



Office of Inspector General | United States Postal Service

Audit Report

Change of Address Identity Verification Internal Controls

Report Number MS-AR-18-005 | August 24, 2018



Table of Contents

Cover	
Highlights.....	1
Objective	1
What the OIG Found.....	1
What the OIG Recommended	2
Transmittal Letter	3
Results.....	4
Introduction/Objective	4
Background.....	4
Finding #1: Lack of Identity Verification for Hardcopy COA Requests	7
Recommendation #1	7
Finding #2: Lack of [REDACTED].....	7
Recommendation #2.....	8
Management’s Comments.....	8
Evaluation of Management’s Comments	8
Appendices	9
Appendix A: Additional Information.....	10
Scope and Methodology.....	10
Prior Audit Coverage	11
Appendix B: Recommendation Status from Prior OIG Report	12
Appendix C: Management’s Comments.....	13
Contact Information	16

Highlights

Objective

Our objective was to evaluate the U.S. Postal Service's identity verification internal controls for its Change of Address (COA) service.

The Postal Service offers COA service whereby residential and business customers can apply to have their mail forwarded to a new address. This service helps customers manage potential adjustments to their mail delivery.

The Postal Service processed 36.8 million COA requests in fiscal year (FY) 2017 — 20.6 million hardcopy requests and 16.2 million online requests. Nearly 96 percent of the total COA requests during that time were from residential customers (4 percent were from businesses).

The Postal Service has a variety of controls in place to help prevent identity theft using the COA service and to protect the mail and privacy of its customers. These controls include electronically validating online COA requests using credit card addresses. The Postal Service also sends hardcopy letters to both the old and new addresses as a means to confirm and validate every COA request.

We initiated this audit based on concerns expressed by Congress, news outlets, and customer complaints regarding the internal controls and security related to the COA service and the potential risk this service could be used for fraudulent activities. The congressional inquiry specifically asked us to identify additional safeguards the Postal Service implemented subsequent to our 2008 report titled *Identity Theft Potential in the Change of Address Process*. All recommendations related to identity verification controls from that report have been implemented. Furthermore, the identity verification-related controls mentioned in that report — such as those related to verifying that hard copy requests have valid customer signatures and to sending verification letters — remain in place today. Since that time, the Postal Service has implemented additional enhancements to its COA-related identity verification controls, including the development of a watch list for suspect addresses, domain blocks, and flags for requests made from foreign internet provider addresses.

What the OIG Found

The Postal Service has opportunities to improve its COA service identity verification controls. First, the Postal Service lacks a control requiring customers to present a government-issued form of identification for review when submitting a hardcopy COA request at a retail facility or to their letter carrier. Leading practices, including those from foreign posts in developed countries, include having employees perform identity verifications when conducting these types of in-person transactions.

“The Postal Service has opportunities to improve its COA service identity verification controls.”

Second, the current online identity verification processes [REDACTED]

[REDACTED] Such a test could help verify the customer's identity by demonstrating their control over the linked account. The Postal Service [REDACTED], which uses pre-determined questions and answers such as matching the credit card holder's billing address with that of the address in the online COA request. Leading practices advocate having a verification process that includes [REDACTED]

The Postal Service recognizes potential vulnerabilities in these areas, and is evaluating control enhancements. Implementing such enhancements would help reduce the risk of COA-related identity theft. Since January 2016, the U.S. Postal Inspection Service received nearly 25,000 COA complaints, including 8,900 in 2016, 11,000 in 2017, and 5,000 for the first three months of 2018.

What the OIG Recommended

We recommend management:

- Develop and implement a national policy requiring customers to present a government-issued form of identification for review when submitting a hardcopy COA request.
- Develop and incorporate [REDACTED] into its online COA identity verification processes.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 24, 2018

MEMORANDUM FOR: GREGORY S. CRABB
VICE PRESIDENT, CHIEF INFORMATION SECURITY
OFFICER

ISAAC S. CRONKHITE
VICE PRESIDENT, ENTERPRISE ANALYTICS

KEVIN L. MCADAMS
VICE PRESIDENT, DELIVERY OPERATIONS

KELLY M. SIGMON
VICE PRESIDENT, RETAIL & CUSTOMER SERVICE
OPERATIONS

A digital signature of Janet M. Sorensen, showing her name in a cursive font over a white background with a small yellow icon in the top right corner.

Janet Sorensen

FROM: Janet M. Sorensen
Deputy Assistant Inspector General
for Retail, Delivery and Marketing

SUBJECT: Audit Report – Change of Address Identity Verification Internal
Controls (Report Number MS-AR-18-005)

This report presents the results of our audit of the Postal Service's identity verification internal controls for its Change of Address service (Project Number 18RG007MS000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Joseph Wolski, Director, Sales, Marketing and International, or me at 703-248-2100.

Attachment

cc: Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of U.S. Postal Service's Change of Address (COA) Identity Verification Internal Controls (Project Number 18RG007MS000). Our objective was to evaluate the Postal Service's identity verification internal controls for its COA service. See [Appendix A](#) for additional information about this audit.

An [OIG Blog](#) titled *The Changing Change of Address System* contained 477 responding posts as of February 15, 2018. Respondents were concerned about identity theft and did not understand why it was so easy for anyone to change their address.

Source: [OIG](#).



We initiated this audit based on concerns expressed by Congress, customer complaints, and news outlets regarding the internal controls and security related to the COA service and the potential risk that this service could be used for fraudulent activities. The congressional inquiry specifically asked us to identify additional safeguards the Postal Service implemented subsequent to our 2008 report titled *Identity Theft Potential in the Change of Address Process*.¹ That report contained six recommendations, five of which were related to identity verification related internal controls

(see [Appendix B](#)). All of those recommendations have subsequently been addressed, and the controls mentioned in the report remain in place today.

Background

The Postal Service offers COA service whereby residential and businesses customers can apply to have their mail forwarded to a new address. This service helps customers manage potential adjustments to their mail delivery. The Postal Service processed 36.8 million COA requests in fiscal year (FY) 2017. Customers initiate COA requests through the Postal Service in one of two ways²:

36.8 million
COA requests were processed
by the Postal Service in FY 2017

Customers can initiate
COA requests in one of two ways:



ONLINE

The Postal Service processed **16.2 million** of these requests through its Moversguide.com platform in FY 2017. Data for these online requests is transmitted to PARS for further processing.



HARDCOPY

The Postal Service processed **20.6 million** of these requests in FY 2017. These forms are scanned by PARS and the associated data is entered into the Postal Address Database for further processing.



1. **Online** – The Postal Service processed 16.2 million of these requests through its Moversguide.com platform in FY 2017. Data for these online requests is transmitted to the Postal Automated Redirection System (PARS) for further processing.
2. **Hardcopy** – The customer completes a hardcopy COA request form and submits it to their local post office, gives it to the letter carrier, or drops it in a mail box. The Postal Service processed 20.6 million of these hardcopy requests in FY 2017. These forms are scanned by PARS and the associated data is entered into the Postal Address Database for further processing.

Nearly 96 percent of total COA requests during that time were from residential customers, and the remaining 4 percent were from businesses (see [Table 1](#)).

¹ U.S. Postal Service Office of Inspector General (OIG), *Identity Theft Potential in the Change of Address Process* (Report Number [IS-AR-08-016](#), dated August 29, 2008).

² Postal Service employees also can complete a COA for customers that have moved and left no forwarding address. Specifically, a Postal Service employee completes PS Form 3575Z on behalf of customers who have moved and left no forwarding address or have a PO Box that is closed with no forwarding order for subsequent mail.

Table 1. COA Program Data, FYs 2017 and 2018

Type of COA Order	FY 2017	Percent of Total	FY 2018 (as of March 2018)	Percent of Total
Online				
Business	623,620	1.7%	287,720	1.7%
Residential	15,564,921	42.3%	7,012,904	41.2%
Subtotal Online	16,188,541	44.0%	7,300,624	42.9%
Hardcopy				
Business	1,005,981	2.7%	499,088	2.9%
Residential	19,608,780	53.3%	9,220,546	54.2%
Subtotal Hardcopy	20,614,761	56.0%	9,719,634	57.1%
Total COA Orders	36,803,302	100.0%	17,020,258	100.0%

Source: OIG review of Postal Service data.

The Postal Service has a variety of controls in place to help prevent identity fraud using the COA process and to protect the mail and privacy of its customers. For example:

- Customers making an online COA request are charged a \$1 fee, payable by credit card. The credit card billing information is then used to validate the COA request — the Postal Service matches the address from the request with that of the credit card.
- For customers submitting a free, hardcopy COA request, the customer must sign the form to verify that he or she has read the notice and understands that an unauthorized COA order is a federal offense.
- When the Postal Service receives a COA order, two confirmation letters are sent out to validate the authenticity of the order. The first is a Confirmation Notification Letter (CNL) which is sent to the new address and contains the

customer’s name, new and old address, move type (family or individual), and move effective date. The second is a Move Validation Letter (MVL) which is sent to the customer’s old address. The MVL contains the customer’s name, old address, move type, and the move effective date. The letter is addressed to the name on the COA order or “CURRENT RESIDENT” to ensure delivery to the address, if occupied. The letter contains a notice stating that “The Postal Service received a change-of-address order for the named family or individual at that address, and asks that the customer review the information and report any incorrect or fraudulent information by calling 800-ASK-USPS (800-275-8777)”. If the named individual or family has moved, the current resident can ignore the notice and it will not have any effect on the delivery of their mail.

“The Postal Service has a variety of controls in place to help prevent identity fraud using the COA process and to protect the mail and privacy of its customers.”

The Postal Service implemented additional enhancements to its COA-related identity verification controls since our 2008 audit,³ including the following:

- **Watch List** – [REDACTED]
- **COA Watch Process** – [REDACTED]

³ U.S. Postal Service Office of Inspector General (OIG), *Identity Theft Potential in the Change of Address Process* (Report Number IS-AR-08-016, dated August 29, 2008).

- **Business Alliance Partners** – [REDACTED]
- **Domain Blocks** – [REDACTED]
- **Foreign Internet Provider (IP) Address Identification** – [REDACTED]
- **Email Alerts** – [REDACTED]
- **Invalid Email** – [REDACTED]

Groups throughout the Postal Service have various responsibilities related to these controls, including Retail staff accepting hardcopy COA requests at post offices. Furthermore, National Customer Service Center (NCSC) staff review online and hard copy COA requests and can refer potential COA-related identity theft cases to the Inspection Service for further investigation. In FY 2017, NCSC staff referred 3,546 Enterprise Customer Care (eCC) complaints related to COA requests, over 70 percent of which originated from online requests, to the Inspection Service (see Table 2). Since January 2016, the U.S. Postal Inspection Service received nearly 25,000 COA complaints,⁴ including 8,900 in 2016, 11,000 in 2017, and 5,000 for the first three months of 2018. The Enterprise Analytics group also analyzes potentially fraudulent behavior using COA and Hold Mail data from various Postal Service and Inspection Service systems, and coordinates their analysis with the Inspection Service.

⁴ These complaints originated from one of the following three sources: (1) eCC cases from the NCSC, (2) cases referred to the Inspection Service by local post office staff, and (3) cases generated by Inspection Service staff.

Table 2. eCC Complaints Referred to the Postal Inspection Service by the NCSC for Further Investigation, FYs 2017 and 2018

COA Type	FY 2017	FY 2018 (as of March 2018)
Online	2,502	945
Hardcopy	1,044	615
Totals	3,546	1,560

Source: Postal Service COA data from the National COA System, COA Support Database, and Inspection Service COAFAD.

Considering the growing threat of COA service being used to perpetrate identity theft, the Postal Service is continuing to evaluate a variety of additional controls to enhance the security of the COA process. Potential controls including collecting more information from customers during the application process (e.g., email addresses and phone numbers) and other security measures (e.g., leveraging information from other Postal Service accounts or adding in additional layers of verification for online submissions).

A news outlet recently reported on a scheme whereby a manual COA form was filed claiming that United Parcel Service (UPS) had moved its headquarters from a business park in Atlanta, GA, to a tiny apartment in the Rogers Park neighborhood in Chicago. “[N]ot only did the change go through, but it also took months for anyone to catch on. In the meantime, thousands of pieces of First-Class Mail meant for UPS poured into the apartment”.

Source: Jason Meisner, *Change-of Address Scam Moved UPS Corporate Headquarters to Tiny Rogers Park Apartment, Feds Say*, Chicago Tribune, April 23, 2018.



Finding #1: Lack of Identity Verification for Hardcopy COA Requests

The Postal Service lacks a control requiring customers to present a government-issued form of identification for review when submitting a hardcopy COA request. While Postal Service employees are performing identification verifications for COA requests in select retail units, there is no national policy outlining such a control for retail staff who receive COA requests in post offices, or delivery staff who receive COA requests along their routes.

Leading practices advocate that employees validate an individual's identity by verifying their government issued identification when conducting in-person transactions.⁵ Additionally, we reviewed mail forwarding procedures at three foreign posts in developed countries and found they each require valid identification when manually submitting a hardcopy request (see Table 3).

Table 3. Identity Verification Procedures for the Submission of Hardcopy Mail Forwarding Requests at Select Foreign Posts

Foreign Post	Control
Australia Post	Photo identification, such as an Australian driver's license or passport OR a document with your name and address, such as a bank statement AND a document that shows your signature, such as a student identification card.
Canada Post	Government issued photo identification.
Royal Mail	One item from list A: driver's license, birth certificate, passport, debit or credit card, etc. AND one item from list B: two recent utility bills, bank statement, original mortgage statement, or original bank statement.

Source: OIG analysis of foreign post identity verification procedures.

While the Postal Service is considering requiring government-issued photo identification for COA requests, there is no timetable for implementing this new control. The lack of a national policy to support such an ID-requirement control

⁵ Reducing Counterfeit Fraud through Acceptance Best Practices, Visa, 2014.

⁶ [REDACTED]

⁷ [REDACTED]

may perpetuate additional fraudulent activities and harm the Postal Service's brand as a trusted provider.

“There is no national policy outlining such a control for retail staff who receive COA requests in post offices, or delivery staff who receive COA requests along their routes.”

Recommendation #1

We recommend the Vice President, Retail and Customer Service Operations, and the Vice President, Delivery Operations, develop and implement a national policy requiring customers to present a government-issued form of identification for review when submitting a hardcopy Change of Address request.

Finding #2: Lack of [REDACTED]

The Postal Service's online COA-related identity verification processes do not incorporate [REDACTED]

[REDACTED] An example of which would be requiring a customer to enter a random 8-digit code sent to a separate email or cell phone account linked to that customer in records from authoritative sources (e.g., credit bureaus). Such a test helps verify the customer's identity by demonstrating their control over the linked account. The Postal Service currently relies on [REDACTED] such as matching the credit card holder's billing address with that of the address in the online COA request.

Leading practices [REDACTED] advocate having a verification process that includes [REDACTED]

Furthermore, many major national organizations already incorporate such [REDACTED]. Our research of these leading practices found that there are technical and customer service hurdles for developing and incorporating [REDACTED]

This includes the complexities associated with developing the enhanced technology to support the [REDACTED] and that it may take customers a little longer to complete the [REDACTED]. This research, however, concluded this more stringent layer of identity proofing is more effective for protecting customer and information security.

The Postal Service is currently considering [REDACTED]
[REDACTED]
[REDACTED].

“Leading practices advocate having a verification process that includes both

[REDACTED]
[REDACTED]
[REDACTED]”

October 2017 to examine a variety of ideas for updating COA to achieve security enhancement, process improvement, and cost recovery/revenue generation. Postal management also stated they are dedicated to safe-guarding customer information and have implemented various identity verification controls based on prior OIG recommendations.

Regarding recommendation 1, management stated that a policy change will be implemented to require customers to provide a government-issued identification for verification purposes when submitting a COA request in person to a sales and service associate or a mail carrier. The planned implementation date for this policy is March 31, 2019.

Regarding recommendation 2, management stated they developed a strategy for improving internal controls by implementing [REDACTED]. The strategy calls for internet COA to be integrated with the Postal Service’s centralized Identity Verification Service for online identity proofing — upcoming Identity Verification Service updates [REDACTED] in alignment with this recommendation. The planned implementation date for this action is September 30, 2019.

See [Appendix C](#) for management’s comments in their entirety.

Evaluation of Management’s Comments

The OIG considers management’s comments responsive to the recommendations and corrective actions should resolve the issues identified in the report.

These recommendations require 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.

Recommendation #2

We recommend the Vice President, Enterprise Analytics and Chief Information Security Officer, develop and incorporate [REDACTED] into its online Change of Address identity verification processes.

Management’s Comments

Management agreed with our findings and recommendations.

Regarding our findings, management stated COA is critical to ensuring mail is routed correctly and improper or fraudulent COA transactions result in significant cost, customer inconvenience, and negative media attention. The Postal Service launched a COA/Hold Mail Customer Experience Workgroup in

Appendices

Click on the appendix title below to navigate to the section content.

- Appendix A: Additional Information 10
 - Scope and Methodology 10
 - Prior Audit Coverage 11
- Appendix B: Recommendation Status from Prior OIG Report..... 12
- Appendix C: Management’s Comments..... 13

Appendix A: Additional Information

Scope and Methodology

Our objective was to evaluate the Postal Service's identity verification internal controls for its COA service. To accomplish our objective, we:

- Reviewed the Postal Service policies and procedures for its COA service, including the specific identity verification-related internal controls. This included reviewing the Postal Service's contract for validating identities for online requests. We also reviewed performance data on the timeliness and delivery of the MVLs and the number of online COA requests where the COA request did not align with the credit card billing address — and discussed them with Postal Service officials (we did not find any substantive issues).
- Reviewed various COA data, including the number of completed requests by channel (hardcopy and online) and whether they were residential or business requests; the number of COA-related eCC complaints referred to the NCSC; and the number of COA-related eCC complaints referred from the NCSC to the Inspection Service.
- Reviewed staff roles and responsibilities related to the COA service and identity-verification related controls. We also discussed them, along with identity verification threats, with applicable officials from various Postal Service groups including Retail and Customer Service Operations, Delivery Operations, Information Technology, Chief Information Security Office, Processing and Distribution, Computerized Forwarding System, Enterprise Analytics, Sales, and Treasurer.

- Met with Inspection Service staff to discuss their role in the COA identity verification controls and the potential risk of identity theft related to COA requests.
- Reviewed the identity verification-related COA controls for three foreign posts of developed countries – Australia Post, Canada Post, and Royal Mail.
- Reviewed various literature related to COA risks, including posts in an OIG Blog titled *The Changing Change of Address System* and related news articles.
- Reviewed leading practices related to identity verification-related controls and measures, including those from Gartner, Visa, and PIPL.⁸

We conducted this performance audit from February through August 2018 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on July 26, 2018, and included their comments where appropriate. We did not assess the reliability of any computer-generated data for the purposes of this report.

⁸ PIPL is a private company that researches identity protection and fraud.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact (in millions)
<i>National Change of Address Program</i>	Determine whether security controls over the COA manual process and National Change of Address Linkage data adequately protect the confidentiality and integrity of customer data and identify potential solutions for improving the Postal Service's acknowledgement form process.	IT-AR-14-010	9/24/2014	None

Appendix B: Recommendation Status from Prior OIG Report

A congressional inquiry asked us about the status of the recommendations contained in our 2008 report titled *Identity Theft Potential in the Change of Address Process* (Report Number [IS-AR-08-016](#), dated August 29, 2008), and additional safeguards the Postal Service subsequently taken to prevent COA-related identity theft. The report contained six recommendations, five related to controls (see Table 4 below). All of the recommendations have subsequently been addressed.

Table 4. Actions Taken by the Postal Service to Address Recommendations From the 2008 OIG Report

Recommendation	Actions Taken
<p>1 Update the Internet and Telephone COA applications to [REDACTED].</p>	<p>[REDACTED] are blocked by the Global Payment Application.</p>
<p>2 Develop and implement a plan of action, with milestones, to enhance controls for verifying that COA orders are legitimate and authorized by the owner of the address.</p>	<p>The COA scanning system was modified to detect missing signatures. Data for these forms are transmitted to the NCSC, and reject letters are sent to the customer.</p>
<p>3 Implement supervisory review and approval for overriding system warnings when processing individual COA non-business move orders from a business address and update procedures accordingly.</p>	<p>Hardcopy requests made by an individual or family (i.e., non-business) to change from a business address to a residential address are rejected by the COA scanning system. Data for these requests is transmitted to the NCSC and reject letters are sent to the customer. Non-business internet COA requests from a business address to a residential address are blocked at entry.</p>
<p>4 Investigate and provide timely feedback to the NCSC and customers on all potentially fraudulent COA complaints.</p>	<p>In February 2007, the Inspection Service, in conjunction with the NCSC, established a system to ensure all COA complaint referrals from the NCSC are directly sent to the Inspection Service. Additional requirements were set in February 2008 for the Inspection Service to investigate all COA complaints from the NCSC and to provide feedback to the customer.</p>
<p>5 Coordinate, develop, and implement policies and procedures for regularly monitoring and evaluating all potentially fraudulent COA complaints.</p>	<p>The Inspection Service implemented policies and procedures for COA complaints in February 2008, including requiring the Inspection Service monitor complaints to ensure the established policy is followed and evaluating all COA complaints.</p>
<p>6 Coordinate and implement procedures for minimizing COA data losses and system processing issues to ensure the MVLs are provided to customers in three to 10 days.</p>	<p>Reduced the lag time for dispatching MVLs and expanded the time for printing MVLs from five to six days per week.</p>

Source: Postal Service responses to the recommendations in the OIG report, *Identity Theft Potential in the Change of Address Process*, Report Number [IS-AR-08-016](#).

Appendix C: Management's Comments



August 15, 2018

MONIQUE COLTER
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Report: Change of Address Identity Verification
Internal Controls (MS-AR-18-DRAFT) Project No. 18RG007MS000

Change of Address (COA) is critical to ensuring mail is routed correctly. Improper and fraudulent COA transactions result in significant cost, customer inconvenience, and negative media attention, which can become a threat to the Postal Service reputation.

Postal management is dedicated to the safe-guarding of customer information. USPS management implemented various identity verification controls based on prior OIG recommendations.

In terms of ongoing measures, the Postal Service launched a COA/Hold Mail Customer Experience Workgroup in October 2017 that was comprised of representatives across multiple USPS business units (e.g., Enterprise Analytics, Privacy, Legal, and Cybersecurity). The workgroup examined a variety of ideas for updating COA to achieve security enhancement, process improvement, and cost recovery/revenue generation. The group aligns the possible COA updates with the CIO Roadmap for traceability, conducts analysis, performs action items, and tracks status of implementation.

The COA/Hold Mail Customer Experience Workgroup identified the following item: *explore opportunities to leverage the Identity Verification Service for Internet COA*. The Digital Integration team within the Corporate Information Security Office, which operates the Identity Verification Service (IVS), took the lead in investigating this recommendation for use. In order to understand target security controls for improvement, a Failure Modes Effects Analysis was completed and shared with the group. Subsequently, market research was conducted to identify solutions that could improve security while maintaining a positive customer experience, and estimates were obtained from potential vendors currently under contract. With the knowledge gained, a strategy for updating IVS to protect Internet COA was developed in July 2018 and briefed to stakeholders that aligns with recommendation number 2 from the report.

Recommendation 1:

We recommend the Vice President, Retail and Customer Service Operations, and the Vice President, Delivery Operations, develop and implement a national policy requiring customers to present a government-issued form of identification for review when submitting a hardcopy Change of Address request.

Management Response/Action Plan:

Management agrees with this recommendation. A policy change will be implemented to require customers who submit a Change of Address request, in person, to a sales and service associate (SSA) or a mail carrier to also provide government-issued identification for verification purposes.

Target Implementation Date:

March 31, 2019

Responsible Officials:

Vice President, Retail and Customer Service Operations
Vice President, Delivery Operations

Recommendation 2:

We recommend the Vice President, Enterprise Analytics and Chief Information Security Officer, develop and incorporate [REDACTED] controls into its online Change of Address identity verification processes.

Management Response/Action Plan:

Management agrees with this recommendation. A strategy for improving our internal controls by implementing [REDACTED] approaches was developed, which analyzes the cost, security, and customer experience impacts of [REDACTED] on USPS. The strategy calls for Internet Change of Address to be integrated with USPS' centralized Identity Verification Service for online [REDACTED]. Upcoming updates to the Identity Verification Service will implement [REDACTED] in alignment with the recommendation.

Target Implementation Date:

September 30, 2019

Responsible Officials:

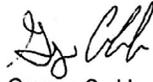
Vice President, Enterprise Analytics
Vice President, Chief Information Security Officer



Kelly M. Sigmon
Vice President
Customer Service Operations



for Kevin L. McAdams
Vice President
Delivery Operations



Gregory Crabb
Vice President
Chief Information Security Officer

Stephen M
Dearing

for Isaac S. Cronkhite
Vice President
Enterprise Analytics

Digitally signed by Stephen M Dearing
DN: cn=Stephen M Dearing, o=Corporate
Reporting, ou=Enterprise Analytics,
email=steve.m.dearing@usps.gov, c=US
Date: 2018.08.16 07:32:48 -0400

cc: CARM



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

Contact us via our [Hotline](#) and [FOIA](#) forms.

Follow us on social networks.

Stay informed.

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