Office of Inspector General | United States Postal Service

Management Alert

Issues Identified with Internet Change of Address

Report Number 22-058-R22 | April 12, 2022

Table of Contents

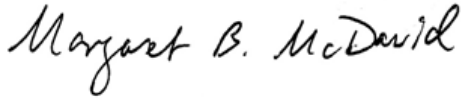
Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

April 12, 2022

MEMORANDUM FOR: JEFFREY C. JOHNSON
VICE PRESIDENT, ENTERPRISE ANALYTICS

GARY C. REBLIN
VICE PRESIDENT, INNOVATIVE BUSINESS TECHNOLOGY



FROM: Margaret B. McDavid
Deputy Assistant Inspector General for Inspection Service and Cybersecurity and Technology

SUBJECT: Management Alert – Issues Identified with Internet Change of Address (Report Number 22-058-R22)

Our objective is to notify U.S. Postal Service management of risks associated with ineffective identify verification controls on Moversguide. These issues came to our attention during our ongoing audit of the *Review of National Change of Address and Moversguide Applications* (Project Number 21-146).

We appreciate the cooperation and courtesies provided by your staff. If you have questions or need additional information, please contact Mary Lloyd, Director, Cybersecurity and Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit Response Management
Postmaster General

Results

Introduction

This management alert presents issues identified during our *Review of National Change of Address and Moversguide Applications* audit (Project Number: 21-146). Our objective is to notify U.S. Postal Service management of risks associated with ineffective identify verification controls on the Moversguide application. See Appendix A for additional information about this alert.

Background

A change of address (COA) request informs the Postal Service to reroute mail including letters, packages, and flats for all or selected individuals at a specified address. Customers can submit COA requests online, in person, or by mail. For each COA submitted, the Postal Service sends a change of address validation letter to the customer's old address to notify them that a request was received and provides instructions on reporting inaccurate or fraudulent requests. They also send a customer notification letter/welcome kit to the new address. The Postal Service's Moversguide application (Moversguide) allows customers to submit a COA request online. If customers choose this option, they must pay $1.10 using a debit or credit card to validate their identity.[1]

In 2021, the Postal Service processed nearly 36 million COA requests, completing approximately 20 million (56 percent) online. Additionally, third-party sites completed over one million online requests on behalf of Postal Service customers. These websites charge $20 to $89.95 for the service.[2]

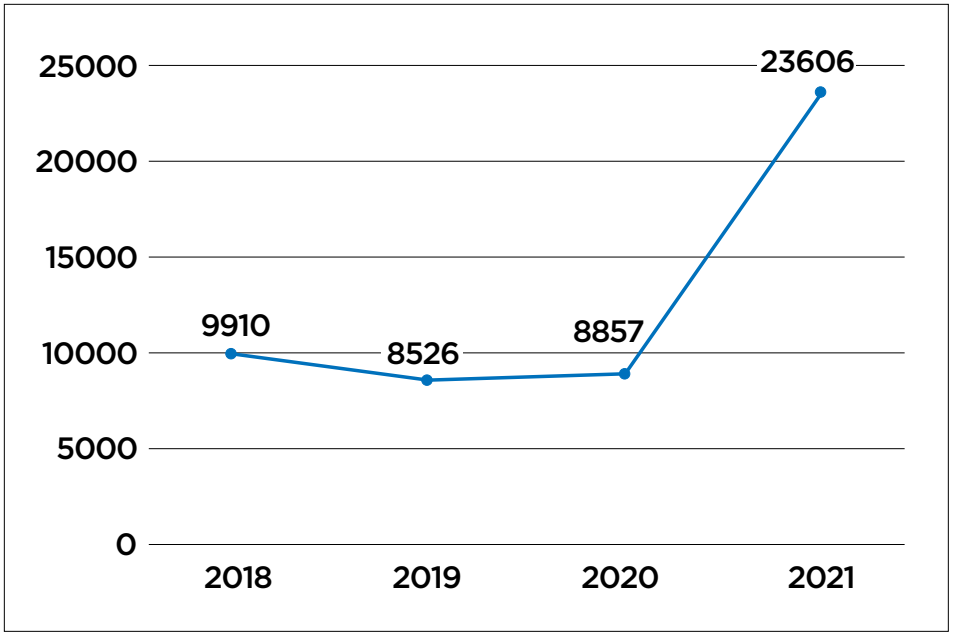
Identity verification is an important security measure to combat fraud because it ensures that a person is who they claim to be when performing online transactions.[3] With data breaches and identity theft on the rise, it is important that businesses ensure that they protect customer information from identity fraud.

Fraud can occur during the online COA process when an individual changes the address of another customer to intercept their mail and steal their identity.

Since 2018, the U. S. Postal Inspection Service has investigated and analyzed complaints received from the Postal Service to verify and document online COA fraud. The Postal Service's National Customer Support Center's COA support team performs an initial assessment to rule out non-fraud related complaints. If the team rules the COA to be potentially fraudulent, they forward it to the Inspection Service to add to their Fraudulent Analysis Database. The Inspection Service also contacts the customer to confirm fraud and/or perform analysis based on prior data received.

Figure 1 shows the total number of confirmed fraudulent COAs submitted each year — a number that more than doubled in 2021.

Figure 1. Total Fraudulent COAs Per Year



Source: U.S. Postal Inspection Service Fraud Analysis Database, retrieved February 10, 2022.

1 *Change of Address* – The Basics, USPS, December 8, 2021.
2 *Fraud Risk Steering Committee (FRSC) Fraud Report: Internet Change of Address (iCOA) Transactional Fraud & Third-Party iCOA Providers*, USPIS, January 18, 2022.
3 Identity Verification, OneSpan, January 2022.

Finding #1: Moversguide Identity Verification

The Postal Service did not implement effective identity verification controls on Moversguide and charged customers $1.10 for identity verification services that it did not provide. The Postal Service [redacted] During our testing, we found that the Moversguide only verified [redacted] Additionally, the application allows users on Moversguide and third-party sites to enter a [redacted] Our testing also confirmed that the COA validation letter and welcome packet were sent to the old and new addresses; however, if the customer does not follow the instructions to report issues, their mail is automatically forwarded. According to best practices,[4] the objective of identity proofing or verification is to ensure the applicant is who they claim to be. In addition, verification enhances security by making it more difficult for adversaries to compromise online transactions and provides confidence that digital identities are adequately protected.[5]

Table 1 shows that individuals submitted fraudulent COAs using the same forwarding address several times during 2020 and 2021. Management stated that they did not implement identity verification controls because that would deter customers from submitting online COAs and the number of fraudulent COAs are small compared to the total number submitted online.

We identified refundable revenue[6] in the amount of $21,828,827 for identity validation services that were not provided. To determine the total amount of refundable revenue, we multiplied the total number of online COAs processed in fiscal year (FY) 2021 by the fee the Postal Service charged for identity validation on the Moversguide application.

Table 1. Forwarding Addresses with Multiple Cases of Fraud

New Forwarding Address	Year of Fraudulent Activity	# Of Fraudulent Activities per Year
[redacted]	2020	50
	2021	66
[redacted]	2020	2
	2021	68
[redacted]	2020	17
	2021	38
[redacted]	2020	10
	2021	14

Source: U.S. Postal Inspection Service Fraud Analysis Database, retrieved December 20, 2021.

In 2018, the OIG issued a report[7] on ineffective identity verification controls for online COA requests. Management agreed with the recommendation and stated that they would develop a strategy to analyze the cost, security, and customer experience of identity verification controls. They also stated that they would implement the online COA process into their centralized Identity Verification Service. The target implementation date for this recommendation was September 30, 2019; however, it was closed as "Not Implemented" in November 2021. According to management, they evaluated several options that did not reveal any significant improvements in reducing the risk of fraud in the online COA process based on the added cost of performing the additional identity validation.

4 National Institute of Standards and Technology Special Publication 800-63-3, *Digital Identity Guidelines*, Section 2, March 2, 2020.
5 *Identity Proofing*, Experian, April 2013.
6 Amounts the Postal Service may owe to customers who have overpaid for a service or product.
7 *Change of Address Identity Verification Internal Controls* (Report Number MS-AR-18-005, dated August 24, 2018).

Based on our analysis, online COA fraud and attempted identity theft by individuals and organized groups increased from 8,857 to 23,606 (167 percent)[8] from 2020 to 2021. We received several recent inquiries from congressional offices regarding COA fraud. In November 2021 and January 2022, we received inquiries from the House Committee on Oversight and Reform and congressional offices in DE, IL, and NH, which included customer complaints regarding fraudulent COA requests. Further, a postmaster in IL stated that three customers complained that their mail was fraudulently forwarded to addresses in NY — a matter also brought to our attention by a congressional office.

In January 2022, the Inspection Service met with the Postal Service's Fraud Risk Steering Committee[9] to present an overview of fraud risk associated with Moversguide. During the meeting, the Inspection Service identified a recent increase in fraudulent COAs in which fraudsters [redacted] The Inspection Service connected this issue to weak identity verification controls which do not align with industry standards. On February 8, 2022, the Steering Committee voted unanimously to recommend implementing Identity Verification Services on Moversguide to mitigate identity/mail theft against Postal Service customers and eliminate third-party sites. On March 1, 2022, the Moversguide program manager rejected the recommendation citing that the Identity Verification Services do not provide significant improvements compared to the added cost of performing the additional identity validation and the increased customer friction produced from false-positive results. For example, if a customer transaction is rejected, they would have to submit the COA request in person or by mail. Management stated that they would continue to proactively monitor risk in collaboration with the Inspection Service and the Corporate Information Security Office.

Recommendation #1

We recommend the **Vice President, Enterprise Analytics**, develop controls to verify that online change of address requests are authorized by the resident of the address.

Finding #2: [redacted] Identity Verification

The Postal Service did not leverage [redacted] identity verification controls and used a less effective control for customers who [redacted] through the Moversguide application. During our testing, we verified that when customers sign up for [redacted] services directly through its website, the Postal Service validates their identity using the Customer Registration application.[11] However, when [redacted] through Moversguide, the Postal Service designed the system so that it would not utilize Customer Registration and [redacted]. According to best practices, identity verification enhances security by making it more difficult for adversaries to compromise online transactions and provides confidence that digital identities are adequately protected.[12] Management stated that they designed the application to make it easier for customers to sign up for [redacted] and they accepted the risk because they relied on customers receiving the confirmation letters for COA requests and [redacted] enrollment. However, management acknowledged that the risk was not documented or formally accepted.

Ineffective identity verification controls allow bad actors to use Moversguide to facilitate mail and identity theft against Postal Service customers, which could result in a financial loss to customers and negative impact on the Postal Service brand.

8 See Figure 1 for an analysis of the total number of fraudulent COAs per year from the Inspection Service's Fraud Analysis Database.
9 Established to combat fraud and ensure the Postal Service is fulfilling its intended purpose, spending funds efficiently, and safeguarding assets.
10 [redacted]
11 Enterprise-wide solution for registering customers and providing identity, authentication, and authorization services for USPS applications, products, and services.
12 *Identity Proofing*, Experian, April 2013.

Recommendation #2
We recommend the **Vice President, Enterprise Analytics**, and the **Vice President, Innovative Business Technology**, ensure controls are in place to verify the customer's identity when they [redacted] for [redacted] through the Moversguide application.

Management's Comments

Management disagreed with the findings and recommendations and, in subsequent email correspondence, disagreed with the monetary impact.

Regarding the findings, management stated that Moversguide is operating according to the approved controls for the COA process. Additionally, management stated that they thoroughly reviewed identity verification in a prior audit. Management stated that other than a significant fraud scheme in FY 2022, no material facts have changed since November 2021 when the recommendation from the prior audit was closed as not implemented. Finally, management concluded that based on their analysis of the proposed recommendation, millions of customers would be harmed to achieve an incremental risk reduction for several thousand customers.

Regarding recommendation 1, management stated that they thoroughly assessed the risk, cost, and failure rate of options and continue to assess these controls as sufficient. They stated that they will continue assessing opportunities to improve identity verification and security controls and requested to close this recommendation as not implemented.

Regarding recommendation 2, management stated that they thoroughly assessed the risk, cost, and failure rate of controls supporting customers [redacted] through Moversguide. Additionally, they stated that [redacted] registration happens subsequently to a successful COA. Finally, management stated that they have implemented an extensive suite of compensating controls to ensure that the [redacted] process is monitored for potential fraud and that customers are appropriately engaged. Management requests to close this recommendation as not implemented.

Regarding the monetary impact, management believes that their verification of provided source details is sufficient, appropriate, supported by National Institute of Standards and Technology standards, and operating as designed and approved in documents previously provided to the OIG.

See Appendix B for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments nonresponsive to the findings and recommendations in the report.

Regarding the findings, we considered and identified the control environment for the COA process in our report, such as the process for investigating and confirming fraudulent COAs, the automatic seven-day delay before forwarding mail to a new address, and the move validation letters sent to customers. In addition, we addressed management's concerns regarding the 2018 recommendation and our rationale for proceeding with the management alert on several occasions throughout the audit and documented this on page three of the report. Finally, the Postal Inspection Service connected the fraud scheme in FY 2022 to weak identity verification controls on Moversguide which allowed bad actors [redacted]

Regarding recommendation 1, we requested support for the analysis of the risk, cost, and failure rate of options on several occasions throughout the audit. Management provided a spreadsheet after the exit conference showing the cost and potential customer failure rate if Identity Verification Services were implemented; however, without source data we could not determine whether this information was accurate.

Regarding recommendation 2, during our testing, we verified that when customers sign up directly through the [redacted] website, the Postal Service validates their identity using the Customer Registration application; however, Moversguide was not designed to use Customer Registration. Therefore, the suite of controls implemented for [redacted] is not applicable to Moversguide.

Regarding the monetary impact, as stated in the report, Moversguide only verifies that [redacted]

We view the disagreements the recommendations as unresolved and plan to pursue them through the audit resolution process. All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action(s) are completed. 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.

Appendix A: Additional Information

Scope and Methodology

Our scope included identity verification controls and procedures over Moversguide.

To accomplish our objective, we:

- Interviewed National Customer Support Center employees to gain an understanding of how fraudulent COA requests are reported, tracked, and remediated.
- Interviewed Inspection Service employees to determine their role in tracking and monitoring fraudulent COAs.
- Obtained and analyzed data on all confirmed fraudulent COAs from FYs 2018 through 2022.
- Tested Moversguide to validate and document the identify verification process for COAs by:
  - Establishing addresses using P.O. Boxes to make online address changes.
  - Submitting a COA [redacted]
  - Verifying that the COA confirmation was sent within seven days.
  - Verifying that mail was forwarded after the confirmation card was received.
- Verified whether customers could sign up for [redacted] through Moversguide and [redacted]

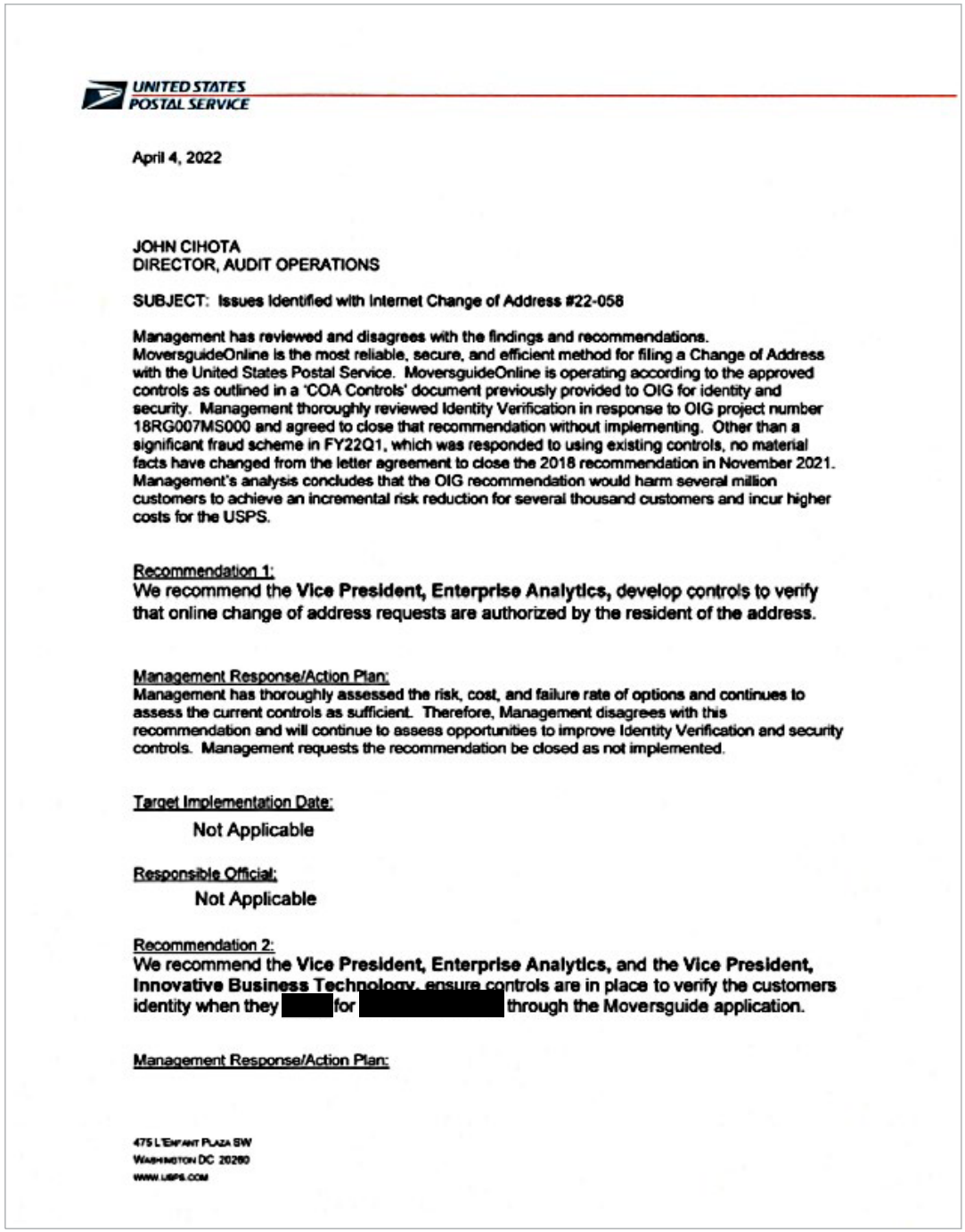
We conducted this performance audit from January through April 2022 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain 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. We discussed our observations and conclusions with management on March 11, 2022 and included their comments where appropriate.

We assessed the reliability of Fraudulent Analysis Database data by obtaining screenshots of how the Inspection Service pulled the data. We also compared the number of records in the database with the number of records in the spreadsheet. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date
Management Alert: Issues Submitting and Processing Change of Address Requests	Notify Postal Service officials of issues present in the COA system	21-017-R21	2/2/2021
Change of Address Identity Verification Internal Controls	Evaluate and present results regarding the Postal Service's identity verification internal controls for COA service	MS-AR-18-005	8/24/2018

Appendix B: Management's Comments



UNITED STATES POSTAL SERVICE

April 4, 2022

JOHN CIHOTA
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Issues Identified with Internet Change of Address #22-058

Management has reviewed and disagrees with the findings and recommendations. MoversguideOnline is the most reliable, secure, and efficient method for filing a Change of Address with the United States Postal Service. MoversguideOnline is operating according to the approved controls as outlined in a 'COA Controls' document previously provided to OIG for identity and security. Management thoroughly reviewed Identity Verification in response to OIG project number 18RG007MS000 and agreed to close that recommendation without implementing. Other than a significant fraud scheme in FY22Q1, which was responded to using existing controls, no material facts have changed from the letter agreement to close the 2018 recommendation in November 2021. Management's analysis concludes that the OIG recommendation would harm several million customers to achieve an incremental risk reduction for several thousand customers and incur higher costs for the USPS.

Recommendation 1:
We recommend the **Vice President, Enterprise Analytics,** develop controls to verify that online change of address requests are authorized by the resident of the address.

Management Response/Action Plan:
Management has thoroughly assessed the risk, cost, and failure rate of options and continues to assess the current controls as sufficient. Therefore, Management disagrees with this recommendation and will continue to assess opportunities to improve Identity Verification and security controls. Management requests the recommendation be closed as not implemented.

Target Implementation Date:
Not Applicable

Responsible Official:
Not Applicable

Recommendation 2:
We recommend the **Vice President, Enterprise Analytics, and the Vice President, Innovative Business Technology,** ensure controls are in place to verify the customers identity when they [redacted] for [redacted] through the Moversguide application.

Management Response/Action Plan:

475 L'Enfant Plaza SW
Washington DC 20260
www.usps.com

Management has thoroughly assessed the risk, cost, and failure rate of controls supporting customer [redacted] to [redacted] through Moversguide. [redacted] registration happens subsequently to a successful Change of Address and relies on the control processes implemented for Change of Address. [redacted] will continue to conform to the identity validation procedures set forth by the Change of Address application.

Additionally, management has already implemented an extensive suite of compensating controls to ensure that [redacted] through Moversguide is monitored for potential fraud and customers are appropriately engaged. Therefore, Management disagrees with this recommendation and will continue to assess opportunities to improve Identity Verification and security controls, as it does on an ongoing basis. Management requests the recommendation be closed as not implemented.

Target Implementation Date:

Responsible Official:

Jeffrey C. Johnson
Vice President, Enterprise Analytics

Gary C. Reblin
Vice President, Innovative Business Technology

cc: Manager, Corporate Audit Response Management
Postmaster General

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

For media inquiries, please email
press@uspsoig.gov or call 703-248-2100