Enterprise Payment Account Fraud

MANAGEMENT ALERT

Report Number 25-072-2-R26 | February 10, 2026

Table of Contents

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

February 10, 2026

MEMORANDUM FOR: LUKE GROSSMANN
CHIEF FINANCIAL OFFICER AND EXECUTIVE VICE PRESIDENT

SHIBANI GAMBHIR
VICE PRESIDENT, SALES INTELLIGENCE & SUPPORT

ANGELA LAWSON
VICE PRESIDENT, TECHNOLOGY APPLICATIONS

FROM: Mary K. Lloyd
Deputy Assistant Inspector General for Operations, Performance & Services

SUBJECT: Management Alert: Enterprise Payment Account Fraud (Report Number 25-072-2-R26)

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

All recommendations require U.S. Postal Service Office of Inspector General (OIG) concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All 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.

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
Vice President, Chief Information Security Officer
Vice President, Controller
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 prevention of Enterprise Payment Account (EPA) fraud. See Appendix A for additional information about this audit.

Background

The Postal Service offers mailers the ability to obtain and pay for package labels through various systems designed to improve customer experience. One of these systems is the [redacted]. In May 2022, the [redacted] was updated to provide mailers with the ability to buy package labels using their EPA. Mailers can prefund their EPA or make payments through supported methods, such as Automated Clearing House (ACH) bank transfers and credit cards. The system deducts payments for labels from mailer EPAs at the end of each day.

When a mailer obtains a shipping label through the [redacted], the system creates a label for the mailer to use on their package [redacted], which is used internally by Postal Service systems to [redacted]. One system that uses the [redacted] is the counterfeit postage Intercept Process. This system, first introduced in February 2023, identifies counterfeit-labeled packages on mail processing machines by [redacted]. Generally, if a label has [redacted], the Intercept Process [redacted].

Management of the [redacted] involves multiple Postal Service stakeholders. Sales Intelligence & Support is the business owner, and Technology Applications is responsible for developing and maintaining the [redacted]. Other stakeholders involved related to counterfeit postage include the Chief Information Security Office (CISO), which is responsible for protecting the Postal Service from cyberthreats, U.S. Postal Inspection Service (USPIS), the Postal Service's law enforcement agency, and Corporate Treasury ("Treasury"), the office responsible for managing the agency's cash and banking relationships. The CISO is responsible for the counterfeit postage Intercept Process. USPIS investigates counterfeit postage and proposes criminal or civil action against counterfeiters. Treasury conducts fraud detection and mitigation within Postal Service financial transactions, to include those that may be associated with [redacted] fraud.

Finding #1: Insufficient Controls to Prevent Enterprise Payment Account Fraud

We identified a significant rise in mailers [redacted] This occurred, in part, because the Postal Service did not implement proper controls in its systems to [redacted], resulting in over $125 million in revenue fraud in December 2025 alone.

Surge in Labels Using [redacted]

We found that almost 11 percent of the [redacted] from February through December 2025 were [redacted] (over 110 million of 1 billion). Prior to February 2025, virtually no labels were [redacted] A surge in labels obtained through [redacted] occurred in 2025 because these [redacted] Counterfeiters have increasingly turned to this type of fraud as well as [redacted], which we addressed in an earlier management alert.[1]

Treasury warned stakeholders of the potential for [redacted] fraud as early as January 2025 and provided some recommendations to address the vulnerability. However, not all the recommendations were implemented and, in May 2025, the Postal Service first identified EPA fraud. Within weeks, internal teams discussed system enhancements and potential countermeasures to correct the growing threat. Despite these discussions, the implementation of robust controls lagged, allowing EPA fraud to escalate unabated.

During our ongoing audit, in August 2025, we discovered EPA fraud [redacted] while conducting site visits and through subsequent data analysis. We informed the CISO management team of our observations, and they confirmed the labels were fraudulent. By early January 2026, the Postal Service shut down over 2,800 fraudulent accounts and announced enhanced security features in some systems. Management stated that in November 2025, they [redacted] Additionally, management intends to implement further measures that require [redacted] by February 2026. Despite management's attempts to mitigate EPA fraud, the measures have not been timely or robust enough to counter this fraud scheme, and it continues to persist.

> "Despite management's attempts to mitigate EPA fraud, the measures have not been timely or robust enough to counter this fraud scheme, and it continues to persist."

Lack of Effective Systems and Internal Management Controls

The initiation and perpetuation of this fraud occurred due to multiple Postal Service systems failing [redacted] before allowing customers access to EPAs. A recent executive order emphasized the crucial need for verifying payments in the management of government financial transactions, highlighting the importance of validation.[2] However, these systems [redacted] While some controls were in place to perform basic [redacted], these systems did not effectively prevent the use of:

- [redacted]

1 *Management Alert – Issues Identified with Counterfeit Postage* (Report Number 25-072-1-R26, dated October 15, 2025).
2 Executive Order 14249, Protecting America's Bank Account Against Fraud, Waste, and Abuse, March 25, 2025.

[redacted]

Additionally, during development of the [redacted] there were three critical failures: (1) there was no requirement that Treasury, the team charged with [redacted] fraud risk mitigation at the Postal Service, be consulted and have decision authority over the release; (2) Treasury does not have a list of minimum standard requirements for [redacted] systems; and (3) the [redacted] was not tested to ensure controls were in place to prevent fraud, [redacted]

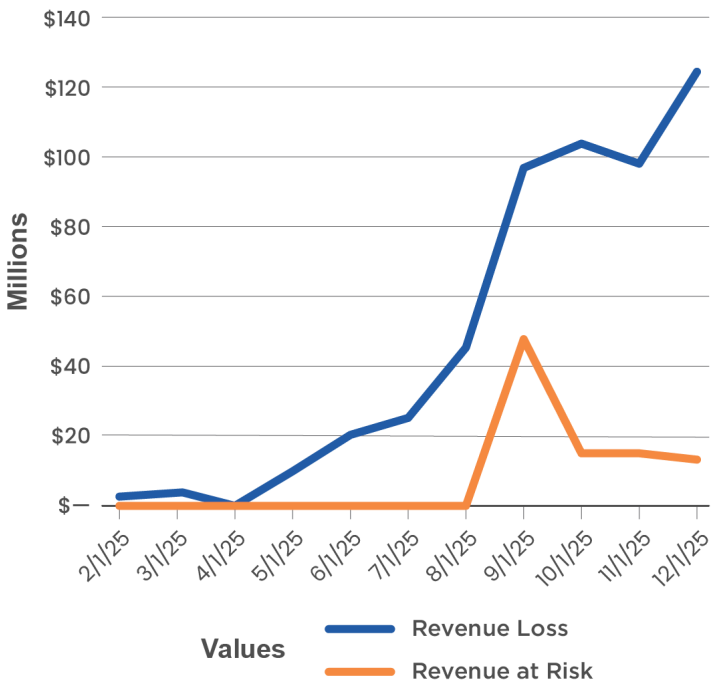
Fraud Scheme Causing Significant Financial Losses

EPA fraud has proven to be a significant issue for the Postal Service. Of the $858 million generated in December from [redacted], more than 14 percent, or $125 million in postage, was fraudulently issued and never collected. This was the highest amount recorded in a single month.

From February through December 2025, as indicated by the blue line in Figure 1, we determined the Postal Service lost over $537 million in expected revenue because of [redacted] the Postal Service delivered to their destinations. Additionally, in Figure 1, the orange line shows that the Postal Service faced a potential loss of another $97 million due to [redacted], with one mailer contributing to the surge in September.[3] Nonetheless, there remains a significant risk that mailers [redacted]

As a part of our broader work on counterfeit postage, we are also assessing USPIS's response to the criminal fraud associated with counterfeit postage, including this issue, and will address this in our main report.

Figure 1. Revenue Loss and Revenue at Risk from Unpaid [redacted]



Source: U.S. Postal Service Product Tracking and Reporting system and data provided by Postal Service management in December 2025 and January 2026.

> "From February through December 2025… the Postal Service lost over $537 million in expected revenue because of [redacted]

[3] [redacted] It is uncertain whether this was legitimate or an act of fraud.

As the Postal Service faced a $9 billion loss in fiscal year 2025 and with the recent report by the Postal Service of the potential of running out of cash by early 2027, the agency must take urgent action to protect its revenue. The Postal Service stated they first identified this type of fraud in May 2025, yet in January 2026, their mitigation efforts have still not been effective. If further action is not taken, we estimate that the Postal Service will lose an additional $1.3 billion in revenue in calendar year 2026 due to EPA fraud.

Recommendation #1

We recommend the **Vice President, Sales Intelligence & Support**, in coordination with the **Vice President, Technology Applications**, shut down access to the [redacted], until the associated fraud issues are fully addressed.

Recommendation #2

We recommend the **Vice President, Technology Applications**, implement a requirement that Corporate Treasury concurrence be required on all future software releases involving [redacted] prior to release.

Recommendation #3

We recommend the **Chief Financial Officer and Executive Vice President**, develop a list of minimum standard requirements for [redacted] systems to prevent fraud and require those minimum standards to be met prior to all future software releases involving [redacted].

Recommendation #4

We recommend the **Vice President, Technology Applications**, implement a requirement to test fraud prevention controls prior to software releases involving [redacted].

Recommendation #5

We recommend the **Chief Financial Officer and Executive Vice President**, only allow [redacted] methods.

Postal Service Response

Management agreed with the finding and provided no further comments regarding it. It also agreed with all five recommendations and agreed in subsequent correspondence with the monetary impact. See Appendix B for management's official comments in their entirety.

Regarding recommendation 1, management agreed that additional controls are needed to address current fraud methods. It stated it has implemented controls, including enhanced [redacted] in early November 2025, [redacted] It also plans to implement additional controls, including the ability to [redacted] The target implementation date is April 30, 2026.

Regarding recommendation 2, management stated it would add Treasury as an approver on the Pricing & Acceptance Tech Services Change Control Board for the Enterprise Payment System and for any [redacted] that require customer [redacted]. Management stated it will also add Treasury as a technology solution life cycle approver for both the technical solutions requirements and customer acceptance testing approvals. The target implementation date is April 30, 2026.

Regarding recommendation 3, management stated that there are existing requirements for Postal Service systems and platforms. Management will build on these requirements to develop a Business Needs Statement, which will include requirements for addressing [redacted] system vulnerabilities. The target implementation date is April 30, 2026.

Regarding recommendation 4, management stated that [redacted] for the Enterprise Payment System and all [redacted] systems prior to release. [redacted] The target implementation date is April 30, 2026.

Regarding recommendation 5, management stated it expects to implement in February 2026 a requirement for new customers using an [redacted] Management believed that this action met the intention of the recommendation. It also stated it will test a third-party software for [redacted] The target implementation date is July 31, 2026.

OIG Evaluation

We consider management's comments to be responsive to the recommendations and the corrective actions should resolve the current issues identified in the report. However, we plan to continue our oversight of the Postal Service's efforts to address counterfeit postage. With new fraud schemes regularly emerging, it is imperative that the Postal Service continue to implement efforts to proactively identify and mitigate counterfeit fraud.

Appendix A: Additional Information

Scope and Methodology

The scope of this management alert focused on EPA fraud. To accomplish our objective, we:

- Conducted site visits at Postal Service processing plants and retail & delivery units with high volumes of fraud.
- Conducted analysis of [redacted] related to EPA fraud.
- Reviewed Postal Service analyses of volume and revenue loss from EPA fraud.
- Interviewed Postal Service Headquarters officials to gain an understanding of [redacted] and EPA processes and identify the causes of EPA fraud.

This management alert presents issues identified during the Counterfeit Postage Program (Project Number 25-072) audit announced in June 2025. We conducted this management alert from December 2025 through January 2026 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 December 17, 2025, we notified management of our intent to draft this management alert. We discussed our observations and conclusions with management on January 23, 2026, and included their comments where appropriate.

In planning and conducting the audit, we obtained an understanding of the EPA fraud internal control structure to help determine the nature, timing, and extent of our audit procedures. We reviewed the management controls for overseeing the program 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 recommendations, if implemented, should correct the weaknesses we identified.

We assessed the reliability of Postal Service-provided revenue loss and volume 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

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Management Alert – Issues Identified with Counterfeit Postage	To provide immediate notification of issues related to an identified deficiency in the detection of counterfeit [redacted]	25-072-1-R26	October 15, 2025	$485.9 million

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

UNITED STATES POSTAL SERVICE

Date: February 3, 2026

Laura Lozon
Director, Audit Services

SUBJECT: Management Response: Management Alert – Enterprise Payment Account Fraud (25-072-2 Draft)

Thank you for providing the Postal Service with an opportunity to review and comment on the findings and recommendations contained in the draft audit report, Management Alert – Enterprise Payment Account Fraud (25-072-2 Draft)

Finding: Insufficient Controls to Prevent Enterprise Payment Account Fraud

Management Response: Management agrees with this finding.

Following are our comments on each of the five recommendations.

Recommendation 1: We recommend the **Vice President, Sales Intelligence & Support**, in coordination with the **Vice President, Technology Applications,** shut down access to the [redacted] until the associated fraud issues are fully addressed.

Management Response/Action Plan: Management generally agrees with the recommendation**.** USPS agrees that additional security and fraud controls need to be implemented to address the current fraud exploit methods. The following controls have been implemented:

[redacted]

The following additional features are being implemented:

[redacted]

Target Implementation Date: April 30, 2026

Responsible Official: Vice President, Sales Intelligence & Support, in coordination with the **Vice President, Technology Applications.**

Recommendation 2: We recommend the **Vice President, Technology Applications,** implement a requirement that Corporate Treasury concurrence be required on all future software releases involving [redacted] prior to release.

Management Response/Action Plan: Management agrees with this recommendation. Treasury will be added as an approver on the Pricing & Acceptance Tech Services Change Control Board (CCB) for Enterprise Payment System (EPS) and for any [redacted]

Target Implementation Date: April 30, 2026

Responsible Official: Vice President, Technology Applications,

Recommendation 3: We recommend the **Chief Financial Officer and Executive Vice President,** develop a list of minimum standard requirements for [redacted] systems to prevent fraud and require those minimum standards to be met prior to all future software releases involving [redacted]

Management Response/Action Plan: Management agrees with this recommendation. The Postal Service has requirements for the various systems and platforms we use. We will build on this to develop and submit a Business Needs Statement detailing requirements for identifying and mitigating vulnerabilities in [redacted] systems.

Target Implementation Date: April 30, 2026
Responsible Official: Treasurer

Recommendation 4: We recommend the **Vice President, Technology Applications,** implement a requirement to test fraud prevention controls prior to software releases involving [redacted].

Management Response/Action Plan: Management agrees with this recommendation. Enterprise Payment System (EPS) and all "[redacted] systems" currently [redacted] These controls include, but are not limited to, [redacted].

Target Implementation Date: April 30, 2026

Responsible Official: Vice President, Technology Applications

Recommendation 5: We recommend the **Chief Financial Officer and Executive Vice President,** only allow [redacted] to use [redacted] methods.

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

a) The Postal Service is now implementing measures to require new customers to [redacted] to be implemented in February 2026. This action meets the intent of the recommendation to ensure that the customer will have available funds for their purchases.
b) We will also test deployment of software from a third-party vendor to [redacted]

Target Implementation Date: July 31, 2026

Responsible Official: Treasurer

E-SIGNED by LUKE.T GROSSMANN
on 2026-02-03 15:49:10 EST

Luke Grossmann
Chief Financial Officer and EVP

E-SIGNED by SHIBANI.S GAMBHIR
on 2026-02-03 16:18:59 EST

Shabani Gambhir
VP, Sales Intelligence & Support

E-SIGNED by ANGELA.R DYER
on 2026-02-03 16:15:03 EST

Angela Dyer
Senior Director, Commerce Applications

cc: Corporate Audit & Response Management

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

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