatives (CSR) are required to use to authenticate taxpayer identification, including both the minimum and the additional items that may be required for more risky situations, such as address changes.

      2. Determined if the additional verification data the IRS is asking for in its revised authentication procedures are readily available to the public.

   B. Tested the authenticating measures CSRs employ to ensure that a caller is entitled to the tax account information being sought.

      1. Tested the extent CSRs ask for the minimum or additional verification data. Auditors made 100 test calls requesting tax account information on their accounts or those of family members.

II. Identified if alternative authentication methods existed and if the IRS was considering them.

A. Researched various sources, including the Internet, and technical and trade publications and associations (e.g., Federation of Tax Administrators - a state tax agency trade group), Federal Reserve, banks, credit card companies, and brokerage firms, to identify alternative telephone authentication methods used in private industry.

B. Determined if the IRS had plans for implementing alternative authentication methods.

1. Determined whether use of caller ID (identification) was considered.

2. Discussed with the Office of Electronic Tax Administration the use of electronic filing Personal Identification Numbers as it pertains to the IRS' overall strategy.

3. Determined whether the authentication method the IRS has planned, allowing taxpayers who file electronically to have electronic access to their accounts as stated in the IRS Restructuring and Reform Act of 1998, Pub. L. No. 105-206, 112 Stat. 685 (1998), could have applicability to the telephone program.

III. Determined whether the IRS' new policies and procedures address the disclosure of information to suspended and disbarred practitioners.

A. Obtained and analyzed revised national guidelines and training modules pertaining to disclosure of taxpayer information to suspended and disbarred practitioners.

B. Determined whether the revisions provide the necessary guidance to clarify the misunderstandings cited in the prior report.

Appendix II

Major Contributors to This Report

Maurice S. Moody, Associate Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs)
Kerry R. Kilpatrick, Director
Richard Hayes, Audit Manager
Mark Nathan, Audit Manager
Edward Chin, Senior Auditor
Russell Martin, Senior Auditor
Richard Borst, Auditor
Dolores Castoro, Auditor
Charles Ekholm, Auditor

Appendix III

Report Distribution List

Deputy Commissioner Operations C:DO
Chief Operations Officer OP
Assistant Commissioner (Customer Service) OP:C
National Director, Customer Service - Telephone Operations Division OP:C:T
National Director for Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis M:O
Office of Management Controls M:CFO:A:M
Office of the Chief Counsel CC
Audit Liaison - Assistant Commissioner (Customer Service) OP:C:T:L

Appendix IV

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

COMMISSIONER

January 12, 2000

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

FROM: for Charles O. Rossotti
Commissioner of Internal Revenue

SUBJECT: Draft Audit Report – The Internal Revenue Service Needs to Improve Telephone Authentication Practices to Better Prevent Unauthorized Tax Account Disclosures

This memorandum consolidates our response to the recommendations contained in the above-referenced report. We appreciate that your review recognized the actions we have taken to reduce the risk of unauthorized disclosure to suspended/disbarred practitioners. Customer Service's establishment of clear policies and procedures, including a job aid for Internal Revenue Service's (IRS) field personnel, will prevent the disclosure of account information to such practitioners.

We are in the process of strengthening our policies and procedures, as described below, to more effectively and consistently authenticate the identity of all taxpayers who call in and request account information, particularly in high-risk situations. However, we also need to balance our disclosure requirements with service to customers. It is extremely important that we not take any action (or implement a new policy) that could discourage taxpayers from calling in and requesting account information simply because we have created burdensome requirements. We feel that the actions we are taking to strengthen our telephone authentication practices will not only prevent unauthorized tax account disclosures but will also enhance our service to our customers.

IDENTITY OF RECOMMENDATION/FINDING
Customer Service should provide refresher training for Customer Service Representatives (CSR), emphasizing the need for compliance with authentication requirements when high-risk situations are encountered. Ensure managers of CSRs enforce compliance.

ASSESSMENT OF CAUSE
Customer Service representatives have not been consistent in their application of authentication procedures to taxpayers who call in and request account information, particularly in high-risk situations. Treasury Inspector General for Tax Administration

(TIGTA) found that CSRs did not always ask for the required authentication items in spite of the fact that Customer Service management expanded the number of items that CSRs must request.

CORRECTIVE ACTIONS
Customer Service is in the process of providing Refresher training for all CSRs. This training stresses the importance of the revised authentication procedures, as outlined in Internal Revenue Manual (IRM) 21.2.3. Refresher training for call sites is due to be completed by early January 2000. Refresher training at all other sites will be ongoing through the end of March 2000. The training materials provided mirror the revised IRM instructions.

IMPLEMENTATION DATE
COMPLETED PROPOSED March 31, 2000

RESPONSIBLE OFFICIAL
National Director, Workforce Performance and Analysis Division (OP:C:W)

CORRECTIVE ACTION MONITORING PLAN
On an enterprise level, the Quality Assurance function will continue to monitor CSRs for unauthorized disclosure. On a local level (under the Chief, Customer Service Field Operations), managers will be responsible for ensuring their employees' compliance with authentication requirements.

IDENTITY OF RECOMMENDATION/FINDING
Customer Service should consider identifying those verifiers, confidential to both the caller and the IRS, that are not available on the Internet, and revising national guidelines so that CSRs are required to use them to authenticate call-in taxpayers. Additionally, consider revising the new computer screen used by CSRs to authenticate identities, and to highlight the additional confidential items.

ASSESSMENT OF CAUSE
Although Customer Service management expanded the number of items that CSRs must request to authenticate callers and further defined high-risk situations, some CSRs did not comply with the revised procedures. Thus, unauthorized disclosure of taxpayer information remains at risk.

CORRECTIVE ACTIONS
We have already strengthened our IRM to ***require*** use of the probes (which include items of authentication that are confidential to only the caller and the IRS) by CSRs, and we are in the process of training employees (as noted above) on use of the probes. In the past, Customer Service researched adding additional probes (i.e., mother's

maiden name) but found it to be unfeasible due to the negative impact (significant response delay) on taxpayers. We continue to feel that adding additional probes to authenticate call-in taxpayers will be burdensome to not only taxpayers but CSRs as well. Instead, we are emphasizing to CSRs that they are ***required*** to authenticate the identities of taxpayers. We will be issuing a job aid to CSRs that will serve as a ready reference on disclosure/authentication requirements. We will also address disclosure/authentication as a "hot-item" on Servicewide Electronic Research Project periodically during the filing season. Revising the computer screen to highlight the confidential items will not be necessary if we are successful in training our employees on authentication requirements.

IMPLEMENTATION DATE
COMPLETED PROPOSED April 30, 2000

RESPONSIBLE OFFICIAL
National Director, Compliance and Accounts Division (OP:C:A)

CORRECTIVE ACTION(S) MONITORING PLAN
The Quality Assurance Function will continue to monitor the CSRs for compliance with authentication requirements through the provisions of the Customer Service Quality Review Program (see IRM 21.10.1 dated 01/01/2000).