



August 29, 2008

THOMAS G. DAY  
SENIOR VICE PRESIDENT, INTELLIGENT MAIL AND ADDRESS QUALITY

ALEXANDER E. LAZAROFF  
CHIEF INSPECTOR, POSTAL INSPECTION SERVICE

KATHLEEN AINSWORTH  
VICE PRESIDENT, RETAIL OPERATIONS

JORDAN M. SMALL  
VICE PRESIDENT, DELIVERY OPERATIONS

DEAN J. GRANHOLM  
ACTING VICE PRESIDENT, NETWORK OPERATIONS MANAGEMENT

SUBJECT: Audit Report – Identity Theft Potential in the Change of Address Process  
(Report Number IS-AR-08-016)

This report presents the results of our audit of Identity Theft Potential in the Change of Address (COA) Process (Project Number 08RG009IS000). Our objective was to determine if COA controls ensure that address change requests were properly authorized and validated to minimize potential identity theft. This self-initiated audit addresses the operational risks associated with the U.S. Postal Service's COA process. Click [here](#) to go to Appendix A for additional information about this audit.

### Conclusion

The Postal Service should improve controls to ensure proper authorization and validation of COA requests, which can be made via Internet Change of Address (ICOA), Telephone Change of Address (TCOA), and hard copy (Postal Service [PS] Form 3575, Official Mail Forwarding Change of Address Order, index cards, and letters). The ICOA and TCOA methods are operating as intended [REDACTED]

[REDACTED]. In addition, monitoring controls surrounding the COA complaints process should be improved. Strengthening these controls will further reduce weaknesses in the COA process that, if left unmitigated, could contribute to identity theft.

## Authentication of Internet and Telephone Change of Address Orders

[REDACTED]. This will further reduce the risk of diverting mail to unauthorized addresses, which contributes to potential fraud, identity theft, and monetary loss to customers. Click [here](#) to go to Appendix B for analysis of this topic.

We recommend the Senior Vice President, Intelligent Mail and Address Quality, direct the Manager, Address Management, to:

1. Update the Internet and Telephone Change of Address applications [REDACTED].

## Authentication of Hard Copy Change of Address Orders

Authorization and validation controls surrounding the hard copy COA process do not always prevent the acceptance and processing of unauthorized COA requests. Unlike the electronic COA processes, the hard copy COA process does not have sufficient controls in place to verify COA orders are legitimate and authorized by the owner of the address. The Postal Service faces challenges to ensure a proper balance between providing timely customer service and assuring proper customer authorization for the hard copy COA process. While policy indicates that employees should reject and return orders with no signature to delivery units,<sup>3</sup> in some cases orders without signature are

<sup>1</sup> Postal Service policy requires the customer's credit card billing address to match either the customer's old or new address. The eCapabilities and Paypal payment processing systems for ICOA and TCOA, respectively, interact with the Address Verification System to ensure the customer's billing address matches the customer's old or new ZIP Code [REDACTED]

<sup>2</sup> [REDACTED]

<sup>3</sup> Handbook PO-250, *Consumer Answer Book*, Chapter 4, Section 4-4; *Change of Address Forms Processing System (CFPS) Scanner Site Operations Training Course Operator/Supervisor Participant Handbook*; and CFS Keying Rules-Table B-2, Name and Data Information and Table C-1, Reject Reasons-Form Not Signed; U.S.C., Title 18, Part 1, Chapter 63, Section 1342 (Fictitious Name or Address).

<sup>3</sup> Handbook PO-250, *Consumer Answer Book*, Chapter 4, Section 4-4; *Change of Address Forms Processing System (CFPS) Scanner Site Operations Training Course Operator/Supervisor Participant Handbook*; and CFS Keying Rules-Table B-2, Name and Data Information and Table C-1, Reject Reasons-Form Not Signed; U.S.C., Title 18, Part 1, Chapter 63, Section 1342 (Fictitious Name or Address).

still being processed. Additionally, we identified other issues with these forms, including signature mismatches, and Postal Service employees' signatures or initials rather than the customers'. Ensuring proper authorization of these hard copy forms could prevent illegal diversion of mail, which could damage the postal brand and lead to identity theft. Click [here](#) to go to Appendix B for analysis of this topic.

We recommend the Vice President, Intelligent Mail and Address Quality, coordinate with the Vice President, Retail Operations, the Vice President, Delivery Operations, and the Vice President, Network Operations, to:

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.

### **Employee Override of System Warnings**

Computerized Forwarding System (CFS) employees could override the Change of Address Forms Processing System (CFPS) warning notification messages when manually processing individual COA non-business move orders from a business address. While CFPS procedures<sup>4</sup> prohibit employees from processing these types of COA orders, management instructed CFS employees to override this warning message and process these changes. Implementing stronger controls through supervisory review and approval could mitigate opportunities for employee conflicts of interest and the creation of false or fictitious COA orders, which could lead to identity theft and fraud. Click [here](#) to go to Appendix B for our detailed analysis of this topic.

We recommend the Vice President, Retail Operations, direct the Manager, Customer Service Standardization, to:

3. Implement supervisory review and approval for overriding system warnings when processing individual Change of Address non-business move orders from a business address and update procedures accordingly.

### **Continuous Monitoring and Evaluation of Change of Address Complaints**

The Postal Inspection Service was not regularly monitoring, evaluating, and notifying the National Customer Support Center (NCSC) and customers regarding the status and resolution of potentially fraudulent COA complaints. Policy<sup>5</sup> states promptness and resolution are indicators of increased customer satisfaction in the complaint process, and the referring offices should receive a letter for case closure. These issues occurred because the Postal Inspection Service had no policies or procedures for regularly

---

<sup>4</sup> *CFPS Scanner Site, Operations Training Course, Operator/Supervisor Participant Handbook*, Table C-1, Reject Reasons.

<sup>5</sup> *Postal Operations Manual*, Issue 9, dated July 2002 (updated With *Postal Bulletin* revisions through January 17, 2008), Sections 161, Consumer Services, Overview; and 167.34(e), Responding to Customer Comments and Complaints, By Letter.

monitoring, evaluating, or notifying the NCSC and customers concerning the status and resolution of potentially fraudulent COA complaints. Addressing COA complaints would contribute to the protection of the Postal Service's brand, its commitment to protect customer information, and its efforts to combat identity theft. We will report this non-monetary impact for goodwill/branding in our *Semiannual Report to Congress*. Click [here](#) to go to Appendix B for our detailed analysis of this topic.

We recommend the Chief Inspector, Postal Inspection Service, direct the Inspector in Charge, Criminal Investigations, to:

4. Investigate and provide timely feedback to the National Customer Support Center and customers on all potentially fraudulent change of address complaints.

We recommend the Chief Inspector, Postal Inspection Service, and the Senior Vice President, Intelligent Mail and Address Quality, direct the Inspector in Charge, Criminal Investigations, and Manager, Address Management, respectively, to:

5. Coordinate, develop, and implement policies and procedures for regularly monitoring and evaluating all potentially fraudulent COA complaints.

### **Processing Move Validation Letters in Response to Change of Address Orders**

Generally, we found the Postal Service provides Move Validation Letters (MVLs) to customers in a timely manner. However, we found 230 occurrences where the agency processed MVLs outside the established timeframe<sup>6</sup> of 3 to 10 days, out of 78,389 COA requests filed by customers between April 8 and 13, 2008. This occurred because the Postal Service did not align its MVL processing time with FedEx's delivery schedule.<sup>7</sup> COA data losses and system processing issues at CFS sites and Remote Encoding Centers (REC) also contributed to the delays. Although the 230 exceptions represent a small percentage of the total processed, providing MVLs to customers in a timely manner decreases the likelihood of false or fraudulent COAs contributing to identity theft.

During the audit, management changed its MVL processing schedule to align with FedEx's delivery schedule, and as a result, we are not providing a recommendation regarding this condition. However, we are providing a recommendation to minimize COA data losses and system processing issues to ensure MVLs are provided to customers on a timely basis. Click [here](#) to go to Appendix B for our detailed analysis of this topic.

---

<sup>6</sup> Handbook PO-250, *Consumer Answer Book*, Chapter 4, Section 4-3, Confirmation Letter.

<sup>7</sup> The NCSC utilizes the services of FedEx for transporting MVLs to the delivery points on a 6-day schedule. However, NCSC only operates on a 5-day schedule to create and process MVLs.

We recommend the Senior Vice President, Intelligent Mail and Address Quality, direct the Manager, Address Management, to:

6. Coordinate and implement procedures for minimizing Change of Address data losses and system processing issues to ensure the Move Validation Letters are provided to customers in the 3- to 10-day timeframe.

### Management's Comments

Management agreed with all six recommendations. Regarding recommendation 1, the Manager, Address Management, will work with the Assistant Treasurer, Payment Technologies, and their strategic alliance partner, Imagitas, Inc., to update the ICOA application [REDACTED]. In addition, the Manager, Address Management; the Assistant Treasurer, Payment Technologies; the Manager, Corporate Customer Contact; and the supplier, Convergys PayPal, will work together to update the TCOA application. The completion date for updating both applications is March 31, 2009.

For recommendation 2, the Manager, Address Management, will coordinate with the managers of Customer Service Standardization, Delivery Operations, and Processing Operations to develop a joint action plan to enhance the signature controls for PS Form 3575 by March 31, 2009. Once the plan is finalized and implemented, Address Management will implement a process to review a statistical sampling of all PS Forms 3575 each quarter and will report findings on any deviations from established policy and procedures to the appropriate functional groups. Address Management will continue to pursue ICOA as its long-term strategy to ensure the entries of COA orders are legitimate and duly authorized by the customers. Additionally, on May 7, 2008, Customer Service Standardization issued a standup talk to all CFS units reemphasizing that the units should not finalize PS Forms 3575 without signatures. Management plans an additional joint standup talk for CFS Operations and Delivery by September 1, 2008, to reemphasize the initialing and dating requirements for PS Form 3546, Official Change/Correction to Mail Forwarding Change of Address Order, and PS Form 3575Z, Employee Generated Change of Address.

Regarding recommendation 3, management will make changes to the next release of the CFPS software (version 4.0). The software change will reject the forms for an individual or family COA nonbusiness move order from a business address prior to acceptance. The next release of the CFPS software has a tentative deployment date of May 2009, contingent on other Postal Automated Redirection System dependencies.

In response to recommendations 4 and 5, the Postal Inspection Service plans to issue a policy update by December 31, 2008, addressing investigative procedures for the review of COA complaints and documentation, and requiring close coordination and feedback to the NCSC on the status of their review of COA complaints. The updated Postal Inspection Service policy requires documentation in the Financial Crimes

Database (FCD) on customer and NCSC contacts, as well as quarterly monitoring to ensure compliance with the policy. The Postal Inspection Service will communicate with NCSC and provide semiannual updates on new schemes that may affect the COA process. The NCSC will also monitor and evaluate potentially fraudulent COA complaints in conjunction with the Postal Inspection Service. Management stated the NCSC has already modified its system to record the resolution of complaints as provided by the Postal Inspection Service.


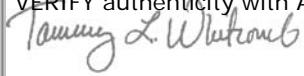
For recommendation 6, management will ensure that customers receive MVLs in a timely manner. The response indicated that the NCSC took several significant actions to improve the timely delivery of MVLs. In February 2008, the NCSC implemented a change to reduce dispatching lag time for MVLs, and in April 2008 expanded the printing of MVLs from 5 to 6 days a week. Management indicated these changes resulted in an 18.7 percent improvement in the number of MVLs delivered within 5 days of the date the customer COA was entered. NCSC will continue implementing procedures to ensure that they receive all COAs and will enhance management oversight of the MVL program. To review management's comments in their entirety, click [here](#) or go to Appendix C.

### Evaluation of Management's Comments

The U. S. Postal Service Office of Inspector General (OIG) considers management's comments responsive to the recommendations, and their corrective actions should resolve the issues identified in the report.

The OIG considers recommendations 1, 2, 4, and 5 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 follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Gary C. Rippie, Director, Information Systems, or me at (703) 248-2100.

E-Signed by Tammy Whitcomb   
VERIFY authenticity with ApproveIt  


Tammy L. Whitcomb  
Deputy Assistant Inspector General  
for Revenue and Systems

Attachments

cc: Ross Philo  
George W. Wright  
Delores J. Killete  
Anthony M. Pajunas  
Harold E. Stark  
Alice M. VanGorder  
James D. Wilson  
Amy S. Rose  
Lori M. Wigley  
Annette P. Raney  
James W. Kiser  
Thomas M. Addams  
John F. Bolger  
Henry Herrera  
Katherine S. Banks

## APPENDIX A: ADDITIONAL INFORMATION

### BACKGROUND

Identity theft is America's fastest growing crime. The Federal Trade Commission defines identity theft as a fraud that is committed by using a person's identifying information without authority. This can occur when mail is diverted to another location by completing unauthorized COA orders. Over 40 million Americans change their address annually, which creates a tremendous challenge for the Postal Service in maintaining a high-quality repository of addresses. A person's identity is valuable and if someone steals it to commit fraudulent acts, it can affect every aspect of that person's life, including their credit and ability to purchase a house or car or obtain a job or medical care.

There are three processes for making a COA request:

- Hard copy COA
- ICOA
- TCOA

**Table 1: COA Orders FY 2007**

Method	No. Orders	Percentage
Hard Copy COA	41,832,042	86.7
ICOA	6,334,336	13.1
TCOA	101,628	0.2
<b>Total Orders</b>	<b>48,268,006</b>	<b>100.0</b>

The ICOA and TCOA methods require a \$1.00 fee charged to the customer initiating the COA request. This fee causes a transaction to occur which is used for customer identity verification purposes. However, the hard copy COA process does not verify the customer's identity. The Postal Service processed ICOA orders using eCap to process credit card payments through First Data Merchant Services<sup>8</sup> until January 2008. Credit card transactions are currently processed through Bank of America Merchant Services. The Postal Service contracts with Convergys<sup>9</sup> to handle TCOA orders using the PayPal payment processor. Both payment processor systems interact with the Address Verification System to ensure the ZIP Code and street number in the address provided matches the billing address on file with the credit card issuer.

<sup>8</sup> Since December 2004, the Postal Service used First Data Merchant Services to process credit card transactions for customers submitting ICOAs using moversguide.com.

<sup>9</sup> Convergys provides services to the Postal Service by allowing customers to change their address over the telephone with or without speaking to a TCOA representative.



Once the Postal Service processes COAs, it mails a MVL and then a Confirmation Notification Letter (CNL) to the customer's old and new address, respectively. Both letters are designed to notify customers of the COA filing and provide contact instructions if the information is incorrect.

Processing a COA involves the Postal Service business units outlined below.

<b>Postal Service Office</b>	<b>COA Function</b>
Customer Service Operations	Manages 115 CFS sites nationwide and oversees the processing of all COA orders.
Corporate Customer Contact	Oversees the contract with Convergys for processing TCOA orders.
Network Operations	Responsible for domestic mail processing and transportation networks, which includes the REC accepting and processing the COA images received from the CFPS.
Delivery Operations	Responsible for delivering MVLs and CNLs within standard delivery time.
NCSC	The NCSC manages COA business operations, which include hosting data transfers between CFS sites and the NCSC; overseeing contract operations for MVLs and CNLs; and managing the alliance with Imagitas, Inc., which handles the ICOA orders. In addition, they are responsible for receiving and reviewing COA complaints and forwarding potential fraudulent complaints to the Postal Inspection Service.
Postal Inspection Service	Receives information from the NCSC on potentially fraudulent COA orders and complaints for further review and investigation.

## **OBJECTIVE, SCOPE, AND METHODOLOGY**

Our objective was to determine if COA controls ensure that address change requests are properly authorized and validated to minimize potential identity theft. To accomplish our objective, we identified risks associated with the three COA methods – ICOA, TCOA, and hard copy COA. We identified and evaluated controls in place for each of the three COA methods and determined if controls were being consistently applied as follows:

- Authorization – Determine if the customer authorized the change.
- Accuracy – Determine if the controls in place ensure COA order data are accurate.
- Completeness – Determine if controls in place ensure COAs are sufficiently complete.

- Segregation of Duties – Determine if controls are in place to prevent inappropriate processing of COAs.
- Timeliness – Determine if employees process MVLs and CNLs timely.
- Monitoring/Evaluation – Determine if management adequately evaluates complaints on an ongoing basis to detect potential identity theft.

We reviewed documentation, policies and procedures, and interviewed key officials at the NCSC, Customer Service Operations, the Postal Inspection Service, Consumer Affairs, Corporate Customer Contact, Delivery Operations, Engineering, and the OIG Hotline to determine their roles in the COA process. In addition, we selected a judgmental sample and visited 10 CFS sites<sup>10</sup> in seven Postal Service areas<sup>11</sup> to review COA documents and scanned images in the COA Reporting System to identify potential control weaknesses that may lead to identity theft.

To review the TCOA process, we visited the Corporate Customer Call Center operated by Convergys in Jacksonville, North Carolina. To determine if controls were operating as intended, we conducted three tests [REDACTED]

[REDACTED]. We also conducted a test to submit an additional ICOA order using a credit card that belonged to an individual not associated with the customer's name and old or new address.

We visited the NCSC to observe the MVL process. To determine the number of days for processing the MVL, we obtained 78,390 MVL data records for the period April 8 through 13, 2008. Finally, we reviewed 139 complaints about potentially fraudulent COAs for the period of October 6, 2006, through December 31, 2007, that the NCSC forwarded to the Postal Inspection Service to determine if complaints are adequately evaluated on an ongoing basis. We interviewed employees of the NCSC, the Postal Inspection Service, Consumer Affairs, Corporate Customer Contact, and the OIG Hotline to determine how they handle incoming COA complaints.

We conducted this performance audit from January through August 2008 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We assessed the reliability of

---

<sup>10</sup> We conducted our audit work at CFS sites in Greensboro and Raleigh, North Carolina; Louisville, Kentucky; Atlanta and Marietta, Georgia; Latham, New York; Indianapolis, Indiana; Santa Ana, California; Phoenix, Arizona; and Memphis, Tennessee.

<sup>11</sup> These CFS sites are in the following Postal Service areas: Capital Metro, Eastern, Southeast, Northeast, Great Lakes, Pacific, and Western.

computer-generated data supporting the audit finding and concluded the data was sufficiently reliable to meet our audit objective. We discussed our observations and conclusions with management officials during the audit and on July 25, 2008, and included their comments where appropriate.

## PRIOR AUDIT COVERAGE

<b>Report Title</b>	<b>Report Number</b>	<b>Final Report Date</b>	<b>Monetary Impact</b>	<b>Report Results</b>
<i>Management Advisory – Postal Service’s Procedures to Validate Change of Address Orders</i>	OE-MA-03-005	May 21, 2003	None	The Postal Service’s process for validating COA orders was adequate. The MVL helped detect when fraudulent orders were processed. However, if the Postal Service considers accepting COA requests by telephone, <sup>12</sup> it might want to explore controls to prevent the acceptance of fraudulent COA orders.
<i>Change of Address – Application Control Review</i>	IS-AR-06-013	July 17, 2006	None	Existing application controls are sufficient to ensure the overall integrity of the data within the COA system. However, improvements could be made primarily in the areas of access controls, segregation of duties, protection of sensitive information, information security assurance documentation, and audit logging.
<i>Identity Theft Potential in Postal Service Information Systems</i>	IS-AR-08-006	March 6, 2008	\$137,428	The Postal Service should enhance controls surrounding the protection of sensitive and personally identifiable information in the systems we reviewed. Specifically, management needs to make improvements in the areas of user access, date protection, and the collection and use of personally identifiable data on forms. Also, the Postal Service should discontinue one of its employment verification systems.

<sup>12</sup> This 2003 audit was conducted prior to the implementation of TCOA.

## APPENDIX B: DETAILED ANALYSIS

### Authentication of Internet and Telephone Change of Address Orders



The Postal Service has a contract with Imagitas, Inc., for providing online services to process ICOAs and a draft Requirements and Analysis Specification for Postal Service COA Phase 3 with Convergys to process TCOAs. The NCSC is responsible for ICOA and TCOA business rules and both methods charge an identity verification fee of \$1. The Postal Service uses this fee to validate if the customer's street number and ZIP Code in the address provided matches the billing address on file with the credit card issuer.



We also conducted tests to submit ICOA orders using credit cards that belonged to individuals not associated with the customer's name and old or new addresses. The system was unable to verify the customer's identity with the information provided and the COA orders were properly rejected.

### Authentication of Hard Copy Change of Address Orders

Authorization and validation controls surrounding the hard copy COA process do not always prevent the acceptance and processing of COA requests which may not be legitimate and authorized by the owner of the address. The Postal Service faces challenges to ensure a proper balance between providing timely customer service and assuring proper customer authorization for the hard copy COA process.

Our review of 217 COA orders (PS Forms 3575<sup>13</sup>) from 10 CFS sites showed:

- Twenty-two COA orders (10 percent) without customer signatures or with lines or marks in the signature box.
- Twenty-four COA orders (11 percent) where the customer name and signature did not match.
- Five COA orders (2 percent) with the Postal Service employee's signature or initials in the customer's signature box.

The Postal Service often receives COA orders in the mail for processing. Some forms do not have signatures and others contain invalid lines or marks in the signature box. CFS site employees normally review PS Forms 3575 prior to scanning.

Customers' failure to sign (authorize) PS Forms 3575 is the most common error and CFS employees should reject forms without customer signatures and return them to delivery units.<sup>14</sup> If not detected before scanning, REC sites also should reject these orders and return them to the delivery units. In addition, any person who uses a fictitious, false, or assumed title, name, or address, or name other than his own proper name, shall be fined under Title 18 or imprisoned not more than 5 years, or both.

The Postal Service has determined that ICOA is the most efficient way for customers to file a COA request. Therefore, the NCSC has planned the "Behind the Counter" pilot project, which will increase the use of the ICOA method. This will be done by replacing all PS Forms 3575 at the counter with ICOA cards. The Postal Service is conducting this pilot project from June 16 to August 31, 2008, at 597 Post Offices in the Denver, Colorado; Minneapolis, Minnesota; and Tampa, Florida, service areas and plans to evaluate the results.

### Employee Override of System Warnings

CFS employees could override the CFPS warning notification message when manually processing individual COA non-business move orders from a business address. When CFS employees manually enter the business address, a screen warning appears indicating they will not be able to complete the record. Procedures state employees should reject address changes for non-business moves from business addresses. However, management issued a bulletin to instruct employees to override the system warning. Also, policy<sup>15</sup> states individuals should not have assigned duties that cause a conflict of interest or present an undetectable opportunity for malicious wrongdoing, fraud, or collusion.

---

<sup>13</sup> PS Form 3575 is a hard copy COA order.

<sup>14</sup> Handbook PO-250, *Consumer Answer Book*, Chapter 4, Section 4-4; *CFPS Scanner Site Operations Training Course Operator/Supervisor Participant Handbook*; and CFS Keying Rules-Table B-2, Name and Data Information and Table C-1, Reject Reasons-Form Not Signed; U.S.C., Title 18, Part 1, Chapter 63, Section 1342 (Fictitious Name or Address).

<sup>15</sup> Handbook AS-805, *Information Security*, March 2002, updated with *Postal Bulletin* revisions through November 23, 2006, Section 6-3.1 Separation of Duties and Responsibilities.

## Continuous Monitoring and Evaluation of Change of Address Complaints

The Postal Inspection Service was not regularly monitoring, evaluating, and notifying the NCSC and customers regarding the status and resolution of potentially fraudulent COA complaints, because it had no policies or procedures for doing so. Addressing COA complaints would contribute to the protection of the Postal Service's brand, its commitment to protect customer information, and its efforts to combat identity theft. We will report this non-monetary impact for goodwill/branding in our *Semiannual Report to Congress*.

The NCSC has a process for evaluating COA complaints. Complaints identified as potentially fraudulent are forwarded to the Postal Inspection Service for further review, investigation, and resolution. We reviewed 139 potentially fraudulent COA complaints the NCSC referred to the Postal Inspection Service. These consisted of only hard copy, ICOA, and White Fence<sup>16</sup> complaints, as there were no TCOA complaints. As indicated in the table below, only 18 (13 percent) were assigned investigation case numbers,<sup>17</sup> while 36 (26 percent) were assigned FCD<sup>18</sup> numbers.

**Table 2: Complaints Assigned a Case or FCD Number by the Postal Inspection Service**

COA Type	Total Complaints	Case Numbers Assigned	Case %	FCD Numbers Assigned	FCD %
Hard Copy	99	14	14	21	21
ICOA	29	2	7	11	38
White Fence	11	2	18	4	36
<b>Total</b>	<b>139</b>	<b>18</b>	<b>13</b>	<b>36</b>	<b>26</b>

The potentially fraudulent COA complaints are for the period October 6, 2006, to December 31, 2007, with reported monetary impact totaling \$468,212. Customers reported loss of identity, stolen checks, and the establishment of auto loans, credit cards, and, in at least one instance, a mortgage, in their names. Currently the Postal Inspection Service selectively reviews complaints based on ongoing investigations and categorization of cases. Improvements are needed in monitoring, evaluating, and notifying the NCSC and customers regarding the status and resolution of this type of complaint.

The Postal Inspection Service and the NCSC are aware of the issues surrounding COA complaints and are evaluating solutions to improve the COA complaint and resolution

<sup>16</sup> White Fence is a third party company providing free COA services online to Postal Service customers.

<sup>17</sup> Management assigns case numbers if COA complaints warrant further investigation by the Postal Inspection Service.

<sup>18</sup> The FCD is a web-based investigative application the Postal Service uses to capture mail theft and identity theft complaints. This system is available to all Postal Service inspectors, however, not all potentially fraudulent COA complaints the NCSC forwarded to the Postal Inspection Service are placed in the FCD database and assigned FCD numbers.

process. Also, the NCSC is in the process of developing the COA Watch Initiative, a trend analysis system designed to prevent the use of Postal Service COA methods for malicious purposes.

### **Processing Move Validation Letters in Response to Change of Address Orders**

Generally, we found the Postal Service provides MVLs to customers in a timely manner. However, we found 230 occurrences where the agency processed MVLs outside the established timeframe<sup>19</sup> of 3 to 10 days, out of 78,389 COA requests filed by customers between April 8 and 13, 2008. Our analysis indicates the average number of days to process MVLs ranged from .20 to 1.39.

We analyzed the MVL data for each of the 10 CFS sites to determine the anomalies by identifying the range of processing days. We found occurrences where the longest MVL processing time ranged from 18 to 98 days. Postal Service's MVL processing time, FedEx's delivery schedule, COA data losses, and system processing issues at CFS sites and RECs contributed to the delays. Although the 230 exceptions represent a small percentage of the total processed, providing MVLs to customers in a timely manner decreases the likelihood of false or fraudulent COAs contributing to identity theft.

---

<sup>19</sup> Handbook PO-250, *Consumer Answer Book*, Chapter 4, Section 4-3, Confirmation Letter.



**APPENDIX C: MANAGEMENT’S COMMENTS**

THOMAS G. DAY  
SENIOR VICE PRESIDENT  
INTELLIGENT MAIL AND ADDRESS QUALITY



August 25, 2008

LUCINE WILLIS  
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Management Response to Audit Report – Identity Theft Potential in the Change of Address Process (Report Number IS-AR-08-DRAFT)

Thank you for the opportunity to review and comment on the subject draft audit report. Management agrees with each of the findings presented in the report and provides the following responses to each of the audit findings and recommendations. We do not believe that this report contains any propriety or restricted business information and may be disclosed pursuant to the Freedom of Information Act.

**Recommendation 1.** Update the Internet and Telephone Change of Address applications to

Management agrees with the recommendation to update the Internet and Telephone Change of Address applications

**Recommendation 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.

The Manager Address Management will coordinate with the Manager, Customer Service Standardization, Manager, Delivery Operations, and Manager, Processing Operations to develop a joint action plan to enhance the signature controls for PS Form 3575 *Official Mail Forwarding Change of Address Order* by March 31, 2009. Once the plan is finalized and implemented, Address Management will implement a process to review a statistically valid sampling of all PS Forms 3575 each quarter, and report findings to the appropriate functional groups as needed should any deviation from established policy and procedures be identified. Address Management will continue to pursue as its long-term strategy the use of Internet Change of Address to ensure the entry of change-of-address orders are legitimate and duly authorized by the customer.

475 L'ENFANT PLAZA SW  
WASHINGTON DC 20260-4400  
202-268-8200  
Fax: 202-268-4482  
www.usps.com

- 2 -

**Recommendation 5.** Coordinate, develop, and implement policies and procedures for regularly monitoring and evaluating all potentially fraudulent COA complaints.

Management agrees with the recommendation to monitor and evaluate potentially fraudulent COA complaints in conjunction with Inspection Service. The National Customer Support Center has already modified its existing information management system to record all change of address complaint resolutions status as provided by the Inspection Service.

**Recommendation 6.** Coordinate and implement procedures for minimizing Change of Address data losses and system processing issues to ensure the Move Validation Letters are provided to customers in the 3- to 10-day timeframe.

Management agrees with the recommendation to ensure that Move Validation Letters (MVL) are provided to the moving customer timely. As noted in the draft report, the National Customer Support Center has already taken several significant actions to improve the timely delivery of the MVL. In February 2008 a change was implemented to reduce the lag time in dispatching outgoing MVLs to both FedEx and Postal Service ground transportation networks. In April 2008 a change was implemented to expand the printing of MVLs from 5 days per week to 6 days per week. As a result of these changes, an 18.7% increase in the number of MVLs delivered within 5 days of the customer entry of their change-of-address has been achieved. NCSC will continue to implement procedures to ensure that all COAs are received and to enhance the management oversight of the MVL program.

If you have any questions, please contact Alice VanGorder, Manager, Address Management, at 901-681-4650.



Thomas G. Day

cc: Mr. Lazaroff  
Mr. Pajunas  
Mr. Philo  
Ms. Ainsworth  
Mr. Granholm  
Ms. Kilette  
Mr. Small  
Mr. Wright  
Mr. Hill  
Ms. VanGorder  
Ms. Banks  
Ms. Harris  
Ms. Raney  
Mr. Kiser  
Mr. Wilson

Alexander LAZAROFF  
Chief, Postal Inspection



August 20, 2008

LUCINE WILLIS  
DIRECTOR, AUDIT OPERATIONS  
USPS OFFICE OF INSPECTOR GENERAL

SUBJECT: Management Response to the Audit Report – Identity Theft Potential in the Change of Address Process

We appreciate the opportunity to provide comment to the audit report of the Potential Identity Theft in the Change of Address Process. The attached represents management's response to the USPS Office of Inspector General recommendations.

If you have any questions, please contact Debra Harris, Acting Inspector in Charge, Criminal Investigations, at 202-268-8496.

Alexander Lazaroff

Attachment

cc: Thomas G. Day  
Anthony M. Pajunas  
Ross Philo  
Kathleen Ainsworth  
Dean J. Granholm  
Delores J. Killete  
Jordan M. Small  
George W. Wright  
Zane Hill  
Alice M. VanGorder  
Katherine S. Banks  
Debra A. Harris  
Annette Raney  
James W. Kiser  
James D. Wilson

475 L'ENFANT PLAZA SW  
WASHINGTON, DC 20260-2100  
202-268-5515  
FAX: 202-268-7318  
WWW.USPS.COM

**Response to USPS-OIG Audit of  
Identity Theft Potential in the Change of Address Process**

Summary of Management Response

We have reviewed the draft report of the Identity Theft Potential in the Change of Address Process. The report contains no confidential business sensitive or law enforcement sensitive information that would preclude disclosure under the Freedom of Information Act. We are in agreement with the conclusion reached in the report and concur completely with both recommendations. We agree and will continue to provide professional and timely responses to reports of potential fraud against Postal Service customers. The Inspection Service remains committed to protecting the reputation of the Postal Service. In fact, the Inspection Service has initiated a process to enhance the transmission of information between the National Customer Support Center (NCSC) and the Inspection Service regarding suspicious change of address (COA) requests.

**OIG Recommendation 4**

The Chief Postal Inspector direct the Inspector in Charge, Criminal Investigations, to investigate and provide timely feedback to the NCSC and customers on all potentially fraudulent COA complaints.

**OIG Recommendation 5**

The Chief Postal Inspector, in conjunction with the Senior Vice President, Intelligent Mail and Address Quality, direct the Inspector in Charge, Criminal Investigations, and Manager, Address Management, respectively, to coordinate, develop, and implement policies and procedures for regularly monitoring and evaluating all potentially fraudulent COA complaints.

Management Response

Management agrees with both recommendations.

The Inspection Service in February 2007, in conjunction with the NCSC, established an e-mail system which enabled the NCSC to electronically refer complaints directly to the Postal Inspection Service's Loss Prevention Coordinator assigned to the geographic location of the complainant and to Inspection Service National Headquarters. In February 2008, the Inspection Service enhanced their Financial Crimes Database (FCD) to enable referrals from the NCSC to be downloaded directly into the FCD. Each complaint is assigned a unique complaint number, and each complaint can be readily identified as an NCSC referral.

To ensure all COA referrals from the NCSC are provided adequate investigative attention and attention is properly documented, the Inspection Service will issue a policy update addressing required investigative attention. The requirements will be:

- (1) All COA complaints received from the NCSC will be reviewed.
- (2) The investigating inspector will contact the customer and annotate contact in the FCD.
- (3) The investigating inspector will respond to the NCSC via e-mail with the results of their initial review. The response will indicate whether the Inspection Service will initiate an investigation or close the complaint. If the complaint is closed with no further attention warranted, the inspector will provide a reason why no further attention will be given.
- (4) The Inspection Service National Headquarters will quarterly monitor NCSC complaints to ensure established policy is followed.

- (5) The National Headquarters Program Manager will communicate with the NCSC and semiannually provide updated information on new schemes identified which could impact the change of address process.

The Inspection Service will issue a policy update addressing the required investigative attention by December 31, 2008.

KATHY AINSWORTH  
VICE PRESIDENT, RETAIL OPERATIONS



August 20, 2008

JOHNSON JOHN

SUBJECT: Identity Theft Potential in the Change of Address Process Report Number [IS-AR-08]-  
DRAFT

Recommendation [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.

Note: Responses provided below are from the Vice President of Retail Operations only. Other functional groups will provide their responses separately.

Response:

- o May 7-Customer Service Standardization issued a Standup Talk to all CFS Units that re-emphasized that under no circumstances is CFS Operations to finalize a PS Form 3575 without a signature. (Signed Certification on file)
- o September 1-Joint Standup Talk for CFS, Operations and Delivery. Standup Talk will be generated to re-emphasize use of PS Form 3546 and PS Form 3575Z must be initialed and dated in order for the forms to be finalized.

Management agrees that stronger controls need to be in place to minimize identity theft and fraud.

Recommendation [3]:

Implement supervisory review and approval for overriding system warnings when processing individual Change of Address non-business move orders from a business address and update procedures accordingly.

Response:

Management agrees with the recommendation. Changes will be made to the next release of the COA Forms Processing System software (Version 4.0). Software change will address the issue by rejecting the forms for an individual or family Change of Address non-business move order from a business address prior to acceptance. This action is performed by software and the forms will not be presented to a CFS employee for finalization.

Target Completion:

CFPS is a subsystem of the Postal Automated Redirection System and interacts with all PARS components. CFPS software version 4.0 has a tentative deployment date of May 2009, contingent upon other PARS dependencies.

A handwritten signature in black ink, appearing to read "Kathy Ainsworth".

Kathy Ainsworth

475 L'ENFANT PLAZA SW ROOM 7017  
WASHINGTON, DC 20260-1600  
202-268-6500  
FAX: 202-268-3331  
www.usps.com