

OIG

Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

Audit Report

Access Controls for the Social
Security Number Verification Service

A-03-12-11204 | April 2013

MEMORANDUM

Date: April 18, 2013

Refer To:

To: The Commissioner

From: Inspector General

Subject: Access Controls for the Social Security Number Verification Service (A-03-12-11204)

The attached final report presents the results of our audit. Our objective was to determine the effectiveness of the Social Security Administration's (SSA) controls to detect whether companies were improperly using SSA's employer verification programs for non-employment purposes.

If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.



Patrick P. O'Carroll, Jr.

Attachment

Access Controls for the Social Security Number Verification Service

A-03-12-11204



April 2013

Office of Audit Report Summary

Objective

To determine the effectiveness of the Social Security Administration's (SSA) controls to detect whether companies were improperly using SSA's employer verification programs for non-employment purposes.

Background

In 2005, SSA implemented the Social Security Number Verification Service (SSNVS) to assist employers with accurate wage reporting and increase the ease and convenience of verifying employee names and Social Security numbers (SSN).

SSA developed several fraud detection reports to help detect whether registered companies were properly using SSNVS. The SSNVS Failed Master Earnings File (MEF) check report helps ensure there is an employer/employee relationship between the user and individual verified. The Same Name/Different SSN Potential Fraud Identification report identifies users attempting to verify more than 50 combinations of the same name and different SSN for a single Employer Identification Number (EIN). The Same SSN/Different Name Potential Fraud Identification report identifies users attempting to verify more than 50 combinations of the same SSN and different name for a single EIN.

Our Findings

The controls to detect whether employers were improperly using SSA's SSNVS program for non-employment purposes need to be improved. The Failed MEF Check reports for Calendar Years 2009 and 2010, which included about 26 million transactions, were unreliable. The reports contained numerous false positive (meaning an employer/employee relationship existed), non-SSNVS, and duplicate transactions, which made it difficult for SSA staff to identify instances where employers may have been verifying individuals who were not employees.

The Same Name/Different SSN and Same SSN/Different Name Potential Fraud Identification reports effectively identified instances where registered companies may have been searching for valid name/SSN combinations. Our review of the reports generated in Fiscal Year 2010, found that seven employers may have inappropriately used SSNVS to search for valid name/SSN combinations for non-employees. Although SSA staff agreed that four of the seven employers may have used SSNVS for non-employment purposes, they were not consistent in contacting these employers to inform them about the appropriate use of SSNVS.

Our Recommendations

1. Determine whether to modify the existing Failed MEF Check report to ensure it is a reliable tool to detect whether registered companies are improperly using SSNVS for non-employment purposes or develop a more useful fraud detection tool.
2. Conduct outreach with registered companies regarding using the appropriate EIN when submitting verifications to reduce the number of transactions posted to the Failed MEF Check report.
3. Develop consistent procedures for contacting employers who appear on the fraud detection reports to ensure the appropriate use of SSNVS.

SSA agreed with all our recommendations.

TABLE OF CONTENTS

Objective	1
Background	1
Results of Review	3
SSNVS Failed MEF Check Report	3
Non-SSNVS Transactions Posted to the Failed MEF Check Report	5
Duplicate Transactions Posted to the Failed MEF Check Report	6
Fraud Identification Reports	7
Conclusions and Recommendations	9
Agency Comments	9
Appendix A – Social Security Number Verification Service	A-1
Appendix B – Scope and Methodology	B-1
Appendix C – Agency Comments	C-1
Appendix D – Major Contributors	D-1

ABBREVIATIONS

BSO	Business Services Online
CBSV	Consent Based Social Security Number Verification
CY	Calendar Year
EIN	Employer Identification Number
FY	Fiscal Year
IRS	Internal Revenue Service
MEF	Master Earnings File
SSA	Social Security Administration
SSN	Social Security Number
SSNVS	Social Security Number Verification Service

Form

W-2	<i>Wage and Tax Statements</i>
-----	--------------------------------

OBJECTIVE

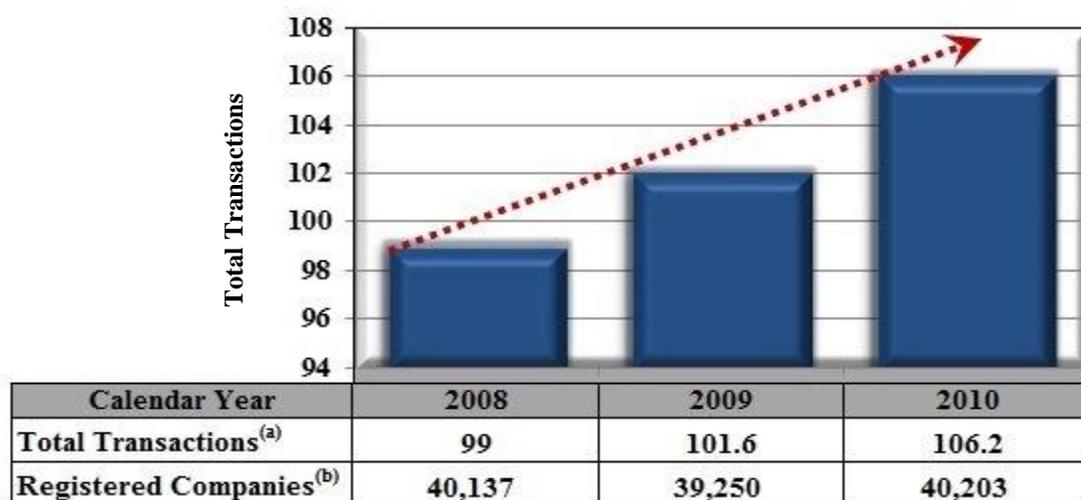
Our objective was to determine the effectiveness of the Social Security Administration's (SSA) controls to detect whether companies were improperly using SSA's employer verification programs for non-employment purposes.

BACKGROUND

In 2005, SSA implemented the Social Security Number Verification Service (SSNVS) to assist employers with accurate wage reporting and increase the ease and convenience of verifying employee names and Social Security numbers (SSN). SSNVS is a free verification program that allows registered companies (employers and submitters) to verify employees' names and SSNs against SSA's records before submitting *Wage and Tax Statements* (Form W-2) to SSA.¹

As shown in Figure 1, the volume and use of SSNVS increased from Calendar Years (CY) 2008 to 2010. In CY 2008, SSA processed about 99 million transactions, and, in CY 2010, it processed about 106 million transactions, an increase of about 7 million transactions over the 3-year period. In addition, the number of companies that registered and used the service decreased in 2009 but increased in 2010. The net increase was 66 companies, 40,137 in CY 2008 to 40,203 in CY 2010.

Figure 1: SSNVS Transactions for CYs 2008 Through 2010



Notes:

- (a) Total transactions are in the millions.
- (b) Total registered companies that used SSNVS.

¹ See Appendix A for more information about SSNVS.

Registered companies can use SSNVS to verify current or former employees for wage reporting purposes.² It is appropriate to use SSNVS only when an official employer/employee relationship has been established. SSA defines an employer/employee relationship when one of the following has occurred.³

- The employer has offered, and the person being hired has accepted, employment (even though he/she has not started working).
- The future employee has completed the paperwork to establish a payroll record.

Registered companies cannot use SSNVS to verify potential new hires, contractors, or individuals related to other business functions. Companies that need to verify SSNs for non-employment purposes (such as identity, credit, or mortgages) can use SSA's Consent Based Social Security Number Verification (CBSV) program. To use CBSV, companies must obtain valid consent⁴ from the individual before verifying their SSN and pay SSA in advance a \$1.05 fee per transaction.⁵ Because both verification programs are available to the public, there is a risk that companies may try to avoid CBSV's consent and cost requirements by using SSNVS for non-employment purposes.

In 2005, SSA developed several fraud detection reports to help detect whether registered users were improperly using SSNVS.

- **SSNVS Failed Master Earnings File (MEF) Check Report.** Compares a valid name/SSN combination submitted for verification against SSA's MEF to determine whether the individual worked for the same company that submitted the verification. The MEF contains all earnings data reported by employers and self-employed individuals. This check helps ensure there is an employer/employee relationship. If the data do not match, the verification data are copied to the report for SSA staff to review.
- **Same Name/Different SSN Potential Fraud Identification Report.** The weekly report identifies users attempting to verify more than 50 combinations of the same name and different SSN for a single Employer Identification Number (EIN). SSA compiles the data on a rolling 6-month basis to determine whether companies are phishing for a valid name/SSN combination. The report identifies up to 500 names.

² When registering for SSNVS, users attest they are verifying SSNs solely to ensure the records of current or former employees are correct for completing Internal Revenue Service (IRS) Form W-2.

³ SSA, Business Services Online Social Security Number Verification Service (SSNVS) Handbook, September 2011.

⁴ Obtaining consent is required by the *Privacy Act of 1974*, as amended. See 5 U.S.C. § 552a (b).

⁵ In Fiscal Year (FY) 2009, SSA implemented the CBSV program to assist companies with consent-based SSN verification for non-program-related reasons. At that time, the cost per transaction was \$5.00, but in FY 2012, the cost was reduced to \$1.05.

- **Same SSN/Different Name Potential Fraud Identification Report.** The weekly report identifies users attempting to verify more than 50 combinations of the same SSN and different name for a single EIN. SSA compiles the data on a rolling 6-month basis to determine whether companies are phishing for a valid name/SSN combination. The report identifies up to 500 SSNs.

RESULTS OF REVIEW

The controls to detect whether companies were improperly using SSNVS for non-employment purposes need to be improved. The Failed MEF Check reports for CYs 2009 and 2010, which included about 26 million transactions, were unreliable. The reports contained numerous false positive (meaning an employer/employee relationship existed), non-SSNVS, and duplicate transactions, which made it difficult for SSA staff to identify instances where employers may have been verifying individuals who were not employees. Specifically, 129 (65 percent) of the 200 sample transactions we reviewed were posted to the reports even though there was a verified employer/employee relationship between registered companies and individuals. The postings occurred because either registered companies did not use the same EINs for verification and wage reporting or SSA generated the reports before the wages were posted to the MEF. In addition, we found that 1.6 million of the 26 million transactions posted to the Failed MEF Check reports did not relate to SSNVS. We determined that 1.2 million (79 percent) of these transactions related to CBSV and were erroneously posted to the Failed MEF Check reports because of a programming error. Lastly, we found that 4.2 million transactions were duplicates that should have been removed before the reports were generated.

Further, we found that both the Same Name/Different SSN and Same SSN/Different Name Potential Fraud Identification reports effectively identified instances where registered companies may have been searching for valid name/SSN combinations. Our review of the reports generated in FY 2010 found seven employers may have inappropriately used SSNVS to search for valid name/SSN combinations for non-employees. Although SSA staff agreed that four of the seven employers may have used SSNVS for non-employment purposes, they were not consistent in contacting these employers to inform them about the appropriate use of SSNVS.

SSNVS Failed MEF Check Report

As shown in Table 1, the Failed MEF Check reports for the 2-year period contained approximately 26 million records. The 2009 SSNVS Failed MEF Check report contained about 2.7 million records related to 4,149 registered companies, and the 2010 report included approximately 23.4 million records related to 34,564 registered companies. This was a 20.7-million record increase over 1 year. When compared to the total number of records submitted to SSNVS for both years, the 2009 Failed MEF Check data represented 3 percent of the transactions and 11 percent of the companies, and the 2010 Failed MEF Check data represented 22 percent of the transactions and 86 percent of the companies. We discussed with Agency staff why there was such a significant increase in the number of transactions posted to the Failed MEF Check reports from 2009 to 2010; however, they could not provide an explanation for the significant increase.

Table 1: Failed MEF Check Report for CYs 2009 to 2010

CY	Total SSNVS Transactions ^(a)	Total Registered Companies	MEF Check Transactions ^(a)	MEF Check Registered Companies	Percent of Transactions	Percent of Registered Companies
2009	101.6	39,250	2.7	4,149	3	11
2010	106.2	40,203	23.4	34,564	22	86
Total	207.8		26.1			

Note: (a) Records are in millions.

To understand why the Failed MEF Check reports included such a significant number of transactions, we reviewed a sample of 200 transactions related to 81 employers for the 2-year period. We found the reports had limited value for SSA staff to detect SSNVS misuse because 129 (65 percent) of the 200 transactions were false positive transactions:

- 98 transactions (49 percent) related to employers using more than 1 of their EINs for verification and wage reporting. While a verified employee/employer relationship existed between employers and individuals, the employers did not use the same EIN for verification and wage reporting, causing SSA to post the transactions to the Failed MEF Check reports. SSA's policy requires that the submitter provide the EIN of the employer who reports the wages for verification.⁶ SSA should take steps to remind employers about this requirement to help keep these types of transactions from being erroneously posted to the report.
- 27 transactions (14 percent) related to submitters using their own EINs for verification even though SSA's policy requires that the submitter provide the EIN of the employer who reports the wages for verification. We found submitters (that is, companies that conducted background checks, processed payroll, and provided staffing service) used their EINs to verify individuals, but employers who actually hired the individuals reported the wages. As a result, the EINs did not match, causing SSA to post false positive transactions to the Failed MEF Check reports.
- 10 transactions (5 percent) were submitted to CBSV for verification instead of SSNVS. Because companies use CBSV for non-employment purposes, there would not be an employer/employee relationship between the companies and the individuals verified. These records should not have been included on Failed MEF Check reports. We discuss this issue in more detail later in the report.
- 4 transactions (2 percent) were erroneously posted to the Failed MEF Check report because of timing issues. Although there was an employee/employer relationship for the four individuals, SSA posted the transactions to the Failed MEF Check report because the report

⁶ SSA, Business Services Online Social Security Number Verification Service (SSNVS) Handbook, September 2011.

was generated before the wages were posted to the MEF. The 2009 SSNVS Failed MEF Check report was generated in early April 2010, but the wages were not posted to the MEF until the end of April 2010. Had SSA generated the report later in the year when it received a majority of the wage information from employers, these records would not have been included on the report.

The remaining 61 transactions (30 percent) could have related to the improper use of SSNVS because we were not able to confirm whether there was an employer/employee relationship. However, these transactions may also relate to the integrity issues discussed below.

Non-SSNVS Transactions Posted to the Failed MEF Check Report

We found several integrity issues with the Failed MEF Check reports that made them unreliable and not useful for SSA staff to detect whether companies were misusing SSNVS. For example, the 2009 and 2010 Failed MEF Check reports contained about 1.6 million transactions that did not relate to SSNVS (see Table 2). Specifically, in 2009, there were about 180,000 (7 percent) more transactions on the Failed MEF Check report than submitted through SSNVS for 11 companies, and in 2010, the report contained an additional 1.4 million (6 percent) transactions related to 11,429 companies.

Of the 1.6 million transactions, we determined that 1.2 million (79 percent) transactions related to CBSV rather than SSNVS.⁷ In 2009, 6 companies submitted about 172,000 CBSV verifications and in 2010, 51 companies submitted about 1.1 million verifications. Because CBSV is a verification program for non-employment purposes, the transactions met the Failed MEF Check report criteria and were erroneously posted to the reports. A programming error caused the CBSV transactions to be posted to the Failed MEF Check report. Since both SSNVS and CBSV are services offered under Business Services Online (BSO), a suite of Internet services for businesses and employers to exchange information with SSA over the Internet,⁸ SSA staff did not select the SSNVS role identifier when generating the Failed MEF Check reports. Selecting only the SSNVS role identifier would have eliminated CBSV transactions from inclusion in Failed MEF Check reports.

We were not able to determine why the remaining 335,000 transactions (21 percent) were posted to the Failed MEF Check reports. It is possible these transactions related to other services offered under BSO.

⁷ These records represent an exact match on the following data fields: EIN, user personal identification number, SSN, and first and last name.

⁸ BSO allows employers to report Forms W-2 to the Agency electronically. However, BSO also offers other services, such as SSNVS; CBSV; and representative, attorney and non-attorney business activities.

Table 2: Non-SSNVS Transactions for CYs 2009 and 2010

CY	Total Non-SSNVS Transactions	CBSV		Unknown	
		Transactions	Percent	Transactions	Percent
2009	180,000	172,000	96	8,000	4
2010	1,400,000	1,073,000	77	327,000	23
Total	1,580,000	1,245,000	79	335,000	21

Duplicate Transactions Posted to the Failed MEF Check Report

SSA's policy⁹ for producing the Failed MEF Check report requires that staff remove duplicate transactions before generating the report. A duplicate transaction involves an exact match on certain data fields, such as the EIN, user identification number,¹⁰ SSN, and name. However, we found both reports included approximately 4.2 million duplicate transactions (see Table 3). The 2009 report contained about 461,000 (17 percent) duplicate transactions related to 510 employers, and the 2010 report contained about 3.7 million duplicate transactions (16 percent) related to 3,172 employers. SSA should have removed the duplicate transactions from the reports to avoid wasting valuable staff resources researching and analyzing these transactions.

Table 3: Duplicate Transactions for CYs 2009 and 2010

CY	MEF Check Transactions	MEF Check Registered Companies	Duplicate Transactions	Duplicate Companies	Percent of Transactions
2009	2,700,000	4,149	461,000	510	17
2010	23,400,000	34,564	3,700,000	3,172	16
Total	26,100,000		4,161,000		16

Since the Failed MEF Check report was implemented in 2005, SSA has not used it to remove or block companies' access to SSNVS because the reports have not been a useful tool to identify potential misuse. Because SSNVS is used to ensure accurate wage reporting and SSA processes over 100 million transactions annually, the Agency needs to determine whether to modify the existing Failed MEF Check report to help ensure registered companies are using SSNVS as intended or develop a more useful fraud detection tool.

⁹ SSA, Social Security Number Verification Service (SSNVS) Detailed System Specifications (DSS) Chapter 7-Reports, April 2009, page 38.

¹⁰ The user identification number is a unique number assigned to users when they register for BSO services such as SSNVS and CBSV.

Fraud Identification Reports

Both the Same Name/Different SSN and Same SSN/Different Name Potential Fraud Identification reports effectively identified instances where registered companies may have been phishing¹¹ for valid name/SSN combinations. Based on our review of the reports generated in FY 2010, we found that seven employers identified on the reports may have used SSNVS inappropriately to search for valid name/SSN combinations (see Table 4).

Table 4: Analysis of FY 2010 Potential Fraud Identification Reports

Same Name/Different SSN Report	Report	Same Names	Different SSNs	Employers
	Potential Phishing	42	8,258	4 ^(a)
	Submission Errors	36	32,374	6
	Total:	78	40,632	10
Same SSN/Different Name Report	Report	Same SSNs	Different Names	Employers
	Potential Phishing	34	2,085	4 ^(a)
	Submission Errors	5	527	3
	Total:	39	2,612	7

Note: (a) One employer appeared on both fraud reports. Thus, seven employers were potentially searching for valid name/SSN combinations.

Same Name/Different SSN Potential Fraud Identification Reports: The Same Name/Different SSN Potential Fraud Identification reports showed that four employers could have used SSNVS inappropriately to search for valid name/SSN combinations. The employers submitted 42 names associated with 8,258 different SSNs, ranging from 51 to 1,542 different SSNs. The transactions appeared suspicious because the employers verified names with similar SSNs that varied by one or two digits. For example, an employer in the food and beverage industry verified a name with 55 different SSNs where only 1 digit was different, indicating the employer may have been searching for a valid name/SSN combination.

Furthermore, we found that an employer who was a State prison agency submitted a majority of the transactions that appeared on the fraud reports. The employer submitted 28 (67 percent) of the 42 names associated with 7,125 SSNs. It appeared this employer was phishing for a valid name/SSN combination because the employer submitted similar names for verification. In addition, we were not able to find any evidence that the employer had reported any wages for most of the individuals, leading us to believe the verifications were not related to wage reporting.

¹¹ Phishing is the act of attempting to acquire personal information (such as a valid name and SSN combination) that will be used for an illegal purpose.

The remaining six employers appeared on the fraud report because of submission errors. While the reports showed the employers submitted 35 names associated with 32,374 different SSNS, the reported names described company names or known missing/bad data. For instance, an employer included “NOT NOT and SSN BAD” in the name field.

Same SSN/Different Name Potential Fraud Identification Reports: The Same SSN/Different Name Potential Fraud Identification reports showed that four employers could have used SSNVS inappropriately to search for valid name/SSN combinations. The employers submitted 34 SSNs associated with 2,085 different names, ranging from 51 to 74 different names. The State prison agency submitted 30 (88 percent) of the 34 SSNs associated with 1,840 names. The transactions appeared suspicious because the SSNs were reported with names that appeared to be legitimate. Further, we found the 34 SSNs were valid but did not belong to any of the individuals for whom they had been submitted for verification. Moreover, none of the employers reported any wages to SSA using any of the name/SSN combinations indicating the verifications were not related to wage reporting.

The remaining 3 employers who reported 5 SSNs associated with 527 names appeared on the fraud reports because of submission errors. They submitted data in the name field, such as names of companies or bad data, that did not appear to be legitimate. For example, one employer reported a valid SSN with names such as “Mistake Mistake and Account Suspense.”

SSA staff agreed that four of the seven employers who appeared on both fraud reports had inappropriately used SSNVS. At the time of our review, SSA staff had only contacted one of the employers about their inappropriate activity and requested that they stop. The Agency did not contact the other three employers because their activity did not appear to be recurring. While the inappropriate use may not have been repetitive, SSA staff needs to ensure employers have a clear understanding of the various verification programs the Agency offered. Companies that need to verify SSNs for non-employment purposes (such as identity, credit, or mortgages) should be using CBSV, which requires that companies obtain a valid consent from the individual before verifying their SSN and paying a fee of \$1.05 per transaction. Furthermore, since the verifications were inappropriate and the employers may not have obtained proper consent,¹² these transactions could represent an improper disclosure.

For the remaining three employers, SSA concluded that their activity was associated with submission errors. SSA staff did not contact two of the employers because they based their conclusions on the fact that the employers used a fictitious SSN or entered only the first initial when submitting names. SSA staff contacted the State prison agency and was informed that a logic error had occurred when the State prison agency uploaded its files, causing names to be repeated with different SSNs. However, of the 28 names that appeared on the Same Name/Different SSN Potential Fraud Identification reports, we found 26 were reported with valid name/SSN combinations, meaning the reported names and SSNs matched SSA’s records.

¹² SSA, Program Operations Manual System, GN 03305.001 Disclosure With Consent – General, (September 12, 2005).

The number of valid name/SSN combinations for the 26 names ranged from 7 to 53, totaling 805. Based on our review of SSA's earnings records, the State prison did not report any wages for 802 of the 805 individuals indicating the verifications were not related to wage reporting. However, SSA's records showed that 132 of these individuals had a prison record.

CONCLUSIONS AND RECOMMENDATIONS

SSA processes over 100 million SSNVS transactions annually, so the Agency needs to ensure it has proper controls in place to detect whether registered companies are using SSNVS to ensure accurate wage reporting. Our review found that SSA's Failed MEF Check reports were not serving the purpose for which they were intended, which was to detect whether employers were improperly using SSNVS for non-employment purposes. The 2009 and 2010 Failed MEF Check reports, which included about 26 million verification transactions, were unreliable because they included numerous false positive, non-SSNVS, and duplicate transactions, which made it difficult for SSA staff to identify instances where employers may have been verifying individuals who were not employees.

Further, while both the Same Name/Different SSN and Same SSN/Different Name Potential Identification Fraud reports effectively identified instances where registered companies may have been phishing for valid name/SSN combinations, the monitoring controls over the reports could be improved. We reviewed the reports generated in FY 2010 and identified seven employers who may have used SSNVS inappropriately to search for valid name/SSN combinations for non-employees. However, SSA did not consistently contact the employers who appeared on the fraud reports to confirm whether their activity was inappropriate and to inform them of the proper use of SSNVS.

Accordingly, we recommend that SSA:

1. Determine whether to modify the existing Failed MEF Check report to ensure it is a reliable tool to detect whether registered companies are improperly using SSNVS for non-employment purposes or develop a more useful fraud detection tool.
2. Conduct outreach with registered companies regarding using the appropriate EIN when submitting verifications to reduce the number of transactions posted to the Failed MEF Check report.
3. Develop consistent procedures for contacting employers who appear on the fraud detection reports to ensure the appropriate use of SSNVS.

AGENCY COMMENTS

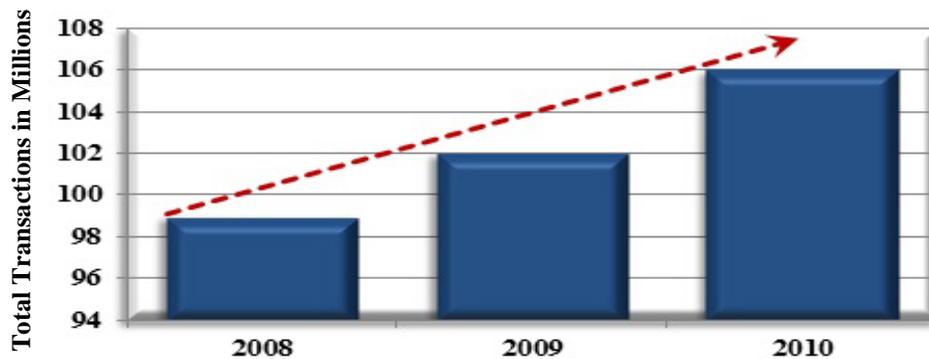
SSA agreed with our recommendations. The Agency's comments are included in Appendix C.

APPENDICES

Appendix A – SOCIAL SECURITY NUMBER VERIFICATION SERVICE

To increase the ease and convenience of verifying employee names and Social Security numbers (SSN), the Agency developed the Social Security Number Verification Service (SSNVS). SSNVS is a free online program, with a batch option, that allows employers and submitters (that is, companies that conduct background checks, process payroll, and provide staffing service) to verify employees' names and SSNs. SSNVS ensures employees' names and SSNs match the Social Security Administration's (SSA) records before their wage reports are submitted to SSA. As of Calendar Year (CY) 2010, SSNVS had processed approximately 106.2 million transactions for about 40,000 employers. As illustrated in Figure 1, SSNVS' use increased by about 7 million transactions (7-percent increase).

Figure 1: SSNVS Transactions for CYs 2008 Through 2010



To access SSNVS, employers and third parties must first register online at SSA's Business Services Online (BSO) Website. After registration, SSA mails an activation code,¹ which is needed to gain access to SSNVS, to the address the Internal Revenue Service has on file.² Once the registered companies activate SSNVS using their user identification number³ and the activation code, they can start submitting verifications. Registered companies can:

- Submit up to 10 employee names and SSNs (per screen) via the online SSNVS and receive immediate results.

¹ The activation code is an alphanumeric code sent by SSA to the employer or registered user when access to certain programs is requested. This code must be entered on the Activate Access to BSO Service web page to enable the user to access the requested service.

² The address is obtained from the Employer's Federal Tax Return (Form 941) or Application for Employer Identification Number (SS-4)

³ The user identification number is a unique number assigned to users when they register for BSO services such as SSNVS.

- Upload files containing up to 250,000 employee names and SSNs and usually receive verification results the next Government business day. This bulk procedure allows employers to verify an entire payroll database or verify at one time the names and SSNs of a large number of newly hired workers.

SSA returns a verification code to the employer for each employee whose information does not match SSA's record. In addition to the verification code, SSA provides a death indicator if the employee's Numident record includes a date of death. Table A-1 describes the SSNVS verification codes.

Table A-1: SSNVS Verification Codes Provided to Companies

SSNVS Code	Description of Code
"Blank"	Name and SSN match SSA's records.
1	SSN not in file (never issued to anyone)
2	Name and date of birth match; gender code does not match
3	Name and gender code match; date of birth does not match
4	Name matches; date of birth and gender code do not match
5	Name does not match; date of birth and gender code not checked
6	SSN Not Verified; Other Reason
Y	Death indicator

Appendix B – SCOPE AND METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable Federal laws and Social Security Administration (SSA) policies and procedures.
- Reviewed prior audit reports from the Office of the Inspector General concerning the Social Security Number Verification Service (SSNVS).
- Obtained Calendar Year (CY) 2009 and 2010 Failed Master Earnings File (MEF) Check transaction data.
 - For CY 2009, the report contained 2.7 million records related to 4,149 employers.
 - For CY 2010, the report contained 23.4 million records related to 34,564 employers.
- Selected a random sample of 100 transactions (200 in total) from the 2009 and 2010 Failed MEF Check reports to determine whether the transactions posted properly to the reports.
- Obtained CY 2009 and 2010 Consent Based Social Security Number Verification (CBSV) transactions data.
- Compared transactions from the Failed MEF Check report with CBSV to identify non-SSNVS transactions.
- Obtained the weekly Same Name/Different Social Security Number (SSN) Potential Fraud Identification Report and Same SSN/Different Name Potential Fraud Identification Report generated in Fiscal Year 2010.
- For the names and SSNs on the potential fraud reports, we reviewed data obtained from the Numident, Master Earnings File, Annual Wage Reporting System, and Prisoner Update Processing System.

We determined that the SSNVS data used for this audit were sufficiently reliable to meet our objective. The entities audited were the Offices of Earnings, Enumeration and Administrative Systems under the Deputy Commissioner for Systems and Electronic Services under the Office of the Deputy Commissioner for Operations. Our work was conducted at the Philadelphia Audit Division, Philadelphia, Pennsylvania, from April 2012 through January 2013. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix C – AGENCY COMMENTS



SOCIAL SECURITY

MEMORANDUM

Date: April 2, 2013 **Refer To:** S1J-3

To: Patrick P. O’Carroll, Jr.
Inspector General

From: Katherine Thornton /s/
Deputy Chief of Staff

Subject: Office of the Inspector General Draft Report, “Access Controls for the Social Security Number Verification Service” (A-03-12-11204)--INFORMATION

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. You may direct staff inquiries to Gary S. Hatcher at (410) 965-0680.

Attachment

**COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT,
“ACCESS CONTROLS FOR THE SOCIAL SECURITY NUMBER VERIFICATION
SERVICE” (A-03-12-11204)**

Recommendation 1

Determine whether to modify the existing Failed MEF Check report to ensure it is a reliable tool to detect whether registered companies are improperly using SSNVS for non-employment purposes or develop a more useful fraud detection tool.

Response

We agree. We will continue to investigate if there are meaningful tools or improvements we can make to protect the use of the Social Security Number Verification System (SSNVS) for its intended purpose.

Recommendation 2

Conduct outreach with registered companies regarding using the appropriate EIN when submitting verifications to reduce the number of transactions posted to the Failed MEF Check report.

Response

We agree. When we correspond with the registered users, we will include information on the proper use of SSNVS. In addition, we plan to explore enhancements to both the online and file upload SSNVS input screens to improve the instructions for users, including inputting the appropriate employer identification number.

Recommendation 3

Develop consistent procedures for contacting employers who appear on the fraud detection reports to ensure the appropriate use of SSNVS.

Response

We agree. With the low volume of issues appearing on the fraud detection reports, we did not see the need for formal procedures; however, we will develop procedures as recommended.

Appendix D – MAJOR CONTRIBUTORS

Cylinda McCloud-Keal, Philadelphia Audit Director

Virginia Harada, Audit Manager

William Kearns, IT Specialist

Luis Ramirez, Audit Data Specialist

MISSION

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

CONNECT WITH US

The OIG Website (<http://oig.ssa.gov/>) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "[Beyond The Numbers](#)" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.



[Watch us on YouTube](#)



[Like us on Facebook](#)



[Follow us on Twitter](#)



[Subscribe to our RSS feeds or email updates](#)

OBTAIN COPIES OF AUDIT REPORTS

To obtain copies of our reports, visit our Website at <http://oig.ssa.gov/audits-and-investigations/audit-reports/all>. For notification of newly released reports, sign up for e-updates at <http://oig.ssa.gov/e-updates>.

REPORT FRAUD, WASTE, AND ABUSE

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website: <http://oig.ssa.gov/report-fraud-waste-or-abuse>

Mail: Social Security Fraud Hotline
P.O. Box 17785
Baltimore, Maryland 21235

FAX: 410-597-0118

Telephone: 1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time

TTY: 1-866-501-2101 for the deaf or hard of hearing