TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Proactive Processes to Identify and Mitigate Potential Misuse of Electronic Payment Systems Are Needed

April 23, 2018

Reference Number: 2018-40-031

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:
1 = Tax Return/Return Information
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions.
5 = Information Concerning a Pending Law Enforcement Proceeding

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.

PROACTIVE PROCESSES TO IDENTIFY AND MITIGATE POTENTIAL MISUSE OF ELECTRONIC PAYMENT SYSTEMS ARE NEEDED

Highlights

Final Report issued on April 23, 2018

Highlights of Reference Number: 2018-40-031 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The IRS uses the Electronic Federal Payment Posting System (EFPPS) to process and record payments received through the Department of Treasury's Electronic Federal Tax Payment System and payments received via paper check converted into electronic payments. During Calendar Year 2016, the IRS processed more than 170.8 million taxpayer payment transactions totaling more than $2.8 trillion through the EFPPS.

WHY TIGTA DID THE AUDIT

This audit was initiated as a result of an investigation conducted by TIGTA's Office of Investigations in which an individual used the IRS's **********1, 2 and 5********** **********1, 2 and 5**********. This audit assessed the IRS's processes and procedures to authenticate and validate payments made through the EFPPS.

WHAT TIGTA FOUND

The IRS reduced the maximum payment amount that can be submitted through the *******2******* ***2*** to reduce the risk of creating a ***2******* **********2**********. However, TIGTA identified that strengthened authentication is needed to mitigate potential misuse of **********2********** *****2***** as the current process is significantly inconsistent when compared with the extensive authentication processes used to validate taxpayer payments submitted through the Electronic Federal Tax Payment System or Direct Pay System. For example, our analysis of **********2********** payment transactions made between September 29, 2016, and December 14, 2016, identified 1,236 suspicious payments with *********2********** **********2********** ****2***** that were confirmed by the IRS's processes as valid. However, 1,084 of the payments could not post to an associated tax account because there was no active tax account for the taxpayer. The IRS advised us that the new **********2********** validation requirements that would address this concern have been **********2**********.

In addition, systemic controls did not ensure appropriate approval of changes to payment information when required. For example, technicians were able to approve each other's changes to a Taxpayer Identification Number and name control, even though internal guidelines require approval by a manager or designee. Our analysis of payment transactions for Calendar Year 2016 identified 13,279 payments totaling $281 million in which an EFPPS technician corrected both the Taxpayer Identification Number and name control associated with the payment. In July 2017, the IRS implemented a system change to address this concern.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Commissioner, Wage and Investment Division, ensure that expanded **********2********** authentication requirements are implemented without further delays to reduce the risk of misuse of the system.

The IRS agreed with this recommendation and has submitted the programming requirements for authentication controls in its annual maintenance request.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

April 23, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Proactive Processes to Identify and Mitigate Potential Misuse of Electronic Payment Systems Are Needed (Audit # 201740032)

This report presents the results of our review to evaluate the Internal Revenue Service's (IRS) processes and procedures to authenticate and validate payments made through the Electronic Federal Payment Posting System. This review is included in our Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

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

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

Background.....Page 1

Results of Review.....Page 4

Actions Were Taken to Reduce the Risk of Financial Institution Overdraft Resulting From Misuse of the *******2*******.....Page 4

Strengthened Authentication Is Needed to Mitigate Potential Misuse of the **********2**********.....Page 4

Recommendation 1:.....Page 6

Systemic Controls Did Not Ensure Appropriate Approval of Changes to Payment Information When Required.....Page 6

Appendices

Appendix I – Detailed Objective, Scope, and Methodology.....Page 8

Appendix II – Major Contributors to This Report.....Page 11

Appendix III – Report Distribution List.....Page 12

Appendix IV – Management's Response to the Draft Report.....Page 13

Abbreviations

CY	Calendar Year
EFPPS	Electronic Federal Payment Posting System
EFTPS	Electronic Federal Tax Payment System
e-file(d)	Electronically File(d)
IRS	Internal Revenue Service
TIN	Taxpayer Identification Number

Background

The Department of Treasury's Electronic Federal Tax Payment System (EFTPS) provides a free service for taxpayers to make Federal tax payments and for the Internal Revenue Service (IRS) to process these payments. Bank of America operates the EFTPS as the Treasury's Financial Agent and is responsible for moving taxpayer payments from the taxpayer to the Treasury General Account as well as reconciling payment data with the Federal Reserve System and transmitting the EFTPS payment and deposit information electronically to the IRS. Payments that are made using the EFTPS include Federal Tax Deposits (*i.e.*, deposits of employment tax, excise tax, and corporate income tax, by businesses), estimated tax payments by both individuals and businesses, and payments associated with electronically filed (e-filed) individual and business tax returns with a balance due. As of December 31, 2016, the IRS reported that there were 5.2 million individuals and 26 million businesses actively enrolled in the EFTPS.

In addition to payments initiated in the EFTPS, the EFTPS processes payments initiated via other payment methods that do not require a taxpayer to be enrolled in the EFTPS to submit their payment. These additional payment methods include:

- Direct Pay System - Individual taxpayers[1] can make payments to the IRS from their bank account at IRS.gov.
- Electronic Funds Withdrawal - Taxpayers that e-file their tax returns can initiate an electronic funds withdrawal from a bank account to make a payment. The IRS generates payment records from the e-file programs and routes these payment records to the EFTPS for processing.
- Credit and Debit Card Payments - Taxpayers can pay when filing a return or in response to a bill or notice using one of three credit and debit card payment processors. The payment processors validate the taxpayer's Taxpayer Identification Number (TIN)[2] with the IRS through the Treasury's Financial Agent. Once a TIN is validated, the payment processors prepare a payment file for processing through the EFTPS.

The Electronic Federal Payment Posting System (EFPPS) used to process and record EFTPS payments

The IRS uses the EFPPS to process and record EFTPS payments and to process payments received via paper check. This process includes converting paper checks received into electronic

[1] Business taxpayers are not eligible to make payments through the Direct Pay System.
[2] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an Employer Identification Number, a Social Security Number, or an Individual TIN.

payments, *i.e.*, Automated Clearing House[3] debits. During Calendar Year (CY)[4] 2016, the IRS processed more than 170.8 million payment transactions totaling more than $2.8 trillion through the EFPPS, of which paper checks accounted for approximately 2.3 million transactions totaling $6.1 billion.

Payment correction process

Prior to posting payments to a taxpayer's Master File[5] tax account, validation and edits are performed by the EFPPS to prepare the payment data for posting. The validation includes the matching of the TIN and name control[6] for the payment to the TIN and name control on an associated Master File tax account. The EFPPS also includes programming to automatically correct certain payment transaction errors. For example, if the name control on a payment transaction is blank, the system will use the name control identified during the Master File validation process.

Those payment transactions that do not pass EFPPS edits, or cannot be automatically corrected, are assigned to technicians in the IRS's EFPPS Corrections Unit for resolution. During the error correction process, EFPPS Corrections Unit technicians have the ability to change one or all of the following fields: TIN, Tax Period,[7] Tax Type,[8] and Name Control. The payment continues to go through the validation process until the information passes the validation check and the transaction is ready for processing to the associated Master File tax account. During CY 2016, the IRS corrected 495,391 of the 170.8 million payment transactions totaling $68.1 billion. This included:

- 225,894 payment transactions totaling $45.2 billion that were systemically corrected by the EFPPS.
- 269,497 payment transactions totaling $22.9 billion that were corrected by EFPPS Corrections Unit technicians.

This review was performed at the IRS Submission Processing Site in Ogden, Utah, and with information obtained from the Wage and Investment Division Headquarters in Atlanta, Georgia, and the Office of Information Technology in Washington, D.C., during the period February through December 2017. We conducted this performance audit in accordance with

[3] A funds transfer system which provides for the interbank clearing of electronic entries for participating financial institutions.
[4] The 12-consecutive-month period ending on December 31.
[5] The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.
[6] A name control is the first four letters in an individual's last name or the first four characters of the business name. However, there are exceptions to the formation of the business name control for special characters and spaces.
[7] Tax period is the month and year in which the length of liability ends for a particular return or payment transaction.
[8] Tax type is the type of tax by specific category (such as Form 941, *Employer's QUARTERLY Federal Tax Return*).

generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Actions Were Taken to Reduce the Risk of Financial Institution Overdraft Resulting From Misuse of the *******2*********

This audit was initiated as a result of an investigation conducted by our Office of Investigations in which an individual used the IRS's ********1********** ********1********** ********1********** ********1********** ********1********** ********1********** **********1**********.

To reduce the risk of similar occurrences to financial institutions, the IRS modified the maximum payment amount that can be submitted through its ********2*******. To determine what the maximum payment amount should be IRS management conducted an analysis of payments received between January 5, 2016, and December 19, 2016, greater than or equal to $1 million, that were made through the *******2*******. There were a total of 2,472 taxpayers that submitted payments greater than or equal to $1 million, with 97 taxpayers making payments totaling ****2**** or more. Based on this analysis, the IRS set the maximum dollar amount that can be processed using the**********2********** because fewer taxpayers would be required to make their payments via the *******2********.[9] It should be noted that the prior payment amount limitation was ****2****.

Strengthened Authentication Is Needed to Mitigate Potential Misuse of the **********2**********

Our review identified that **********2********** are required to provide ****2**** to the IRS for use in validating payments. Specifically, **********2********** send the **********2**********. In response, *****2****** **********2********** it verifies as valid. The authentication criteria used for credit and debit card processors is significantly inconsistent when compared with the extensiveness of the authentication processes used to validate taxpayer payments submitted through the EFTPS or the Direct Pay System. For example:

[9] **********2********** **********2**********.

- Payments initiated in the EFTPS require enrollment by the taxpayer. To enroll, the business or individual must provide entity information including their TIN, name, telephone number, and contact information. After the IRS validates enrollment entity information, the IRS mails a Personal Identification Number within five to seven business days to the taxpayer's address of record (*i.e.*, current address on the taxpayer's tax account). To submit payments, the taxpayer is required to provide their TIN, EFTPS Personal Identification Number, and a password they established as part of the enrollment process. The IRS uses this information to authenticate the taxpayer.
- The Direct Pay System does not require enrollment. However, the IRS requires taxpayers to verify their identity when making a payment. This includes providing their name, TIN, filing status, date of birth, and address.

Of additional concern is the fact that unscrupulous individuals can use *********2********** **********2**********. For example, an unscrupulous individual can **********2********** **********2********** **********2********** **********2********** **********2********** **********2********* transactions made between September 29, 2016, and December 14, 2016, identified potential misuse of this payment process. We identified 1,236 payments with amounts ranging from *********2********** **********2********. Although the TINs associated with these 1,236 payments were confirmed by the IRS's systems as valid, a total of 1,084 (88 percent) of the payments could not post to an associated tax account on the IRS's Master File because there was no active tax account for the taxpayer. For the remaining 152 payments, the payments posted to the taxpayer's account, but there was no amount owed by the taxpayer. Both scenarios raise concern as to the potential misuse of the payment process as it brings into question why a taxpayer would submit a payment on a tax account where they had no recent tax return filings or when no amount was owed.

When we discussed our analysis with IRS management, they acknowledged that the payments we identified were questionable. Management stated that they began updating ******2****** ****2**** validation requirements in CY 2016 to include requiring taxpayers to provide their *********2********* for authentication. IRS management noted that this change was initiated in response to concerns regarding multiple ******2******* attempts they identified in CY 2015. Specifically, the IRS identified a number of **********2********** payments that did not post to taxpayers' accounts.

On March 30, 2017, the IRS advised us that the new credit and debit card validation requirements were scheduled for implementation in January 2018. However, on October 5, 2017, IRS management stated that they **********2**********. The delay resulted from testing of the new validation requirements which identified that **2*** ********2******* were unable to **********2**********

**********2**********,[10] **********2**********. The delay will allow the **********2******** time to update their processes to comply with these new validation requirements.

IRS management explained that the **********2********** plays a major role in the card processors' ability to accept tax payments from taxpayers who have chosen this as the payment option. The volume of payments received using the **********2********** is minimal when compared to those **********2********** **********2**********. The IRS received more than 6 million ********2********** payments totaling more than $5.9 billion in CY 2016. Of these, the IRS reported that 888,703 (14 percent) payments totaling more than $422 million (7 percent) were received through the **********2**********.

Although the IRS initially identified concerns regarding the potential misuse of this payment process in CY 2015, some three years later, the IRS still has not taken the necessary actions to reduce the ability of unscrupulous individuals to use this system to potentially commit fraud. With the risks associated with tax fraud involving identity theft and how it is evolving and becoming more complex, delaying the implementation of authentication strengthening processes continues to be a concern. IRS management noted that for the 2018 Filing Season,[11] they will monitor credit and debit card payments to identify any suspicious payments.

Recommendation

Recommendation 1**:** The Commissioner, Wage and Investment Division, should ensure that expanded **********2********** authentication requirements are implemented without further delays to reduce the risk of misuse of the system.

> ***Management's Response:*** The IRS agreed with this recommendation and has submitted the programming requirements for authentication controls in its annual maintenance request.

Systemic Controls Did Not Ensure Appropriate Approval of Changes to Payment Information When Required

Our review identified that technicians are able to approve each other's changes to a TIN and name control without a manager or designee review. Analysis of payment transactions for CY 2016 identified 13,279 payments totaling $281 million in which an EFPPS technician changed both the TIN and name control associated with the payment. For each of these payments, the EFPPS identified the TIN and name control associated with a payment as invalid

[10] The Interactive Voice Response System is a service provided by each of the credit and debit card processors to allow taxpayers to make payments by telephone using a voice prompt system.
[11] The period from January through mid-April when most individual income tax returns are filed.

requiring a technician to research tax accounts in an attempt to correct the error. EFPPS technicians were able to approve each other's changes to a TIN and name control, even though internal guidelines require a manager or designee to review and approve TIN and name control changes.

When we shared our concerns with IRS management on May 12, 2017, they indicated that a planned EFPPS systemic update will prevent technicians from approving other technician's TIN and name control corrections. On May 26, 2017, the IRS revised its internal guidelines, to require, in the absence of the EFPPS manager or designee, a quality review employee perform the review of TIN and name control changes until the systemic EFPPS update is made. In addition, the EFPPS manager will verify that all approvals were performed by the EFPPS manager, designee, or quality review employee as required. Finally, IRS management advised us that they updated the systemic controls over TIN and name control corrections in July 2017 to restrict approvals to managers and approved designees as required. Our follow-up review confirmed this and, as such, we are not making any recommendations.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the IRS's processes and procedures to authenticate and validate payments made through the EFPPS. To accomplish this objective, we:

I. Evaluated the IRS's processes and procedures to identify and mitigate potential misuse of electronic Federal tax payment systems.

A. Determined if the IRS implemented sufficient payment amount limitations for payments received via the *********2**********2**********.

1. Discussed with IRS management the procedures implemented to ensure that payment amounts received are within reasonable limits.

2. Identified the payment limitations implemented for tax payments received through the **********2**********2**********.

3. Reviewed IRS documentation supporting the analysis conducted for the current payment amount limitations.

B. Determined if the IRS implemented effective processes and procedures to identify suspicious payment activity.

1. Discussed with IRS management the processes and procedures established to identify suspicious payments.

2. Reviewed suspicious activity cases identified by the IRS during CY 2016 to determine if the actions taken by the IRS were sufficient.

3. Obtained an EFPPS extract of tax payments made from January 1, 2016, through December 31, 2016, and evaluated the distribution of payment amounts to identify suspicious payment activity, *e.g.*, ******2******, including payments that did not post to the taxpayer's account.

II. Evaluated IRS processes and procedures to authenticate taxpayers making electronic payments.

A. Identified and evaluated IRS authentication of taxpayers making payments through the IRS Direct Pay System, electronic funds withdrawal, and the credit and debit card payment methods.

B. Evaluated information that the IRS receives and transmits during the authentication and validation process.

C. Identified any planned system changes for weaknesses identified and proposed implementation dates.

III. Evaluated the effectiveness of controls to prevent payments from posting to the wrong taxpayer account during the error correction process.

A. Reviewed the Internal Revenue Manual to identify the processes and procedures for the error correction process, including auto corrections and corrections to credit and debit card payments performed outside of the EFPPS.

B. Assessed whether IRS policy and procedures requiring managerial approval of payment transactions with changes to both the TIN[1] and name control[2] are being followed.

C. Ensured that changes to IRS procedures for the review and approval of payment transactions with changes to both the TIN and name control are in place and functioning as intended.

Data validation methodology

For this review, we relied on IRS-provided CY 2016 payment transaction and error correction data extracted from the EFPPS. We also relied on tax account transaction data extracted from the Individual Master File.[3] To assess the reliability of computer-processed data, programmers within Strategic Data Services validated the data extract files while we ensured that the data extract contained the specific data elements we requested and that the data elements were accurate. In addition, we selected judgmental samples[4] and verified that the data in the extracts were the same as the data contained in the IRS's Integrated Data Retrieval System.[5] We determined that the data were sufficiently reliable for our intended purpose.

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

[1] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the nature of the taxpayer, the TIN is an Employer Identification Number, a Social Security Number, or an Individual TIN.
[2] A name control is the first four letters in an individual's last name or the first four characters of the business name. However, there are exceptions to the formation of the business name control for special characters and spaces.
[3] The IRS database that maintains transactions or records of individual tax accounts. This database includes individual, business, and employee plans and exempt organizations data.
[4] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[5] IRS computer system capable of retrieving or updating stored information. It works in conjunction with a taxpayer's account records.

for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: the IRS's policies and procedures for the receipt and processing of Federal tax payments. We also evaluated controls to authenticate taxpayers making electronic payments, to identify and mitigate potential misuse of electronic Federal tax payment systems, and to prevent payments from posting to the wrong taxpayer account during the error correction process. We accomplished this by interviewing IRS management and reviewing the Internal Revenue Manual, management information reports, and key system documentation related to the receipt and processing of Federal tax payments.

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
Diana M. Tengesdal, Director
Darryl Roth, Audit Manager
Van Warmke, Lead Auditor
Ashley Burton, Auditor
Taylor McDonald, Auditor

Appendix III

Report Distribution List

Commissioner, Wage and Investment Division
Deputy Commissioner, Wage and Investment Division
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Associate Chief Information Officer, Applications Development
Director, Customer Account Services, Wage and Investment Division
Director, Submission Processing, Wage and Investment Division
Director, Office of Audit Coordination

Appendix IV

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

March 30, 2018

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Draft Audit Report - Proactive Processes to Identify and Mitigate Potential Misuse of Electronic Payment Systems Are Needed (Audit# 201740032)

Thank you for the opportunity to review the subject draft report and provide comments. The IRS uses the Electronic Federal Payment Posting System (EFPPS) to process and record payments received through the Department of Treasury's Electronic Federal Tax Payment System. Payments received as paper checks are converted into electronic payments and processed through the EFPPS as well. During the 2016 calendar year, more than 170.8 million payments transactions were processed through the EFPPS, totaling over $2.8 trillion.

We intended to implement ********** 2********** ********** 2********** ********** 2********** ********** 2********** ********** 2********** ********** 2**** In 2016, more than 888,700 payments worth over $422.5 million were initiated through the *****2*****.

********** 2********** **********2**********. This decision was made with due consideration of risks and the best interests of all parties; including taxpayers who choose this method of payment to meet their tax obligations. We agree with the recommendation to implement the expanded authentication controls and have submitted the programming requirements with our annual maintenance request.

Attached are our comments and proposed actions to your recommendations. If you have any questions, please contact me, or a member of your staff may contact James P. Clifford, Director, Customer Account Services, Wage and Investment Division, at (470) 639-3504

Attachment

Attachment

Recommendation

RECOMMENDATION 1
The Commissioner, Wage and Investment Division, should ensure that expanded **2** *********2********** authentication requirements are implemented without further delays to reduce the risk of misuse of the system.

CORRECTIVE ACTION
We agree with this recommendation. The expanded **********2********** authentication requirements have been included in an annual maintenance request (Unified Work Request 208073). **********2**********2**********2**********2**********.

IMPLEMENTATION DATE
N/A

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

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.