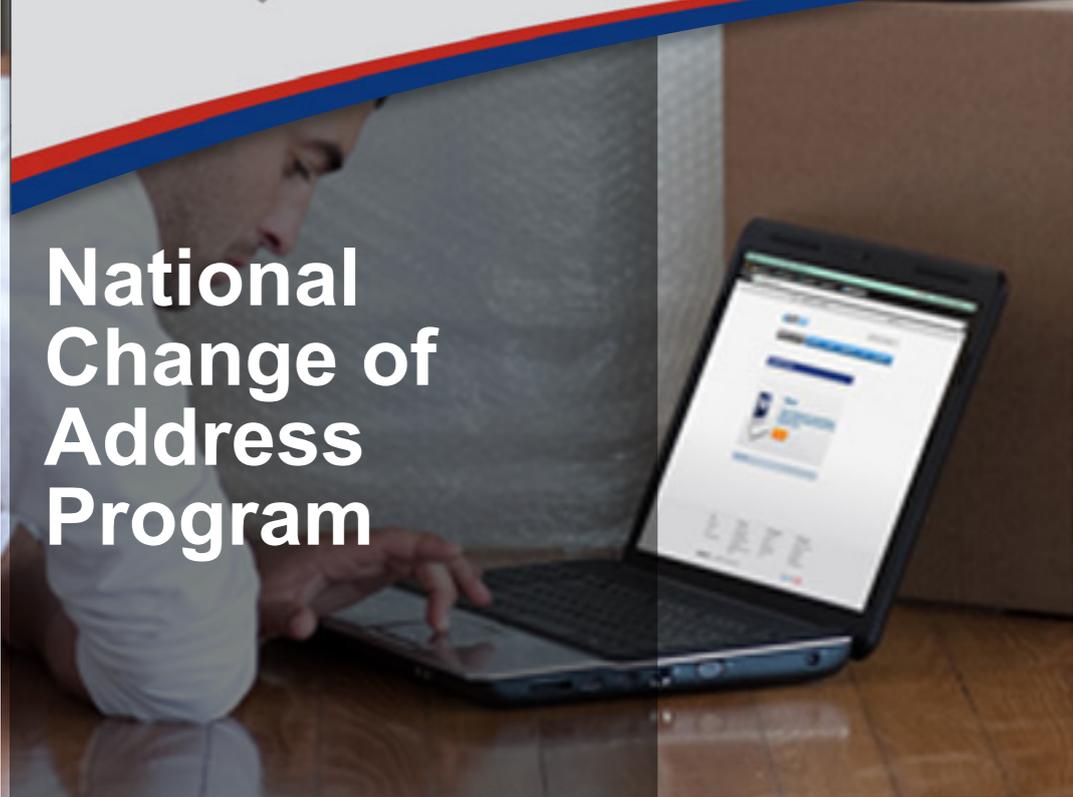




OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

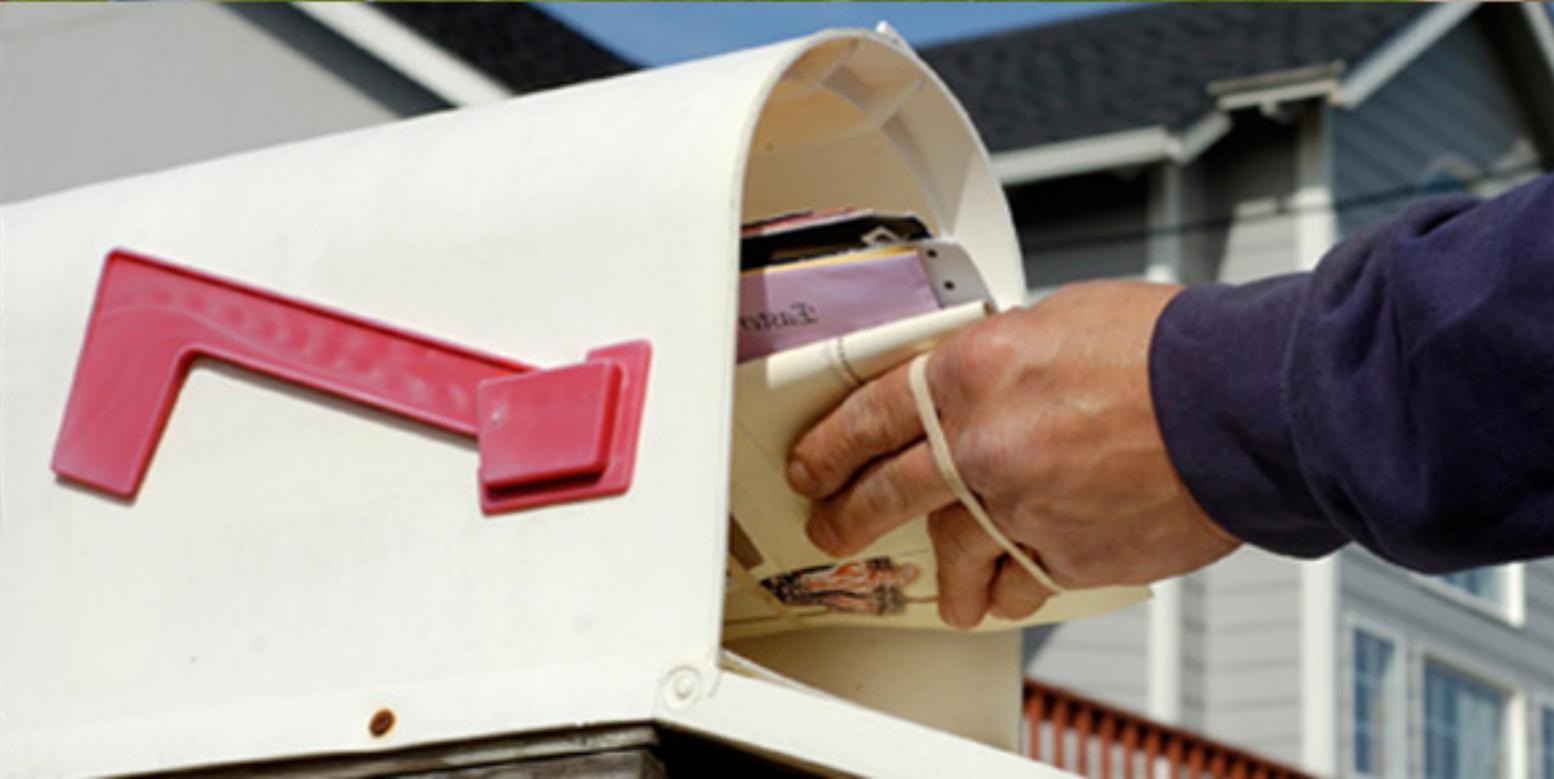
National Change of Address Program



Audit Report

Report Number
IT-AR-14-010

September 24, 2014





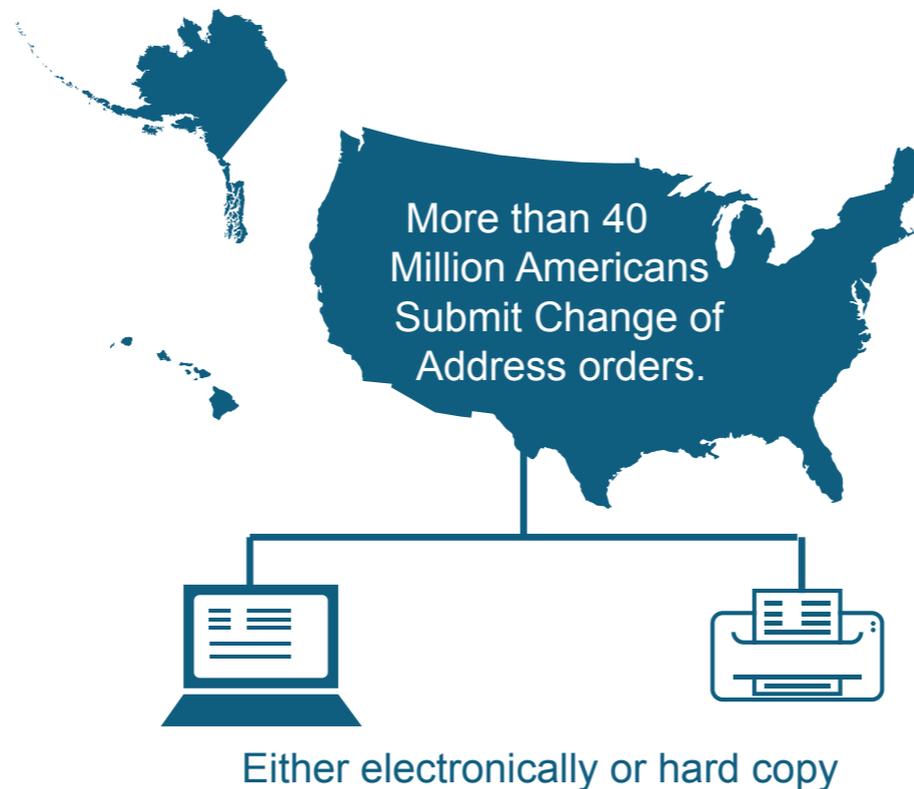
OFFICE OF INSPECTOR GENERAL UNITED STATES POSTAL SERVICE

Highlights

Security controls over change of address and NCOALink data do not protect customer information.

Background

More than 40 million Americans change their addresses annually and submit change of address (COA) orders to the U.S. Postal Service. Customers can submit orders electronically through the Internet or submit hard copy orders through the mail or at a Post Office retail counter. The Postal Service provides COA information for a fee through National Change



of Address Linkage (NCOALink) to licensees who facilitate relationships with business mailers. NCOALink is an application containing about 160 million COA records. The Postal Service requires licensees and their customers to complete a Processing Acknowledgment Form (acknowledgement form) to comply with the Privacy Act of 1974 and document the companies' intended use of the data.

Our objectives were to determine whether security controls over the COA manual process and NCOALink data adequately protect the confidentiality and integrity of customer data and identify potential solutions for improving the Postal Service's acknowledgement form process.

What The OIG Found

Security controls over the COA manual processes and NCOALink data are not sufficient to protect the confidentiality and integrity of customer information. We visited one of the 22 Computerized Forwarding System sites and found personnel did not adhere to controls related to processing and retaining hard copy COA orders.

We also determined the Postal Service is using outdated software to [REDACTED] data. In addition, NCOALink license agreements did not always have sufficient contract provisions to protect customer data, and management did not always monitor these agreements for licensee compliance.



OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

As a result, there is a risk that unauthorized users could access COA data and NCOALink data could be breached, which could lead to fines and a negative impact on the Postal Service brand. We estimated 13,554,542 NCOALink customer records with a potential value of \$228 million are at risk.

In addition, management does not have an enterprise solution in place or plan to automate the acknowledgement form process.

What The OIG Recommended

We recommended management centralize user account management in eAccess for the COA Forms Processing

System, and store hard copy COA orders in accordance with policy. We also recommended management re-initiate the National Change of Address certification and accreditation process, upgrade outdated security software, identify all cooperative database mailers and their activities, and implement a process to ensure current Postal Service requirements are in all license agreements to protect customer information.

Finally, we recommended management implement a plan of action for conducting random site security reviews of licensees and evaluate potential solutions and benefits of automating the acknowledgement form process.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 24, 2014

MEMORANDUM FOR: ROBERT CINTRON
VICE PRESIDENT, PRODUCT INFORMATION

JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY

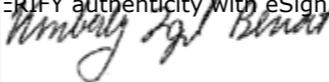
EDWARD F. PHELAN, JR.
VICE PRESIDENT, DELIVERY AND POST OFFICE
OPERATIONS

MICHAEL J. AMATO
VICE PRESIDENT, ENGINEERING SYSTEMS

MICHAEL J. ELSTON
ASSOCIATE GENERAL COUNSEL AND CHIEF ETHICS/
COMPLIANCE OFFICER, CHIEF ETHICS/COMPLIANCE
OFFICE

CHARLES L. MCGANN, JR.
MANAGER, CORPORATE INFORMATION SECURITY
OFFICE

DAVID G. BOWERS
POSTAL INSPECTOR IN CHARGE, SECURITY AND CRIME
PREVENTION

E-Signed by Kimberly Benoit
VERIFY authenticity with eSign Desktop


FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Information Technology and Data Analysis

SUBJECT: Audit Report – National Change of Address Program
(Report Number IT-AR-14-010)

This report presents the results of our audit of the National Change of Address Program (Project Number 14BG006IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Aron Alexander, director, Information Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Table of Contents

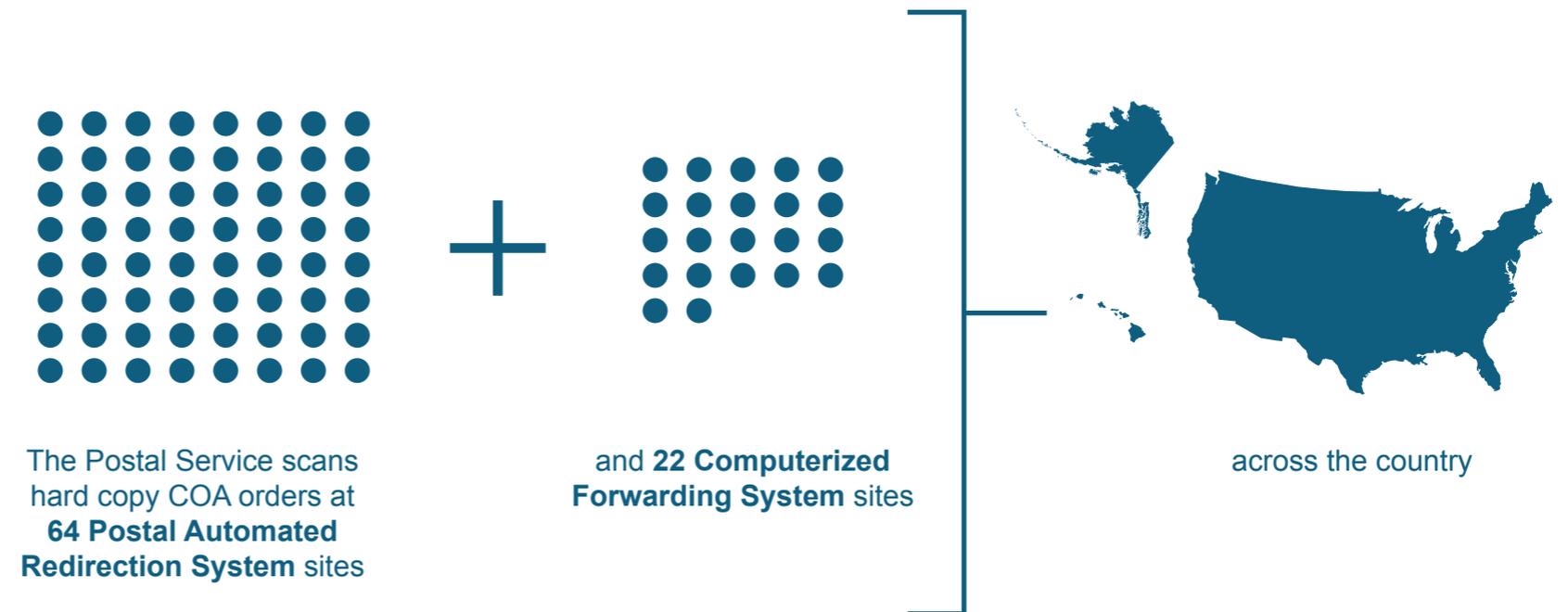
Cover	
Highlights.....	1
Background.....	1
What The OIG Recommended	2
Transmittal Letter.....	3
Findings	6
Introduction	6
Conclusion	8
Access Controls at the Computer Forwarding Site	8
Controls Over National Change of Address Linkage Customer Data	9
National Change of Address Linkage Data Protection	9
National Change of Address Linkage License Provisions	9
National Change of Address Linkage License Monitoring.....	10
Recommendations.....	12
Management’s Comments	13
Evaluation of Management’s Comments	14
Appendices.....	15
Appendix A: Additional Information	16
Background	16
Objectives, Scope, and Methodology.....	16
Prior Audit Coverage	17
Appendix B: Management’s Comments.....	18
Contact Information	30

Findings

Introduction

This report presents the results of our self-initiated audit of the National Change of Address (NCOA) Program (Project Number 14BG006IT000). Our objectives were to determine whether security controls over the change of address (COA) manual process and National Change of Address Linkage (NCOALink) data adequately protect the confidentiality and integrity of customer data and identify potential solutions for improving the U.S. Postal Service's Processing Acknowledgement Form (acknowledgement form)¹ process. See [Appendix A](#) for additional information about this audit.

When mail is misaddressed,² the Postal Service and business mailers incur added costs for sorting, transporting, delivering, and disposing of it. As a result, the Postal Service implemented address correction services in 1924 and the NCOA Program in 1986. The NCOA Program includes COA services that provide customers the option of forwarding mail to their new address by submitting COA orders electronically through the Postal Service's website or submitting hard copy orders³ through the mail or at a Postal Service retail counter.



- ¹ A written request to use COA information for mailing purposes in accordance with the license agreement and the Privacy Act of 1974 (Section 552a).
- ² Undeliverable as Addressed (UAA) mail the Postal Service cannot deliver as addressed and must forward to a different address for the addressee, return to the sender, or, in some cases, destroy.
- ³ Hard copy COA orders consist of the official Change of Address Order (Form 3575) obtained at a retail office and U. S. Postal Service Change of Address Order (Form 3575-WWW) from the official USPS® COA website.

The Postal Service scans hard copy COA orders at 64 Postal Automated Redirection Systems (PARS)⁴ and 22 Computerized Forwarding System (CFS)⁵ sites across the country. Additional processing of scanned COA images may occur at the Remote Encoding Center (REC)⁶ in Salt Lake City, UT. Hard copy COA orders totaled 25 million (or 65 percent) of the 39 million COA orders processed in fiscal year 2013. To confirm the validity of COA orders, the Postal Service sends confirmation and validation letters to the customer's old and new address and places a 5-day hold on mail interception to allow for delivery of the confirmation letter.



The Address Management group in Memphis, TN, stores COA data in the NCOA database.⁷ Address Management provides COA data to licensees through the NCOALink application⁸ to minimize misaddressed mail and related costs incurred by the Postal Service and business mailers. Licensees acquire a license to obtain COA data from the Postal Service.⁹ The licensees then provide NCOALink data to their customers, which include business mailers and other entities.¹⁰ Prior to obtaining NCOALink data and services, the licensees and their customers must complete an acknowledgement form to comply with Privacy Act requirements. Licensees are also required to collect annual updates of acknowledgement forms from their customers and provide the Postal Service with monthly performance reports.

-
- 4 An automated system that identifies and redirects UAA mail in a live mail processing environment at 258 select processing and distribution centers, 64 of which process COA Forms 3575.
 - 5 The 22 CFS sites are responsible for entering the customer's "old" and "new" address information into the CFS database to facilitate address correction notifications and further handling of mailpieces.
 - 6 A postal facility that processes COA unreadable image data to correct delivery address information.
 - 7 The NCOA application is a database of COA records that stores COA information for postal patrons and consists of 20 modules, including NCOALink.
 - 8 NCOALink is a premailing, address correction method consisting of a secure dataset of permanent COA records of about 160 million residential and business customers who have filed COA requests.
 - 9 During our audit, the Postal Service had 515 NCOALink license agreements and 16 additional NCOALink licenses were pending.
 - 10 These entities include broker-agents, who act as middle men between the business mailer and licensee; list administrators, who house, update, and manage the mailing list for the business mailer; list custodians, who are responsible for the address mailing list for a particular company; list brokers, who are third-party companies that compile and sell customer names and addresses; and cooperative database participants that consist of many companies that contribute information to a database in return for aggregate information on customers of other participants.

Controls over change of address orders were not implemented.

Conclusion

Security controls related to the COA manual submission¹¹ process and NCOALink data transmissions and license agreements need to improve. Of the 22 CFS sites, we visited one and found personnel did not adhere to controls related to processing and retaining hard copy COA orders. We also determined the Postal Service is using an outdated [REDACTED] within the application.¹² Further, NCOALink license agreements did not always have sufficient contract provisions to protect customer data and management did not always monitor existing agreements for licensee compliance.

There is a risk that COA data could be accessed by unauthorized users, which could lead to fines and a negative impact on the Postal Service brand. We estimated that 13,554,542 NCOALink customer records with a potential value of \$228 million are at risk.

Access Controls at the Computer Forwarding Site

Management did not implement existing controls over COA orders at the Jackson, TN, CFS site. Specifically, COA orders were not stored in a secured area, as required by policy.¹³ During our visit to the facility, we found numerous hard copy COA orders, some dating back to July 2013, stored in an unsecured open area accessible to all Jackson CFS site employees. See Figure 1 for a photograph of the area where employees stored the orders.

Figure 1. Storage of COA Orders



Source: U.S. Postal Service Office of Inspector General (OIG) photograph taken April 10, 2014.

This site opened in June 2013 and the new supervisor was not aware of the CFS storage process. Improper storage of sensitive COA orders increases the risk an unauthorized individual will access a customer's COA information.

¹¹ Hard copy COA submissions consist of Form 3575 obtained at a retail office and Form 3575-WWW printed from the Internet COA website.

¹² [REDACTED] Per the National Institutes of Standards and Technology, the outdated [REDACTED]

¹³ Handbook AS-805, *Information Security*, Section 3-5.3, Retention and Storage of Information; and Section 7-3.4 Sensitive-Enhanced, Sensitive, and Critical Media, May 2014.

The Postal Service can enhance controls over NCOALink data and licenses. We estimate 13.5 million customer records valued at \$228 million are at risk.

In addition, all four CFS operators at the Jackson CFS site were using the same user account and password to log into the COA Forms Processing System (CFPS).¹⁴ This occurred because the CFS operator responsible for providing user access was not aware of password policies.¹⁵ In addition, the CFPS system is not a part of the eAccess system¹⁶ and, as a result, management cannot establish accountability for individuals responsible for errors in data entry or misuse of the system.

Controls Over National Change of Address Linkage Customer Data

The Postal Service could enhance controls over NCOALink data related to data transmission, license provisions, and license monitoring to secure COA information. We estimated 13,554,542 NCOALink customer records with a potential value of \$228 million are at risk of unauthorized access.

National Change of Address Linkage Data Protection

The NCOA Program office uses an outdated [REDACTED] coupled with an in-house, patented [REDACTED]¹⁸ to [REDACTED]⁹ NCOALink data provided to its licensees. The outdated [REDACTED] does not comply with security policy²⁰ because management was unaware of the policy. In addition, the outdated [REDACTED] was not reviewed in the latest risk assessment process²¹ to determine vulnerabilities associated with the NCOA application. Management stated that changing the current [REDACTED] to conform to the policy would require a major upgrade to Postal Service systems and those of its licensees. Because the Postal Service uses this outdated [REDACTED] a person could crack the [REDACTED] to access or change sensitive NCOALink customer data.

[REDACTED] the National Institute of Standards and Technology required applications in federal agencies to move to an updated [REDACTED]. In addition, Microsoft announced that Windows will stop supporting the current [REDACTED] by [REDACTED]; therefore, if the Postal Service does not begin to convert the NCOALink application to a more secure [REDACTED] standard, it might not be able to transmit data to its licensees as their systems are upgraded.

National Change of Address Linkage License Provisions

NCOALink license agreements did not always contain sufficient contract provisions that require licensees and business mailers to secure customer data. We sampled 36 of 515 NCOALink license agreements and determined they all contained at least one of the following issues:

14 The CFPS automates the COA form process by scanning the cards and transmitting the information to the NCOA database.

15 Handbook AS-805, Section 9-4, Accountability, March 2014.

16 eAccess is an enterprise application used to manage authorization of access to information resources by centralizing the management of personnel identities and access rights over the entire lifecycle, from user account creation and registration to termination.

17 [REDACTED]

18 James D. Wilson, et al., *Method and System for Efficiently Retrieving Secured Data by Securely Pre-processing Provided Access Information*; U.S. Patent No. 7,549,053, June 16, 2009.

19 The process of hiding original data with random characters. The main reason for applying [REDACTED] to data is to protect personal identifiable or sensitive data. [REDACTED] are not encryption methods, but offer additional system security using a [REDACTED].

20 According to Handbook AS-805, Section 9-7.4, the Postal Service's [REDACTED]. In addition, Handbook AS-805-A, *Information Resource Certification and Accreditation Process*, Section 4-3.4.6, Assess Risk; and Section 4-3.4.7, Conduct Risk Assessment, October 2009, require an ongoing risk assessment for all information resources to identify security concerns such as threats, vulnerabilities, and control weaknesses.

21 The risk assessment is part of the certification and accreditation process.

22 [REDACTED]

- Thirty-four license agreements did not have adequate “Security Documentation”²³ to assure third-party adherence to privacy and security requirements.
- Three of the licensees in our sample are commingling Postal Service NCOALink data servers in third-party data centers shared with other companies, which violates policy.²⁴
- Licensees are not identifying all cooperative database business mailers²⁵ who receive NCOALink data as stipulated in their monthly performance report requirements.

These security issues occurred because there is no assigned contracting authority or process to ensure management incorporates the appropriate security, privacy, and acknowledgement form requirements into NCOALink license agreements. In addition, management does not require complete cooperative database mailers’ information on the licensees’ monthly performance reports. Further, cooperative database mailers for a licensee share one set of credentials²⁶ and, as a result, sensitive NCOALink customer data is at risk of unauthorized access in and outside the U.S., which could lead to data breaches, fines, and a negative impact on the Postal Service brand.

National Change of Address Linkage License Monitoring

Management is not monitoring licensee compliance with NCOALink license agreements. For example:

- Licensees are transmitting sensitive customer data in ████████ to business mailers using File Transfer Protocol (FTP),²⁷ which is insecure and violates policy.²⁸
- Management did not adhere to existing policy²⁹ when they decided to no longer require licensees to complete site security review worksheets as part of the licensing and certification process. Moreover, the Postal Inspection Service and the Corporate Information Security Office (CISO) have never performed site security reviews of licensees’ environments, as required by policy and the license agreements.
- Some licensees are using unsupported operating systems³⁰ to store Postal Service COA data; therefore, security updates are no longer available, leaving COA data at risk of data breaches.
- International mailers are participating in the NCOALink service program, which is a violation of the NCOALink agreement.³¹ A total of 2,674 international mailers have agreements with 19 NCOALink licensees located in the U.S. Of the 36 license agreements we reviewed, we also determined nine international mailers stored NCOALink data outside the U.S.

23 As part of the licensing and certification process, the Postal Service requires licensees to provide a self-certifying document to identify their internal, physical, and logical security controls.

24 Handbook AS-805, Section 10.4.8, Isolation of Postal Service Information.

25 Cooperative database mailers consist of many companies that contribute information to a database in return for aggregate information on customers of other participants. Some licensees have over 300,000 companies participating in their cooperative database.

26 A licensee can provide multiple cooperative database mailers one acknowledgement form identification (ID) for accessing NCOALink data.

27 A standard Internet protocol for transmitting files in ████████ between computers on the Internet.

28 Handbook AS-805, Section 9-7.1, Encryption.

29 Handbook AS-805, Section 4-1, Security Risk Management Policy.

30 Unsupported operating systems such as Windows NT, Windows 2000, and Windows XP.

31 According to the NCOALink license agreements the service is only available to entities within the U.S.

- Management stated they do not always ensure all third parties are updating acknowledgement forms. Specifically, some business mailers and other third-party participants only update their acknowledgement form information when their contact information changes. Also, the Postal Service does not ensure the acknowledgement form renewal process between licensees and business mailers is occurring and does not store updated acknowledgement form information.

These monitoring issues occurred because there is no assigned contracting authority or an automated acknowledgement form process to monitor and address compliance issues. The current process requires licensees and the Postal Service to maintain hard copies or scanned images of their acknowledgement forms (some licensees could have up to 300,000 acknowledgement forms to maintain); therefore, monitoring acknowledgement form compliance or conducting research on customers obtaining NCOALink data is labor intensive.

This puts sensitive NCOALink customer data at risk of unauthorized access, which could lead to fines and a negative impact on the Postal Service brand. Without an automated acknowledgement form solution, the Postal Service is at a greater risk of incurring fines for violating the Privacy Act of 1974.

Maintaining hard copy or scanned versions of acknowledgment forms is very costly in the digital age. There are various automated solutions to manage hard copy documents enterprise-wide. Specifically enterprise content management systems can be used by organizations to store and manage documents. A solution such as an enterprise content management system would allow the Postal Service to store hard copy forms electronically to provide improved access and monitoring capabilities. Benefits include:

- Compliance with the Privacy Act and better oversight of NCOALink contractual activities.
- Elimination of paper acknowledgement forms and electronic storage accessible by external and internal stakeholders.
- Elimination of single acknowledgement form ID for multiple business mailers.
- Support for proper governance of NCOALink data by ensuring completion of acknowledgement form process and compliance with policies and regulations.

Recommendations

We recommend the vice president, Engineering, coordinate with the vice president, Information Technology, to:

1. Add the Change of Address Forms Processing System to the eAccess application or use an alternative method for user account management.

We recommend the vice president, Delivery and Post Office Operations:

2. Communicate user account management policies to all Computerized Forwarding System site employees.
3. Direct Computerized Forwarding System site employees to securely store hard copy change of address orders in accordance with policy.

We recommend the vice president, Product Information, direct the manager, Address Management, to:

4. Re-initiate the certification and accreditation process for the National Change of Address application to identify and document security risks as required.
5. Upgrade the outdated [REDACTED] used in the National Change of Address Linkage application to a more secure and compliant [REDACTED] before support for the current [REDACTED] ends.
6. Update license agreements to require that licensees include the names of cooperative database business mailers and their data activities in their monthly performance reports.

We recommend the vice president, Product Information, direct the manager, Address Management, to coordinate with the associate general counsel and chief ethics/compliance officer, and the manager, Corporate Information Security, to:

7. Implement a process to ensure current legal, security, privacy, and compliance requirements are included in all National Change of Address Linkage license agreements.

We recommend the vice president, Product Information, direct the manager, Address Management, to coordinate with the manager, Corporate Information Security, and the postal inspector in charge, Security and Crime Prevention, to:

8. Implement a process and plan of action for establishing and conducting random site security reviews of National Change of Address Linkage licensees to verify adherence to license agreement requirements, as required.

We recommend the vice president, Product Information, direct the manager, Address Management, to consult with the vice president, Information Technology, to:

9. Evaluate solutions to automate the Processing Acknowledgment Form process.

Management's Comments

Management agreed with recommendations 4, 5, 8, and 9. Management disagreed with the findings and recommendations 1, 2, 3, 6, and 7 and with the other impact.

Regarding recommendation 1, management disagreed and stated the basis of the recommendation is flawed because the audit team only visited one CFS site. Management stated the CFS operators did not adhere to the password policy and established procedures cited in the training handbook. They also stated a conversion of the CFPS to eAccess would likely lead to the same scenario and additional expenses. Further, management stated properly enforcing the current CFPS password security measures would correct this issue.

Regarding recommendation 2, management disagreed and stated the observed shortcomings in one CFS site are not indicative of shortcomings in all CFS sites. However, management stated they will communicate with all CFS sites to remind them of the Postal Service policy regarding user account management.

Regarding recommendation 3, management disagreed and stated current policy requires CFS sites to destroy COA forms after 30 days and does not require secure storage before the 30 day period prior to destruction. Therefore, management stated they will continue to communicate and adhere to current policy regarding the destruction of COA's after 30 days.

Regarding recommendation 4, management agreed to resubmit the NCOALink application for a new certification and accreditation review with a target implementation date of April 1, 2015.

Regarding recommendation 5, management agreed and plans to commence a review of alternatives available to eliminate the use of the [REDACTED]. Management will complete the software changes to upgrade the [REDACTED] by [REDACTED].

Regarding recommendation 6, management disagreed with requiring licensees to include the names of cooperative database business mailers and their activities in monthly performance reports. Management stated the current NCOALink Full Service License Agreement requires licensees to comply with the separate "License Performance Requirements" and they will determine whether clarifying language regarding cooperative databases is needed and the appropriate document in which to place the language. Management plans to complete their determination by April 1, 2015.

Regarding recommendation 7, management disagreed with implementing a process to ensure current legal, security, privacy, and compliance requirements are included in all NCOALink agreements. Management stated Section 22.2 of the NCOALink Full Service Provider License Agreement and the "Service Provider Certification Procedures" requires the licensees to provide the Postal Service with current information. Management also stated they will develop supplemental internal administrative processes to remind licensees to update information they provide to the Postal Service. Management plans to develop the internal processes by October 1, 2015.

Regarding recommendation 8, management agreed to implement a process and plan of action for establishing and conducting random site security reviews for NCOALink licensees by April 1, 2015.

Regarding recommendation 9, management agreed to evaluate potential solutions for automating the collection and management of acknowledgement forms by April 1, 2015.

See [Appendix B](#) for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1,2, 4, 5, 8, and 9 and corrective actions should resolve the issues identified in the report. The OIG considers management's comments to recommendations 3, 6, and 7 as nonresponsive.

Although management disagreed with recommendations 1 and 2, their statement does not refute the issue regarding sharing logon IDs and passwords among the Jackson CFS operators. We agree with management that the sharing of logon IDs and passwords does not adhere to policy, which we cited in the report and was the basis of our finding. Also, we reviewed Handbook 4050-01, *CFPS Scanner Site Operations Training Course*, and did not find any information on the proper use of logon IDs and passwords for establishing user accountability. However, we did reference Handbook AS-805, Section 9-4 in the report as criteria for proper account and password administration. In subsequent communications, Jackson CFS management stated this issue has been corrected and the four CFS employees are now using unique logon IDs and passwords. Although establishing a method for user account management would help prevent people from sharing accounts and passwords in the future, actions planned to remind CFS employees of user account management policy, coupled with actions already taken, should resolve the issue identified at the Jackson, TN CFS site.

Management's response to recommendation 3 does not correct the issue identified in this report. We agree policy exists that requires COA orders to be shredded after 30 days. However, storing COA orders in unsecured locations for up to a year does not comply with Handbook AS-805, section 3-5.3 and section 7-3.4 as noted in this report. Improper storage of sensitive COA orders increases the risk of an unauthorized individual gaining access to customer's COA information. Therefore, we believe management should enforce the current security policies regarding the proper storage of COAs.

Management's responses to recommendations 6 and 7 do not correct the issues related to license provisions and monitoring noted in this report. Although the Licensee Performance Requirements provides technical requirements for the licensees, management does not enforce licensees to divulge the identity of cooperative database mailers accessing NCOALink data. Also, including the proper language in the NCOALink licenses to protect customer data lessens the risk of unauthorized access to Postal Service data in and outside the U.S.

Although management disagreed with the non-monetary impact noted in our report, we believe our calculations were conservative and reasonable. Our calculations were based on insufficient contract provisions that require licensees and business mailers to secure customer data, and the absence of monitoring activities to ensure compliance with the NCOALink license agreements. As a result, sensitive-enhanced customer data provided to 466 third-party licensees are at risk of unauthorized access.

The OIG considers recommendations 4, 5, 6, 7, and 8 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

*Click on the appendix title
to the right to navigate to
the section content.*

Appendix A: Additional Information	16
Background	16
Objectives, Scope, and Methodology	16
Prior Audit Coverage	17
Appendix B: Management’s Comments.....	18

Appendix A: Additional Information

Background

The NCOA application is composed of several modules and components, one of which is NCOALink. NCOALink is a premailing address correction method and consists of a secure dataset of about 160 million permanent COA records of residential and business customers who have filed COA requests.

Business mailers who want bulk mail rates must use NCOALink to minimize the processing of UAA mailpieces. This reduction in UAA mailpieces has contributed to lower costs and processing time for business mailers and the Postal Service. Business mailers wanting access to NCOALink data must get it through the licensees who have agreements with the Postal Service. The Postal Service has 515 agreements with licensees that fall under six license categories: Full-Service, Limited Service, Interface Developers, Interface Distributor, End User Mailer, and Mail Processing Equipment (manufacturing-integrator and data user). These licensees charge business mailers a fee for updating their mailing lists with customer address records from the NCOALink application. The Postal Service strictly controls the matching logic of NCOALink data.

Licensees are required to collect annual updates to acknowledgement forms from each of their customers and must secure these agreements before business mailers can perform NCOALink processing. The current acknowledgement form process relies strictly on maintenance of hard copy acknowledgement forms or acknowledgement form data stored by the licensees. Licensees are required to provide the Postal Service with monthly performance reports.

Objectives, Scope, and Methodology

Our objectives were to determine whether security controls over the NCOA manual process and NCOALink data adequately protect the confidentiality and integrity of customer data and to identify potential solutions for improving the Postal Service acknowledgement form process. To accomplish our objectives, we interviewed managers and key officials from Address Management, CISO, Consumer and Industry Affairs, Engineering Systems, Information Technology, Postal Inspection Service, Law Department, Mail Entry and Payment Technology, Post Office Operations, Secure Digital Solutions, and Supply Management.

We obtained and reviewed documentation and relevant information regarding security and privacy controls for the manual COA and NCOALink process. This includes processing COA orders and data through the CFS, PARS, and REC sites and relevant documentation related to NCOALink license agreements, Postal Service policies, and requirements. We reviewed potential solutions (such as cloud, enterprise content management, and digital vault) for automating the acknowledgement form process. Lastly, we developed an understanding of the COA customer notification and fraud process and reviewed COA issues reported to Address Management, the Enterprise Customer Center via usps.com, and the Postal Inspection Service.

To calculate other impact, we reviewed the Ponemon Institute's 2014 *Cost of a Data Breach Study: United States* to determine the Postal Service's cost per compromised record, the total risk for the NCOALink agreements, and the probable threat of a data breach.

We conducted this performance audit from January 2 through September 2014, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management on August 5, 2014, and included their comments where appropriate.

We did not assess the reliability of any computer-generated data for the purposes of this report.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact (in millions)
<i>Delegations of Contracting Authority Outside of Supply Management</i>	SM-AR-14-007	8/05/2014	None
<p>Report Results: Postal Service officials were not aware that Address Management personnel executed agreements with mail service providers without a required delegation. Specifically, Address Management officials did not have delegation granting authority for personnel to sign agreements with service providers who provide address quality data correction service to mailers.</p>			
<i>Cloud Computing Contract Clauses</i>	SM-MA-14-005	4/30/2014	\$12,429,228
<p>Report Results: The 13 cloud computing contracts did not address information accessibility and data security for network access and server locations because the Information Security handbook in effect at the time of the contract award did not include these requirements. In addition, the Postal Service exempted a supplier from following the handbook for one contract that did not contain sensitive data. Although the data may not be sensitive, the handbook provides additional requirements such as insurance against losses resulting from data breaches and procedures for timely notification of these breaches. Management generally agreed with the findings, recommendations, and monetary impact.</p>			
<i>Security of File Transfer Protocol Transmissions</i>	IT-AR-12-009	9/12/2012	None
<p>Report Results: Controls surrounding FTP activities are not adequate to ensure protection of the Postal Service's sensitive data. Specifically, business areas throughout the Postal Service are transmitting sensitive data in [REDACTED]. Further, unnecessary FTP services are running on servers and mainframes on the Postal Service's network. We made seven recommendations management agreed with six, and disagreed with one.</p>			
<i>Patch Management Processes</i>	IT-AR-12-002	1/9/2012	None
<p>Report Results: The Postal Service has not provided consistent oversight and monitoring of the patch management process to ensure uniform application across the enterprise. Specifically, we identified inconsistencies and non-compliant issues with the patch management processes and unsupported operating systems and databases. We made 10 recommendations and management agreed with all but one.</p>			
<i>Data Breach Incident Reporting</i>	IT-AR-11-006	8/11/2011	None
<p>Report Results: Management has adequate policies and operations in place to appropriately report and handle incidents and notify affected individuals of data breach incidents. However, management is not maintaining a complete, reliable record of data breach incidents in the Computer Incident Response Team database. In addition, the Postal Service did not update Chief Privacy Office procedures to reflect current processes for handling data breach incidents and include suggested key practices outlined in federal guidelines. We made two recommendations and management agreed with one and partially agreed with the other.</p>			

Appendix B: Management's Comments



September 10, 2014

LORI LAU DILLARD
ACTING DIRECTOR, AUDIT OPERATIONS

SUBJECT: National Change of Address Program (Report Number IT-AR-14-DRAFT)

We have reviewed the subject audit report on the National Change of Address Program and provide the requested written response below.

Recommendation 1

We recommend the Vice President, Engineering Systems, coordinate with the Vice President, Information Technology, to:

1. Add the Change of Address Forms Processing System to the eAccess application or use an alternative method for user account management.

Management Response

Engineering Systems does not agree with this recommendation. By only going to one site that was not following proper procedures, the basis of the recommendation is flawed. The survey revealed all four Computerized Forwarding System (CFS) operators at the Jackson CFS site were using the same user account and password to log into the Change of Address (COA) Forms Processing System (CFPS). This occurred because the CFS operators responsible for providing user access were not adhering to the password policy. If the Auditors had researched and reviewed the CFPS Scanner Site Operations Training Course Handbook #40501-01, they would have realized the actions at this site were in violation of the set procedures.

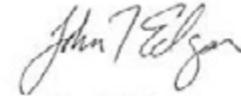
Converting CFPS to use eAccess would not necessarily fix the problem and would likely lead to the same scenario that is occurring with the current password security policy. Properly enforcing the current CFPS password security measures corrects the issue and avoids incurring the additional expense of developing and testing changes to multiple software applications.

The subject report and this response contain information related to disaster recovery that, if released, could be exploited and cause substantial harm to the U.S. Postal Service. The Manager, Corporate Information Security will determine what portions of the report should be considered as classified, restricted, and exempt from disclosure under the Freedom of Information Act.

If you have any questions or comments regarding this response please contact John Keegan, Manager Engineering Software Management at (703) 280-7230.



Michael J. Amato
Vice President, Engineering Systems



John T. Edgar
Vice President, Information Technology

cc: Todd Schimmel
Scott Bombaugh
John Keegan
Ed Phelan
Robert Cintron

EDWARD F. PHELAN
VICE PRESIDENT, DELIVERY AND POST OFFICE OPERATIONS



September 12, 2014

LORI DILLARD
ACTING DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to the Draft Audit Report – National Change of Address
Program (Report Number IT-AR-14-DRAFT)

Thank you for providing the U.S. Postal Service (USPS) with the opportunity to review and comment on the draft report titled National Change of Address Program

The U.S. Postal Service has reviewed the report and disagrees with the findings and provides the following responses to the recommendations.

Recommendation

We recommend the vice president, Delivery and Post Office Operations:

2. Communicate user account management policies to all Computerized Forwarding System site employees.

Management Response:

USPS does not agree that the observed shortcomings in one Computerized Forwarding System Sites are indicative of systemic shortcomings across all CFS sites. With that said, the USPS will initiate communications to CFS sites reminding them of USPS policy regarding CFPS account management.

Recommendation

We recommend the vice president, Delivery and Post Office Operations:

3. Direct Computerized Forwarding System site employees to securely store hard copy

Management Response:

Disagree. Current policy requires that CFS sites destroy (shred) Change of Address (COAs) after 30 days. The policy does not require secure storage of COAs for the 30 day period prior to destruction. USPS will continue to communicate and adhere to current policy regarding the destruction of COAs after 30 days.

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1600
202-268-6500
Fax 202-268-3331
WWW.USPS.COM

This report and management's response does not contain information that may be exempt from disclosure under the Freedom of Information Act.

A handwritten signature in black ink, appearing to read 'E. Phelan, Jr.', written in a cursive style.

Edward F. Phelan, Jr.

cc: Corporate Audit and Response Management
Mr. Amato
Mr. Cintron
Mr. Edgar
Ms. Sigmon
Ellisa Simmons



September 16, 2014

LORI LAU DILLARD
(A) DIRECTOR, AUDIT OPERATIONS

SUBJECT: National Change-of-Address Program
(Report Number IT-AR-14-DRAFT)

Management submits the following with regard to the findings presented in the draft report. Specifically;

NCOA^{Link} Data Protection

Management acknowledges the report's finding that the NCOA^{Link}® product uses the [REDACTED] technology which is non-compliant with current security policy standards. The use of [REDACTED] technology was appropriate when the NCOA^{Link} product was initially created. Management disagrees with the report's conclusion that the use of the [REDACTED] technology puts the NCOA^{Link} data at risk of breach that would allow a person to access or change sensitive NCOA^{Link} customer data. There is no example or demonstration made in the report of any correlation between the use of the [REDACTED] technology and how any unauthorized access or alteration of NCOA^{Link} data could potentially occur. Management contends that any intentional efforts to maliciously exploit NCOA^{Link} data, with the likelihood of a successful malicious exploit considered to be essentially nil, would be unrelated to the use of [REDACTED] technology. Management will undertake efforts to update the [REDACTED] used within the NCOA^{Link} product to undeniably remove any ongoing confusion or concerns related to the use of [REDACTED] technology.

NCOA^{Link} License Provisions

Management disagrees with the finding that the NCOA^{Link} license agreements lack sufficient contract provisions to protect the security of the NCOA^{Link} data. Management contends that the existing NCOA^{Link} License Agreement and the corresponding NCOA^{Link} Licensee Performance Requirements documents have appropriate controls and safeguards to protect the NCOA^{Link} data. Management acknowledges that improvements in oversight by the NCOA^{Link} program office are warranted to ensure that all existing documentation and other license requirements are adhered to by all NCOA^{Link} licensees.

NCOA^{Link} License Monitoring

Management disagrees with the finding that management is not monitoring compliance with the NCOA^{Link} license agreements. Management has not eliminated the requirement for licensee applicants to submit site security review documents as part of the licensing and certification process. Management does not dictate which operating systems a licensee may use and the use of outdated operating systems does not place the NCOA^{Link} data at any greater risk than the

use of current operating systems. Management suggests that the finding within the report is based on a misunderstanding of what is considered to be NCOA^{Link} data and what is considered to be the mailer's proprietary data. International mailers wishing to update a mailing list prior to mailing with the United States may not store the NCOA^{Link} product data outside of the United States but they may store the new address for their customer that was updated through their use of the NCOA^{Link} product. This is consistent with all other address correction updates provided to mailers through any of the Postal Service current programs. Management contends that once the address update is provided to the mailer the Postal Service has no further involvement in how the mailer uses or administrates their customer data as long as said use is not in violation of the restriction on the compilation of new mover lists. Management acknowledges that improvements in oversight by the NCOA^{Link} program office regarding the proper completion and timely update of Processing Acknowledgement Forms by licensees are appropriate to ensure that all existing documentation requirements are adhered to.

Response to Recommendations

For the reasons set forth below, management agrees in principle with some but not all of recommendations 4 through 9 contained in the audit report. Management's agreement with some of the recommendations acknowledges the benefit of performing ongoing reviews of the policies and procedures involved in the administration of change-of-address data. Management observes that the audit recommendations primarily serve to strengthen the already existing security of the NCOA^{Link} product and thus increases the overall confidence in the Postal Service's administration of this program.

Management disagrees with the monetary impact reflected in the audit report. The audit report's conclusion that each of the 466 NCOA^{Link} licensees would have a similar "average number of records breached as reported by the Ponemon Institute (29,087)" cannot be substantiated as valid. The estimated monetary impact is dependent upon the assumption that a potential breach of a customer record contained in the NCOA^{Link} product would be equivalent to the average of financial impacts reported by other industries. The data contained in NCOA^{Link} product contains only an address without any associated customer's name and it does not have any financial information that could be exploited as a result of an unauthorized access. Management contends it is inappropriate to apply an industry average cost to an unsubstantiated average of potentially breached records given that there is nothing in the NCOA^{Link} data to identify a specific individual that would facilitate the ability to exploit that individual's financial information. Without a specific example of how a potential breach of NCOA^{Link} data could be financially exploited Management cannot agree as to the validity of the monetary impact.

Recommendation 4:

Re-initiate the certification and accreditation process for National Change-of-Address application to identify and document security risks as required.

Management Response/Action Plan:

Management agrees with the recommendation.

Address Management will resubmit the NCOA^{Link} application for a new certification and accreditation review.

Target Implementation Date:

April 1, 2015

Responsible Official:

Manager Address Management

Recommendation 5:

Upgrade the outdated [REDACTED] used in the NCOA^{Link} application to a more secure and compliant [REDACTED] before support for the current [REDACTED] ends.

Management Response/Action Plan:

Management agrees with the recommendation.

Address Management will commence a review of the alternatives available to eliminate the use of the [REDACTED]. Address Management will complete the software changes needed to upgrade the [REDACTED] by the [REDACTED]. The Postal Service has given commitments to the mailing industry stakeholders that implementation of major changes in software and data products will only be done on a scheduled basis to allow the mailing industry sufficient time to complete their business planning, development, testing, and implementation of these changes. It is not possible to provide the mailing industry with the expected lead time needed for their implementation of major software changes and complete the conversion prior to [REDACTED]. Address Management will evaluate the potential of supplying a separate version of the NCOA^{Link} product using an upgraded [REDACTED] for those who can accommodate the changes prior to [REDACTED]. Based on current scheduling timelines the required completion of the conversion by all NCOA^{Link} product licensees will be August 1, 2017.

Target Implementation Date:

[REDACTED]

Responsible Official:

Manager Address Management

Recommendation 6:

Update license agreements to require the licensees to include the names of cooperative database business mailers and their data activities in their monthly performance reports.

Management Response/Action Plan:

Management disagrees with the recommendation.

The current NCOA^{Link} Full Service License Agreement requires Licensees to comply with the separate "Licensee Performance Requirements" (LPR) that the Postal Service publishes on its RIBBS web-site. For example, see Paragraphs 1.8, and 4.7 of the License Agreement.

The LPR spells out important technical requirements that Licensees must meet, including the Monthly Reporting requirements, such as Paragraph 9.5 (cooperative databases) and 9.6 (monthly reports). Management will determine whether clarifying language about cooperative databases is needed, and the appropriate document in which the Postal Service should place that language.

Target Implementation Date:

April 1, 2015

Responsible Official:

Manager Address Management

Recommendation 7:

Implement a process to ensure current legal, security, privacy, and compliance requirements are included in all NCOA^{Link} license agreements.

Management Response/Action Plan:

Management disagrees with the recommendation.

Section 22.2 of the NCOA^{Link} Full Service Provider License Agreement published on the ribbs.usps.gov website already requires Licensees to provide the Postal Service with current information:

22.2. Any change to the personnel, location and/or software systems for activities involving or in relation to the NCOA^{Link} Product, Service Materials, or to the information contained in the application materials submitted by Licensee to USPS must be reported to the USPS immediately. USPS may consider Licensee's failure to report such changes to USPS as a default under this agreement.

In addition, on Page 4 of the "Service Provider Certification Procedures" published on the rubbs.usps.gov web-site the Postal Service states at No. 6:

"Applicants shall submit written notice to USPS of any material change to the information submitted as part of the application and supporting documents within thirty (30) days of the occurrence of the change."

Address Management will develop supplemental internal administrative processes to remind Licensees to update the information they provided to the Postal Service.

As indicated by the signature of Michael J. Elston below, Ethics and Compliance agrees to provide legal support with regard to this management response/action plan.

Target Implementation Date:
October 1, 2015

Responsible Official:
Manager Address Management

Recommendation 8:
Implement a process and plan of action for establishing and conducting random site security reviews of NCOA^{Link} licensees to verify adherence to license agreement requirements, as required.

Management Response/Action Plan:
Management agrees with the recommendation.

The Address Management, Corporate Information Security, and the Inspection Service offices will collaborate to develop a process and plan of action for conducting random site security reviews of NCOA^{Link} licensees.

Target Implementation Date:
April 1, 2015

Responsible Official:
Manager Address Management

Recommendation 9:
Evaluate solutions to automate the Processing Acknowledgement Form process.

Management Response/Action Plan:
Management agrees with the recommendation.

The Address Management office will work with the Information Technology office to evaluate potential solutions for automating the collection and management of Processing Acknowledgement Forms.

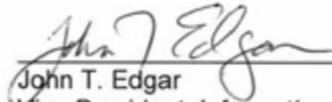
Target Implementation Date:
April 1, 2015

Responsible Official:
Manager Address Management

This report and management's response do not contain information that may be exempt from disclosure under the FOIA.



Robert Cintron
Vice President, Product Information



John T. Edgar
Vice President, Information Technology



Matthew Kennedy, CHIEF PRIVACY OFFICER, FOR
Michael J. Elston
Associate General Counsel and
Chief Ethics and Compliance Officer

Charles L. McGann
Manager, Corporate Information Security



David G. Bowers
Postal Inspector in Charge
Security and Crime Prevention

cc: Manager, Corporate Audit Response Management
Manager, Address Management

This report and management's response do not contain information that may be exempt from disclosure under the FOIA.

Robert Cintron
Vice President, Product Information

John T. Edgar
Vice President, Information Technology

Matthew Kennedy, CHIEF PRIVACY OFFICER, FOR
Michael J. Elston
Associate General Counsel and
Chief Ethics and Compliance Officer

Chuck McLean 2014.09.16 17:33:52
-04'00'

Charles L. McGann
Manager, Corporate Information Security

David G. Bowers
David G. Bowers
Postal Inspector in Charge
Security and Crime Prevention

cc: Manager, Corporate Audit Response Management
Manager, Address Management



OFFICE OF
**INSPECTOR
GENERAL**
UNITED STATES POSTAL SERVICE

Contact us via our [Hotline](#) and [FOIA](#) forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100