

Management Alert – Issues Identified with Counterfeit Postage

MANAGEMENT ALERT

Report Number 25-072-1-R26 | October 15, 2025



COUNTERFEIT

Table of Contents

Cover

Transmittal Letter 1

Results 2

 Introduction 2

 Background 2

 Finding #1 [REDACTED] 4

 [REDACTED] 4

 Recommendation #1: 6

 Postal Service Response 6

 OIG Evaluation 6

 Appendix A: Additional Information 7

 Appendix B: Management’s Comments 9

Contact Information 11

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

October 15, 2025

MEMORANDUM FOR: HEATHER DYER
VICE PRESIDENT,
CHIEF INFORMATION AND SECURITY OFFICER

Mary H. Lloyd

FROM: Mary Lloyd
Deputy Assistant Inspector General
for Operations, Performance, and Services

SUBJECT: Management Alert – Issues Identified with Counterfeit Postage
(Report Number 25-072-1-R26)

This management alert presents issues identified during our ongoing audit of the Counterfeit Postage Program (Project Number 25-072). The objective is to provide U.S. Postal Service officials immediate notification of identified issues that require immediate attention and remediation.

All recommendations require U.S. Postal Service Office of Inspector General's (OIG) concurrence before closure. Consequently, the OIG requests written confirmation when corrective action is completed. The recommendation should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed.

We appreciate the cooperation and courtesy provided by your staff. If you have questions or need additional information, please contact Laura Roberts, Director, Network Operations Team 2, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction

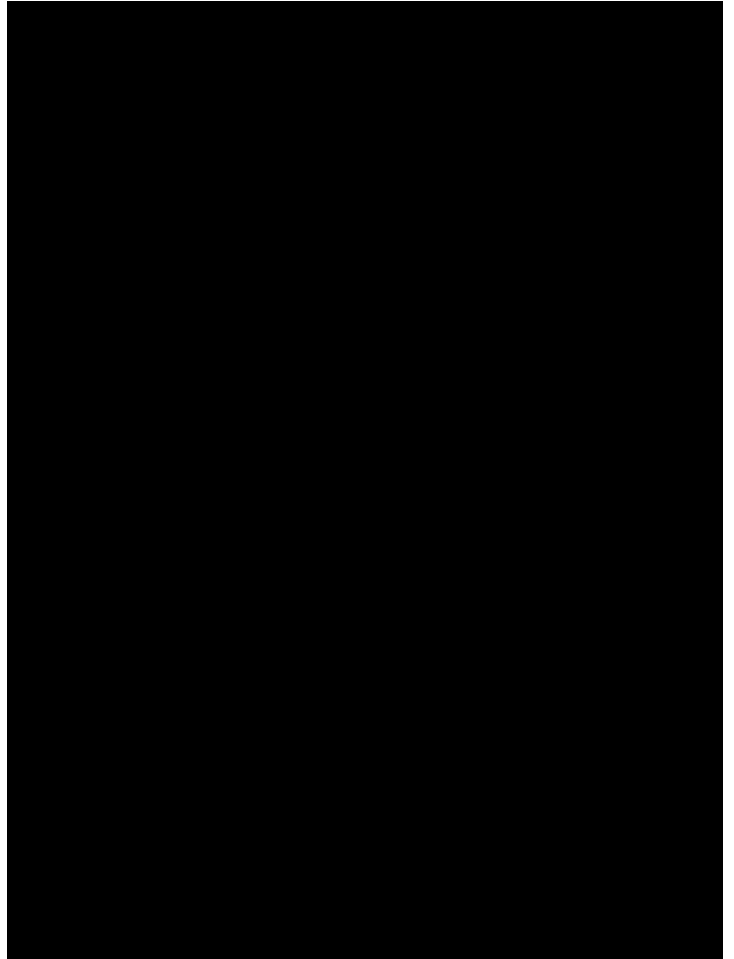
This management alert presents issues the U.S. Postal Service Office of Inspector General (OIG) identified during the Counterfeit Postage Program audit (Project Number 25-072). Our objective is to provide immediate notification of these issues related to an identified deficiency in the [REDACTED] of counterfeit [REDACTED]. See [Appendix A](#) for additional information about this audit.

Background

The Postal Service is a self-funded entity that primarily finances its operations through postage sales, with package delivery comprising a major portion of its services. During fiscal year (FY) 2024, the Postal Service shipped 7.3 billion packages, generating \$32.3 billion in revenue. The Postal Service offers multiple options to purchase postage, including through third party vendors, its Click-N-Ship online service, and over the retail counter at local post offices. Every USPS package label contains specific information that can be used for multiple reasons, to include detecting and intercepting potentially fraudulent package labels (or package labels that have not been paid for). This includes an identifier that specifies [REDACTED]

[REDACTED] (see Figure 1).

Figure 1. [REDACTED]



Source: *Introduction to Revenue Fraud Investigations Training*, dated November 2024.

The U.S. Postal Inspection Service, the law enforcement arm of the Postal Service, noted there has been a significant increase in the creation, sale, and use of counterfeit postage since 2020.¹ According to the Postal Service, in 2022 the Chief Information Security Office assumed responsibility from the Postal Inspection Service for preventing counterfeit postage. In 2023, the Chief Information Security

Office introduced new technology and processes, like the Counterfeit Package Intercept Process (hereafter “Intercept Process”), [REDACTED]

[REDACTED]

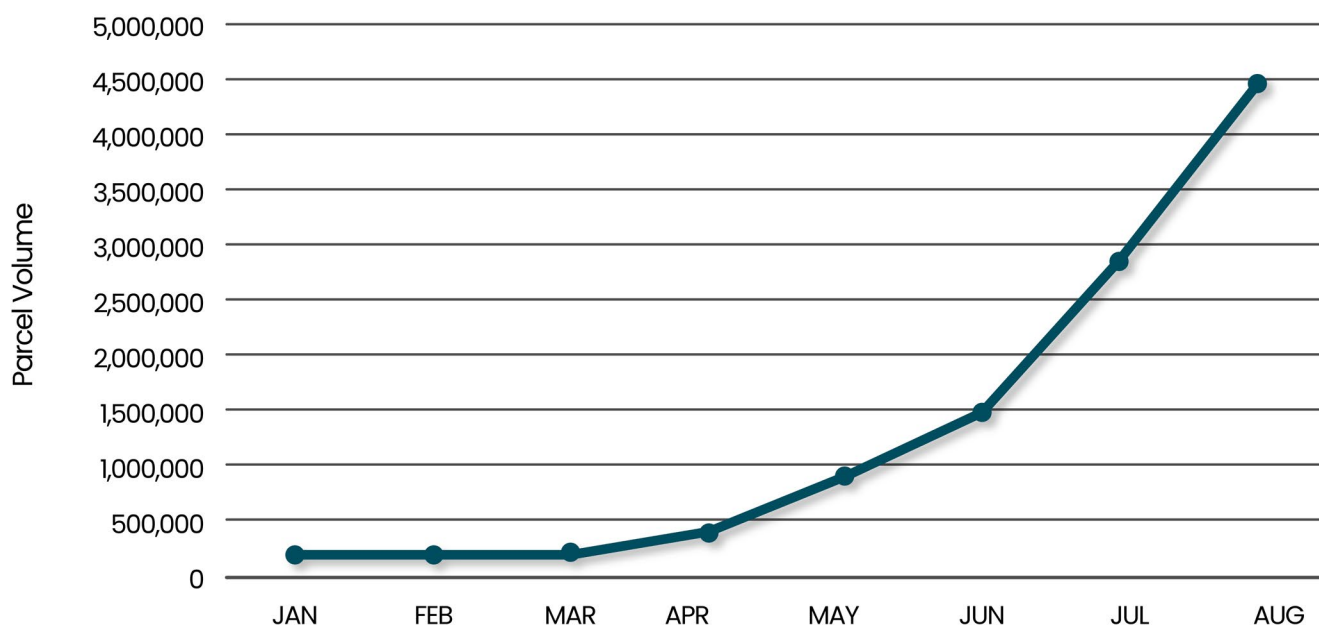
¹ Counterfeit postage refers to unauthorized markings or indicia on mailed items that falsely indicate valid postage has been paid.

Finding #1 [REDACTED]

The Postal Service [REDACTED]
[REDACTED] We reviewed Product Tracking and Reporting (PTR)² data for the period of January 1, 2024, through August 31, 2025, to identify packages with unpaid [REDACTED] The PTR system aggregates package information from

multiple sources based on scan events [REDACTED]. This data can be used to retrieve [REDACTED] information for package labels generated from multiple sources. We found that from April through August 2025, the number of suspected counterfeit [REDACTED] surged over 1,500 percent (see Figure 2).

Figure 2. Increase in Packages With Unpaid [REDACTED]



Source: OIG analysis of PTR data.

We also conducted a limited-scope mail test at nine mail processing facilities³ between May and July 2025 to assess the effectiveness of the Postal Service's Intercept Process. During these site visits, we inducted packages with various counterfeit labels through machines equipped with the Intercept Process.⁴ [REDACTED]

² PTR is the system of record for all delivery status information for packages and mail with trackable services. The PTR system accepts [REDACTED] while also extracting scan events [REDACTED]

³ [REDACTED]

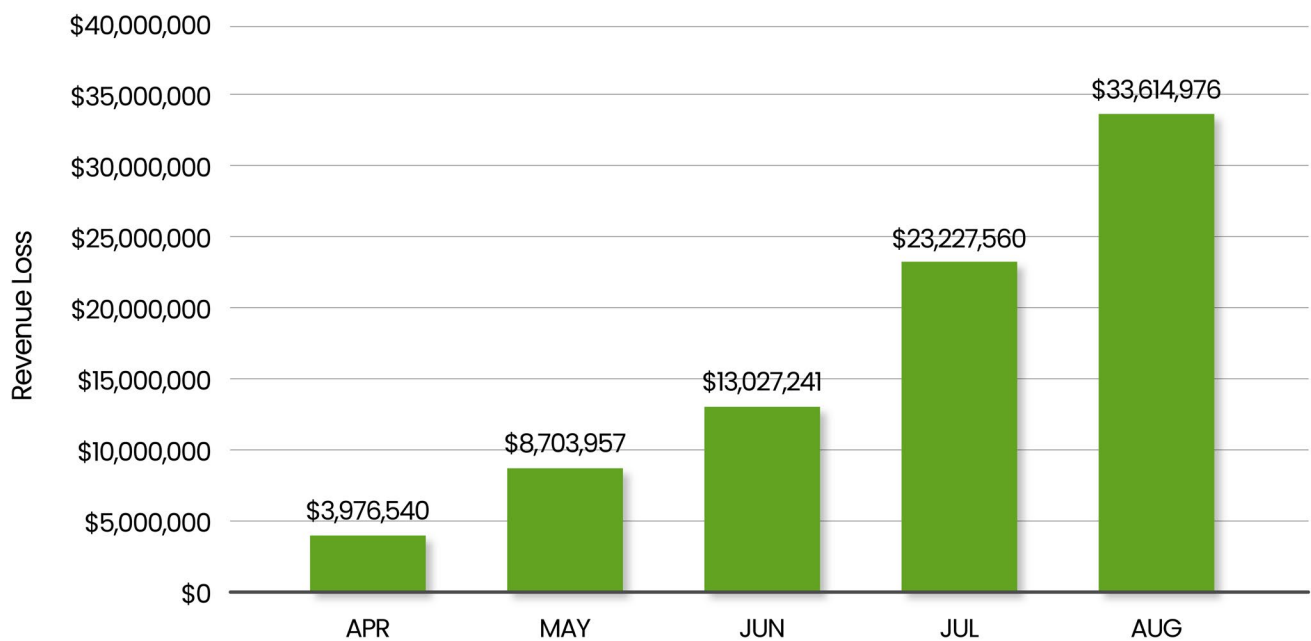
⁴ During our controlled testing, we removed the packages, whenever possible, after the mail processing machine completed its sort.

According to Postal Service management, the Intercept Process was not developed to [REDACTED] [REDACTED] It was developed to detect counterfeit [REDACTED]

Postal Service management stated that when designing its initial detection method, it focused [REDACTED]

If the Postal Service does not verify [REDACTED] in accordance with policy,⁵ further revenue loss will result. Postal Service Headquarters management has recognized the severity of this issue and is committed to implementing corrective measures. Failure to implement controls in a timely manner will likely result in the expanded use of counterfeit labels. We estimate the loss of revenue due to unpaid [REDACTED] [REDACTED] to be approximately \$82.5 million from April through August 2025 (see Figure 3), and without the implementation of timely measures to remedy this issue, the Postal Service could lose an additional \$403 million in revenue during the next 12 months.

Figure 3. Estimated Revenue Lost



Source: OIG analysis of FY 2024 Revenue, Pieces, & Weights and PTR data.

5 Domestic Mail Manual, Section 604.6.1, dated July 13, 2025.

Recommendation #1:

We recommend that **Vice President, Chief Information Security Officer**, prioritize enabling detection and interception of counterfeit [REDACTED].

Postal Service Response

Management agreed with the finding and recommendation. Regarding recommendation 1, management stated that it agreed to prioritize detection and interception enhancements and plans to implement system changes to related equipment by June 1, 2026. With its response, management provided examples of efforts it is making to address counterfeit [REDACTED]. Specifically, it provided examples of trucks containing packages with unpaid [REDACTED] that were rejected during a sampling blitz in August and September of 2025. Management also initiated a technical solution to include counterfeit [REDACTED] in the intercept process. The target implementation date is June 1, 2026.

Regarding the monetary impact, management agreed that \$33.6 million of the estimated revenue loss and \$403 million of the projected revenue loss were the “upper bounds” of estimated monetary impacts. In additional communications, we subsequently confirmed that management agreed with the remaining \$48.9 million of our estimated revenue loss.

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

OIG Evaluation

The OIG considers management’s comments responsive to this recommendation as the corrective actions should resolve the issue identified in the report.

Appendix A: Additional Information

Scope and Methodology

The scope of this management alert focused on the Postal Service Counterfeit Package Intercept Process. To accomplish our objective, we:

- Interviewed Postal Service Headquarters management to gain an understanding of the Intercept Process and the internal control environment regarding the detection of counterfeit package labels.
- Reviewed PTR to identify packages with unpaid [REDACTED].
- Judgmentally selected nine mail processing facilities and conducted unannounced site visits between May and July 2025 (see Table 1).
- Performed a limited-scope mail test to determine if counterfeit [REDACTED] can pass through the Intercept Process undetected.

Table 1. Judgmentally Selected Site Visit Locations

Processing Facilities	State	Date
[REDACTED]	[REDACTED]	05/15/25
[REDACTED]	[REDACTED]	06/24/25
[REDACTED]	[REDACTED]	07/29/25
[REDACTED]	[REDACTED]	07/28/25
[REDACTED]	[REDACTED]	06/25/25
[REDACTED]	[REDACTED]	05/15/25
[REDACTED]	[REDACTED]	06/24/25
[REDACTED]	[REDACTED]	06/26/25
[REDACTED]	[REDACTED]	05/14 - 05/15/25

Source: OIG analysis based on Postal Service data from Facilities Database and site visits.

We conducted this performance audit from August through October 2025 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.

On August 19, 2025, we notified management of the identified issue prior to our issuance of a draft of this

management alert. We discussed our observations and conclusions with management on September 29, 2025, and included its comments where appropriate.

In planning and conducting the audit, we obtained an understanding of the Counterfeit Package Intercept Process internal control structure to help determine the nature, timing, and extent of our audit procedures. We reviewed the management controls for overseeing the process and mitigating associated risks. Additionally, we assessed the internal control components and underlying principles, and we determined that the control activity component is significant to our audit objective.

We developed audit work to ensure that we assessed this control. Based on the work performed, we identified internal control deficiencies related to control activities that were significant within the context of our objectives. Our recommendation, if implemented, should correct the weaknesses we identified.

We assessed the reliability of Product Tracking and Reporting data by performing testing for completeness, reasonableness, accuracy, and

validity. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

The OIG did not identify any prior audits or reviews related to the objective of this audit within the last five years.

Additional information or recommendations regarding the issues addressed in this Management Alert may also be included in the final report resulting from our related ongoing audit.

Appendix B: Management's Comments



October 8, 2025

LAURA LOZON
ACTING DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: *Management Alert – Counterfeit* [REDACTED]
[REDACTED]

Thank you for providing the Postal Service with an opportunity to review and comment on the finding and recommendation contained in the draft audit report, *Management Alert – Counterfeit* [REDACTED]

Address the Finding: The United States Postal Service (USPS) agrees with the OIG that we [REDACTED] but we have an identified action plan to resolve this.

Since the summer of 2023, the Fraud prevention team has tracked and monitored fraudulent activity on all revenue streams. During this time, the team has made strategic decisions to prioritize investments that would focus on the largest sources of fraud and maximize impact of disrupting fraudulent behaviors while minimizing the risks/harm to good shipper behavior. [REDACTED]

[REDACTED] Management identified this issue six months prior to the OIG's finding and quickly began strategizing how to close the gaps. [REDACTED]

The USPS agrees that the OIG's assessment of monetary impact of \$33.6M per month, or \$403M per year, represents the upper bound of a range while our estimate of \$19.7M per month and \$236.4M per year, represents the lower bound.* CISO's priority in fraudulent package intervention is to act on fraudulent behavior in such a manner that minimizes the risk of harm to good shippers and customers. [REDACTED]

[REDACTED] There are inherent delays [REDACTED] which could reduce the monetary impact by as much as 50%.

Finally, it is important to note that both estimates do not represent a net increase to fraud liability, but rather a shift from one source of fraud to another. The CISO team has closed many of the initial system gaps and is in the midst of closing more gaps across multiple channels. Overall fraud has declined since 2023, and this trend will continue as we continue to roll out our mitigation plans.

*Please note, the monthly lower and upper bounds were calculated using August 2025 data. Annual figures represent the August data multiplied by 12.

Recommendation 1:

We recommend that **Vice President, Chief Information Security Officer**, prioritize enabling detection and interception of counterfeit [REDACTED]

Management Response/Action Plan:

Management agrees to prioritize enabling detection and interception of counterfeit [REDACTED] and plans to implement system changes to certain [REDACTED] equipment in Q3 FY2026.

Target Implementation Date: 06/01/2026

Responsible Official:

- Chief Information Security Officer
- Director of Cybersecurity Engineering

E-SIGNED by HEATHER L DYER
on 2025-10-08 14:05:40 EDT

Heather Dyer
Vice President, Chief Information and Security Officer

cc: Corporate Audit & Response Management

OFFICE OF INSPECTOR GENERAL UNITED STATES POSTAL SERVICE



This document contains sensitive information that has been redacted for public release. These redactions were coordinated with USPS and agreed to by the OIG.

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