# Efforts to Mitigate Counterfeit Postage

## AUDIT REPORT

Report Number 25-072-R26 | September 10, 2026

# Table of Contents

**Cover**
**Highlights** ... 1
Background ... 1
What We Did ... 1
What We Found ... 1
Recommendations and Management's Comments ... 1
**Transmittal Letter** ... 2
**Results** ... 4
Introduction/Objective ... 4
Background ... 4
Findings Summary ... 6
Finding #1: Lack of Comprehensive Oversight and Formal Decision Authority to Address Counterfeit Postage Fraud ... 7
Recommendation #1 ... 9
Postal Service Response ... 9
OIG Evaluation ... 10
Finding #2: Ineffective Controls to Combat Counterfeit Labels Fraud ... 11
Recommendation #2 ... 13
Postal Service Response ... 13
OIG Evaluation ... 14
Recommendation #3 ... 14
Recommendation #4 ... 14
Postal Service Response ... 14
OIG Evaluation ... 15
Recommendation #5 ... 17
Postal Service Response ... 17
OIG Evaluation ... 17
Finding #3: Potential for New Technology ... 18
Recommendation #6 ... 18
Postal Service Response ... 18
OIG Evaluation ... 18
Finding #4: Challenges in Prosecuting Counterfeit Label Cases ... 19
Recommendation #7 ... 20
Recommendation #8 ... 20
Postal Service Response ... 20
OIG Evaluation ... 20
Recommendation #9 ... 23
Postal Service Response ... 23
OIG Evaluation ... 23
Finding #5: Challenges in Addressing Counterfeit Label Sales on Social Media Platforms and eCommerce Websites ... 24
Recommendation #10 ... 25
Recommendation #11 ... 25
Postal Service Response ... 25
OIG Evaluation ... 25
Looking Forward ... 25
**Appendices** ... 26
Appendix A: Additional Information ... 27
Scope and Methodology ... 27
Prior Audit Coverage ... 29
Appendix B: The Counterfeit Label Lifecycle ... 30
Appendix C: Management's Comments ... 31
**Contact Information** ... 40

# Highlights

## Background

The Postal Service primarily finances its operations through postage sales, with package delivery as one of its most important services. In fiscal year (FY) 2025, it shipped 6.8 billion packages, generating $32.6 billion in revenue. However, it lost an additional $1.6 billion in revenue the same year by accepting counterfeit postage labels. To address this growing concern, the Chief Information Security Office and U.S. Postal Inspection Service were tasked with combatting counterfeit labels and pursuing legal action against offenders.

## What We Did

Our objective was to evaluate the Postal Service's and Postal Inspection Service's efforts to address counterfeit postage. We interviewed management and analyzed data related to counterfeit label volumes and revenue losses. We also conducted site visits at 20 processing plants and 27 retail and delivery units to observe mitigation efforts.

## What We Found

The Postal Service and Postal Inspection Service made progress mitigating the use of counterfeit labels, but lacked comprehensive oversight and a formal decision authority to address this issue, and the volume of counterfeit labels remained high. We identified gaps in their ability to detect and intercept counterfeit labels, resulting in an estimated revenue loss of $3.1 billion from March 2024 through February 2026, with the additional risk of losing $520 million in unrecoverable revenue by February 2028. We also identified opportunities for the USPS to collaborate with industry partners to explore the use of new label technology. Additionally, the USPS incurs millions of dollars in re-processing costs for misidentified counterfeit labels, and could recoup some of these costs from late paying mailers. Lastly, while the Postal Inspection Service made efforts to combat counterfeit labels, opportunities exist to improve case referral oversight, funds recovery, case tips analysis, and response to counterfeit labels advertised online.

## Recommendations and Management's Comments

We made 11 recommendations to address the issues identified in the report. Postal Service management agreed with eight recommendations and disagreed with three. Management's comments and our evaluation are at the end of each finding and recommendation. The U.S. Postal Service Office of Inspector General (OIG) considers management's comments responsive to recommendations 1, 2, 3, 4, 5, 6, 10, and 11, as corrective actions should resolve the issues identified. We view management's disagreement with recommendations 7, 8, and 9 as unresolved and will work with management through the formal audit resolution process. See Appendix C for management's comments in their entirety.

# Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 10, 2026

**MEMORANDUM FOR:** KEITH WEIDNER
GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT

GARY BARKSDALE
CHIEF POSTAL INSPECTOR

HEATHER DYER
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

JENNIFER VO
VICE PRESIDENT, RETAIL AND POST OFFICE OPERATIONS

JOHN MORGAN
VICE PRESIDENT, DELIVERY OPERATIONS

ROBERT CINTRON
VICE PRESIDENT, LOGISTICS

ANGELA LAWSON
VICE PRESIDENT, TECHNOLOGY APPLICATIONS

LINDA MALONE
VICE PRESIDENT, APPLIED ENGINEERING

CARA GREENE
VICE PRESIDENT, CONTROLLER

PETER PASTRE
VICE PRESIDENT, GOVERNMENT RELATIONS AND PUBLIC POLICY

JEFFERY ADAMS
VICE PRESIDENT, CORPORATE COMMUNICATIONS

Mary K. Lloyd

**FROM:** Mary Lloyd
Deputy Assistant Inspector General
for Operations, Performance & Service

**SUBJECT:** Audit Report – Efforts to Mitigate Counterfeit Postage
(Report Number 25-072-R26)

# Transmittal Letter

This report presents the results of our audit of the Postal Service's efforts to mitigate counterfeit postage.

All recommendations require U.S. Postal Service Office of Inspector General's (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 any questions or need additional information, please contact Laura Roberts, Director, Network Operations Team 2, or me at 703-248-2100.

Attachment

cc: Postmaster General
Chief Information Officer and Executive Vice President
Chief Retail and Delivery Officer and Executive Vice President
Chief Logistics Officer and Executive Vice President
Chief Technology Officer and Executive Vice President
Chief Financial Officer and Executive Vice President
Corporate Audit Response Management

# Results

## Introduction/Objective

This report presents the results of our self-initiated audit of the Postal Service's efforts to mitigate counterfeit postage (Project Number 25-072). Our objective was to evaluate the U.S. Postal Service's and U.S. Postal Inspection Service's efforts to address counterfeit postage. 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 being one of its most important services. During fiscal year (FY) 2025, the Postal Service shipped 6.8 billion packages, generating $32.6 billion in revenue. However, the U.S. Postal Inspection Service, an investigative agency within the Postal Service, noted that since 2020 there has been a significant increase in the creation, sale, and use of counterfeit postage,[1] including counterfeit package labels. In fact, former Postmaster General Louis DeJoy told Congress in March 2025 that counterfeit postage had become a $1 billion problem and requested assistance from the Department of Government Efficiency to review the Postal Service's efforts to combat counterfeit postage.[2] Consequently, counterfeit labels accounted for a $1.6 billion revenue loss in FY 2025. That same year, the Postal Service reported a $9 billion net operating loss, highlighting the urgent need to reduce the acceptance and processing of counterfeit labels in the Postal Service network. Without strong, dedicated efforts to address this continuous and significant concern, counterfeit labels will continue to exacerbate the Postal Service's severe financial challenges.

Historically, the Postal Inspection Service investigated incidents and made recommendations to the Postal Service concerning counterfeit labels. Postal Service management stated that it became aware of the scale of financial losses resulting from counterfeit labels in the summer of 2022 and transferred responsibility for counterfeit label detection from the Postal Inspection Service to the Chief Information Security Office (CISO) that same year. Subsequently, the CISO launched two primary initiatives: the Counterfeit Postage Intercept Process ("Intercept Process") in FY 2023 and the [redacted] sampling pilot in FY 2025.

During package processing on mail sorting equipment, the Intercept Process [redacted] (see Figure 1).

The Intercept Process was initially designed to target [redacted] labels, and [redacted]

1 Counterfeit postage is any marking or indicia that has been made, printed, or otherwise created — without authorization from the Postal Service — that is printed, applied, or otherwise affixed on an article placed in the mail that indicates or represents that valid postage has been paid to mail the article.
2 As of March 2026, Postal Service management noted that the Department of Government Efficiency had not provided input around combatting counterfeit postage.
3 [redacted]
4 [redacted]
5 [redacted]
6 [redacted]

**Figure 1.** [redacted]

[redacted]

Source: OIG-generated figure, based on the [redacted]

When the Intercept Process identifies a package with a suspected counterfeit label, it is [redacted] At this [redacted] If payment is confirmed, the package is [redacted]

The [redacted] sampling pilot, launched in April 2025, expanded detection efforts to mail processing plant entry points. Sampling packages at the [redacted] helps the Postal Service identify shipments with counterfeit labels and gives the Postal Service a clearer picture of how counterfeit volume varies across entry points.

As the audit progressed, the Postal Service implemented several new mitigation tactics, such as [redacted] The Postal Service also has numerous initiatives in progress, including but not limited to:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Although CISO now leads counterfeit label detection efforts, the Postal Inspection Service highlighted counterfeit label enforcement as a top priority in its FY 2025-2027 strategic plan. The Postal Inspection Service investigates tips from customers and Postal Service employees, issues cease-and-desist orders to mailers, executes search and seizure warrants, works with U.S. Customs and Border Protection at ports of entry, collaborates with other federal agencies, and identifies and shuts down websites selling counterfeit labels.

While this report focuses primarily on counterfeit package labels, we previously issued a report pertaining to counterfeit stamps.[7] For a full picture of the counterfeit label lifecycle, see Appendix B.

## Findings Summary

The Postal Service and Postal Inspection Service faced several challenges in their efforts to address counterfeit postage. Although both organizations took steps to mitigate the issue, their collective efforts were not organized into a formal program with defined decision-making authority. Additionally, existing fraud controls did not fully encompass all forms of counterfeit postage. Despite ongoing efforts, the volume of counterfeit labels moving through the mailstream remained high. We also identified the potential for new technology to enhance mitigation efforts. Further, the Postal Inspection Service faced challenges in getting its counterfeit label cases prosecuted, recovering funds, and preventing the sale of counterfeit labels online. Without additional resources and strategies to combat counterfeit labels, the organization will continue to face challenges in effectively responding to evolving counterfeit fraud trends. We estimate the agency lost $3.1 billion in unrecoverable revenue due to counterfeit labels from March 2024 through February 2026 and project additional losses of $520 million through February 2028. This amounts to a $3.62 billion revenue loss over four years.

> "The agency lost $3.1 billion in unrecoverable revenue due to counterfeit labels from March 2024 through February 2026 and projects additional losses of $520 million through February 2028."

7 *Counterfeit Stamps* (Report Number 25-121-R26, dated June 16, 2026).

# Finding #1: Lack of Comprehensive Oversight and Formal Decision Authority to Address Counterfeit Postage Fraud

The Postal Service did not have a formal, comprehensive, organization-wide program dedicated to detecting, mitigating, and removing counterfeit postage from its network. However, during our audit, management began taking steps to formalize its efforts. Starting in June 2025, the Postal Service assembled contractors to support initiatives aimed at reducing counterfeit postage and referred to this group as the "Fraud Analytics and Mitigation" (FAM) team. After laying this foundation, in November 2025, management decided to hire five full-time Postal Service employees to join the team, adding operational expertise. The hiring is expected to be completed by the end of fiscal year 2026. Alongside the FAM team, CISO regularly brings together cross-functional stakeholders to plan and coordinate mitigation initiatives. However, these meetings function more as informal working groups rather than a structured program. The FAM team oversees and manages the initiatives discussed in these meetings. Although the Postal Service stated these initiatives constitute its program for combating counterfeit postage, it has not provided evidence that this program has been formally approved and funded.

As the Postal Service moves forward in its efforts to mitigate counterfeit postage, opportunities exist to further implement a programmatic framework to how it responds to the issue. Key elements of effective program management are missing from its approach, particularly a formal governance framework, clear decision authority, thorough documentation of key decisions and actions, and a comprehensive scope that covers all types of counterfeit postage (see Table 1).

**Table 1. Program Elements Aligned With Fraud Efforts**

| Element | Description | USPS Efforts |
|---|---|---|
| *Strategic Alignment* | Programs must be aligned with the organization's corporate strategy. | Efforts align with the Postal Service's goal to achieve financial stability and service excellence by protecting revenue. |
| *Program Charter* | The program charter formally authorizes the program, defines its scope, objectives, and success criteria, and assigns the program manager. | Documentation formally authorizing the program by executive leadership or defining its scope and objectives does not exist. |
| *Governance* | Program governance defines roles, responsibilities, decision-making processes, and oversight mechanisms. | Efforts are coordinated cross-functionally without a clear decision-making authority and defined roles and responsibilities. |
| *Stakeholder Engagement* | Effective programs involve active engagement with stakeholders throughout their lifecycle. | Efforts maintain active internal stakeholder involvement. However, there may be opportunities to collaborate with external stakeholders, as noted in Finding 3. |
| *Benefits Management* | Programs identify, plan, deliver, and measure the benefits the program is intended to achieve. | While efforts are tracked and cost benefit analyses on one initiative has been captured, return-on-investment is not being measured. |
| *Documentation* | Programs should maintain agendas, minutes, decision logs, and action-item tracking. | While agendas and some action-item tracking were provided, there are no formal meeting minutes capturing attendees, action-items or decisions. |

Source: Program management elements obtained from the *Project Management Institute*, The Standard for Program Management, Fifth Edition, dated 2024.

The absence of formally defined roles, responsibilities, and decision authority has resulted in ad hoc decisions made across different functions over time. For example, the CISO introduced the counterfeit postage Intercept Process, the [redacted] sampling program, and several other controls. However, these controls were largely reactive in nature, and therefore, the Postal Service has struggled to get ahead of fraud and counterfeit schemes before they happen, resulting in significant revenue losses. Further, there are cases in which internal communication broke down on mitigation efforts. For example, in a previously issued management alert,[8] we noted that warnings of potential payment fraud vulnerabilities came to light during internal meetings as early as January 2025, yet these vulnerabilities were not acted upon until they were eventually exploited by fraudsters later that year. This resulted in over $600 million lost as of February 2026. These examples highlight the importance of designating a clear decision authority to direct, approve and be accountable for efforts to mitigate counterfeit postage.

> “The Postal Service has yet to formally establish a program charter with clear lines of authority or a process to document key decisions for actions that carry operational or financial impacts.”

Although the CISO currently serves as the lead for mitigation efforts and acts as the de facto decision authority, the Postal Service has yet to formally establish a program charter with clear lines of authority or a process to document key decisions for actions that carry operational or financial impacts. For example, management provided topics discussed during the cross-functional meetings but could not provide official meeting minutes or documentation around the decisions made during these discussions. In July 2026, the Postal Service provided presentation slides used to monitor ongoing fraud-mitigation activities, tracks milestones, and identify stakeholders. Management indicated that this presentation is updated regularly and used to coordinate with stakeholders. Further, the Postal Service tracks certain performance measures, such as the number of fraudulent accounts deactivated, but it does not track the return-on-investment resulting from these actions.

By operating informally to address counterfeit postage, the Postal Service faces several organizational risks, such as:

- **Revenue Loss & Legal Exposure:** Counterfeit postage directly impacts revenue protection and potential criminal prosecution. Undocumented decision-making makes it difficult to defend operational changes or produce evidence in legal proceedings.
- **Resource Misallocation:** Without formal benefits management and tracking, Postal Service leadership cannot accurately measure the return on investment for efforts to reduce counterfeit postage. This makes it difficult to determine if resources are being used efficiently and effectively.
- **Single-Point-of-Failure & Continuity Risk:** All important know-how and information about the program is kept only in the minds of those attending the meetings. If key members leave, the Postal Service could lose valuable operational knowledge, impacting its ability to continue the program smoothly.

Creating a formalized program and structure is consistent with logistics industry best practices. Other logistics organizations have established teams dedicated to mitigating fraud within their organizations, leaning on diverse skillsets across different groups. However, it is unclear whether the CISO is the appropriate office to serve as the lead decision-maker. Although the CISO is positioned to

8 *Management Alert: Enterprise Payment Account Fraud* (Report Number 25-072-2-R26, dated February 10, 2026).

respond to cyber-related risks, many counterfeit postage decisions require an understanding of business operations, revenue protection, mail processing, and customer impact. These responsibilities fall outside traditional cybersecurity functions. Assigning responsibilities is ultimately a management decision. However, organizations comparable to the Postal Service, which also must deter fraud in their operations, take different approaches to mitigate these risks in their operations. According to officials at other organizations, these approaches include establishing cross-functional teams or assigning teams in security, legal, or other operational functions with primary responsibility for addressing counterfeit and fraud issues. As such, a more suitable decision authority may reside within revenue assurance or processing operations, where leaders have the perspective needed to weigh financial, operational, and service risks in real time.

Program management best practices also suggest that programs should have appropriate governance, including transparency, responsibility, and accountability. Programs should include a holistic and systematic approach, which in this case, should include all aspects of counterfeit postage and related fraud.[9] The Postal Service's approach is focused on counterfeit labels and does not include all types of counterfeit postage. For example, a previous OIG audit found that the Postal Service lacked a comprehensive strategy for mitigating counterfeit stamps,[10] and the current list of initiatives is solely focused on addressing counterfeit labels. Managing this through a coordinated and wholistic program would be prudent.

Until the Postal Service fully establishes the key elements of a program, its counterfeit postage efforts risk being fragmented, reactive, and ultimately unaccountable. Establishing a formal decision structure with defined roles, responsibilities, and documentation requirements would enhance program accountability and enable the organization to proactively prioritize and mitigate emerging counterfeit postage schemes.

### Recommendation #1

We recommend the **Vice President, Chief Information Security Officer**, establish key programmatics across counterfeit postage efforts, upon final approval, to include:

a. a documented program charter signed by an executive sponsor,

b. a defined program scope that includes coverage of all types of counterfeit postage,

c. clearly defined roles and responsibilities, including voting rights, approval gates, and signatory authority, and

d. documentation of key decisions and approvals.

### Postal Service Response

Management agreed with finding 1 and recommendation 1. Management stated that while official documentation may not have been sent out to the entire organization when the fraud program was established, the other components of the finding have been addressed.

Regarding recommendation 1, management stated that it submitted an organization chart and mission statement, asserting that it included clearly defined roles and responsibilities and that the mission statement covers all types of counterfeit postage. While management acknowledged a formalized project charter documenting that key decisions and approvals may be a useful tool, it asserts that the formal approach to programmatics is administrative red tape and the nature of fraud necessitates quick action that balances risks and benefits. Lastly, management acknowledged that it did not formally obtain signatures from all stakeholders on the documentation referenced in this recommendation. Because management believed it had met the intent of the recommendation, it did not provide a target

9 Project Management Institute, *The Standard for Program Management*, Fifth Edition, section 1.2, dated 2024.
10 *Counterfeit Stamps* (Report Number 25-121-R26, dated June 16, 2026).

implementation date in its official management comments. However, after further discussion, management agreed to take additional action with a target implementation date of March 31, 2027.

### OIG Evaluation

We consider management's comments partially responsive to recommendation 1. Our recommendation aims to align the Postal Service's counterfeit postage efforts with basic program management standards to enable accountability within the program.

While management provided a mission statement, written program goal, organizational chart, and a listing of the individual Postal Service teams with responsibilities related to counterfeit postage, there remains no documented program charter signed by an executive sponsor. Creating a charter gives any initiative a clear foundation by defining its purpose, authority, and structure. This helps teams move forward efficiently, without confusion or unnecessary rework. Instead of creating an administrative burden, a charter helps everyone share the same understanding of what the program is trying to achieve. It also promotes accountability, speeds up onboarding for new team members, and maintains consistency when there are changes in stakeholders. Further, the roles and responsibilities provided did not clearly define which team or teams have ultimate authority over decisions related to counterfeit postage efforts. Establishing formal voting rights, approval gates, and signatory authority establishes accountability for decisions made. We will continue discussions with management and verify appropriate action before this recommendation is closed.

# Finding #2: Ineffective Controls to Combat Counterfeit Labels Fraud

To address counterfeit postage, the Postal Service introduced tactical measures such as the Intercept Process and the [redacted] sampling pilot program, which did not fully resolve the problem. Specifically, from October 2023 to December 2025, counterfeit label volume increased significantly. However, the volume of counterfeit labels has declined since December 2025, likely due to controls the Postal Service has put in place since that time. Measures included enhancing the Postal Service's [redacted] and involving relevant stakeholders in those changes. Further, the Postal Service began implementing new preventative controls at [redacted]

Despite these efforts, which have reduced the number of counterfeit labels, packages with both existing and emerging types of counterfeit labels continue to make it to their final delivery point. We identified vulnerabilities that are not yet addressed by the Intercept Process and insufficient controls at mail entry points to prevent [redacted] of packages with counterfeit labels; thus, further controls are needed to strengthen revenue protection.

Additionally, the measures introduced have, in some cases, impacted non-counterfeit volume. For example, the Intercept Process inadvertently intercepted approximately 2 million packages with paid labels from December 2024 through February 2026, impacting paying customers and the Postal Service brand.

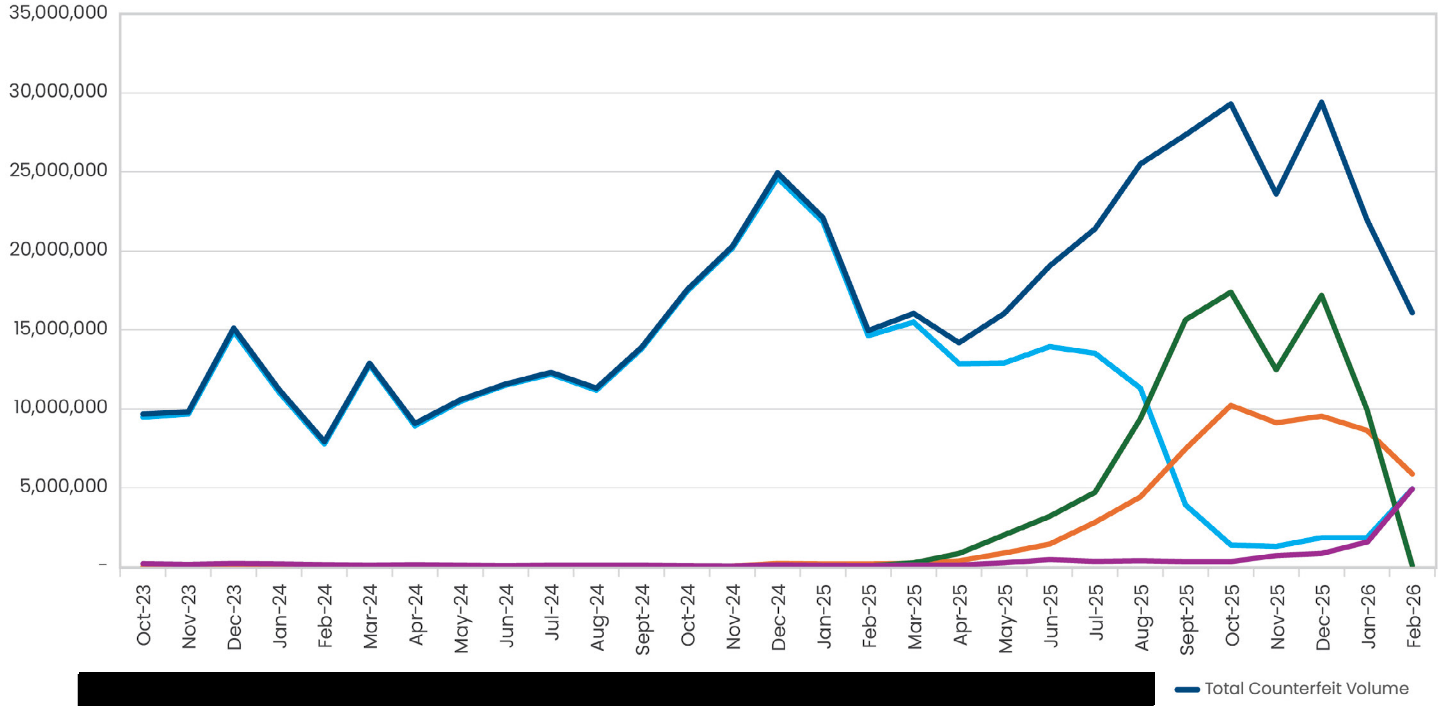
### Insufficient Intercept Controls

The number of packages with counterfeit labels increased from 9.7 million in October 2023 to a peak of 29.4 million in December 2025 (over 200 percent) as shown in Figure 2. Initially, most counterfeit labels were counterfeit [redacted], so management focused interception efforts on these. With their focus on counterfeit [redacted] it did not proactively address other vulnerabilities in the Intercept Process. Thus, starting around February 2025, counterfeiters began to exploit unaddressed vulnerabilities. This includes three emerging counterfeit label schemes to which we alerted management.[11] The first two of these schemes could easily be generated without accessing a Postal Service system. The three methods, which represented most counterfeit labels in the mailstream as of December 2025, are:

1. **Counterfeit [redacted].** These bypass the Intercept Process because the [redacted] which is supposed to only be used on legitimate [redacted].
2. **Counterfeit [redacted].** These bypass the Intercept Process because the [redacted] and the Intercept Process [redacted]
3. **Enterprise Payment Account (EPA) fraud [redacted].** These [redacted] are from the [redacted] but the mailers did not pay for these [redacted] as required because the [redacted] lacked effective controls.

11 See *Management Alert – Issues Identified With Counterfeit Postage* (Report Number 25-072-1-R26, dated October 15, 2025); *Management Alert: Enterprise Payment Account Fraud* (Report Number 25-072-2-R26, dated February 10, 2026); *Management Alert: Emerging Counterfeit Label Trend* (Report Number 25-072-3-R26, dated April 8, 2026).

## Figure 2. Volume of Known Counterfeit Label Methods




Source: OIG analysis of Product Tracking and Reporting System data and EPA fraud revenue loss data provided by Postal Service management.

Note: The data may not include all counterfeit labels, as there may be types of counterfeit labels of which we are unaware.

The Postal Service was aware of the EPA fraud issue in 2025. Following our management alert, the Postal Service implemented controls to address the fraud, leading to a decline in overall counterfeit label volume from January 2026 to February 2026. However, the volume of counterfeit labels could increase in the future due to unaddressed deficiencies in the Intercept Process, such as:

- [redacted]
- [redacted]
- [redacted]

Government Accountability Office guidance states that internal control systems, like the Intercept Process, should provide reasonable assurance that an organization will achieve its objectives.[13] In this case, the Postal Service does not have reasonable assurance that its Intercept Process validates that mail is prepaid at the time of mailing.[14]

The Postal Service did not proactively keep up with evolving counterfeit label schemes because management did not fully recognize the extent of the issue. For example, in response to an OIG management alert in October 2025,[15] a management official wrote, "Overall fraud has declined since 2023, and this trend will continue as we continue

12 [redacted]
13 U.S. Government Accountability Office *Standards for Internal Control in the Federal Government* (Report Number GAO-25-107721, dated May 15, 2025).
14 U.S. Postal Service *Domestic Mail Manual*, Section 604.6.1.
15 *Management Alert – Issues Identified with Counterfeit Postage* (Report Number 25-072-1-R26, dated October 15, 2025).

to roll out our mitigation plans." However, this assessment conflicted with OIG analysis, which showed that counterfeit label volume rose significantly from 2023 until December 2025, as shown above in Figure 2.

Additionally, as of September 2025, the Postal Service's internal method for tracking counterfeit labels primarily focused on [redacted] which the Intercept Program was originally established to detect. This tracking was shown in a weekly report, which management stated it used to provide an estimate of overall counterfeit label volume to internal stakeholders. However, management did not update reports as new schemes emerged.[16] As a result, internal stakeholders may have been led to believe that counterfeit label problems were being addressed, when in fact, total counterfeit activity continued to rise.

The ability to effectively mitigate counterfeit labels remains at risk without additional controls and proactive analysis to identify future trends, as counterfeiters keep adapting their methods. While the Postal Service stated it was aware of these loopholes, it had not implemented timely updates to the [redacted] to address them. As a result, package tracking data showed that 97 percent of counterfeit labels were processed for delivery from October 2023 through February 2026, demonstrating the limited effectiveness of implemented controls.

To better identify new fraud methods and improve interception, in March 2026 the Postal Service began updating their fraud dashboards to track shifts and trends in fraud patterns. These dashboards track probable and potential fraud trends, enables analysts to follow the fraud by [redacted] This information is reported regularly to the executive leadership team. Therefore, we will not be making a recommendation on this issue.

> "We estimate the agency lost $3.1 billion in unrecoverable revenue due to counterfeit labels from March 2024 through February 2026."

Although we recognize the Postal Service has made efforts and progress toward reducing counterfeit label volumes, we estimate the agency lost $3.1 billion in unrecoverable revenue due to counterfeit labels from March 2024 through February 2026, and we estimate it is at risk of an additional unrecoverable revenue loss of $520 million through February 2028. This amounts to a $3.6 billion loss over four years.[17]

### Recommendation #2

We recommend the **Vice President, Chief Information Security Officer**, conduct a review to identify known vulnerabilities not yet addressed by mitigation efforts and develop a plan, with dedicated milestones, to address these vulnerabilities.

### Postal Service Response

Management agreed with finding 2, the monetary impact, and recommendation 2.

In response to recommendation 2, management acknowledged that ongoing evaluations are necessary to identify vulnerabilities that have not yet been addressed. Management stated that when new vectors are discovered, a plan with dedicated milestones is developed to address the vulnerabilities. Additionally, management provided expected completion dates to address current known vectors:

- [redacted]

16 For example, management identified the counterfeit [redacted] scheme in April 2025 and the EPA fraud [redacted] scheme in May 2025. However, as of September 2025, weekly reports did not reflect these schemes.

17 For the purposes of monetary impact, we are claiming only $1.2 billion of the $3.6 billion as unrecoverable revenue loss in relation to this finding and recommendation 1 because we subtracted amounts claimed in previous reports regarding counterfeit labels. See the "Prior Audit Coverage" section in Appendix A for the previously claimed monetary impact amounts.

- [redacted]
- [redacted]

The target implementation date is August 31, 2027.

**OIG Evaluation**

The OIG considers management's comments responsive to recommendation 2, as corrective action should resolve the issues identified in the report.

### Paid Packages Mistakenly Intercepted

We also found that Postal Service employees and the Intercept Process mistakenly routed paid packages to the [redacted] From December 2024 to February 2026, approximately 2 million packages were misrouted because of processing or mail entry errors, resulting in unnecessary customer impacts and operational inefficiencies. In an April 2026 analysis,[18] management determined that roughly half of the errors were manual and technical processing errors by Postal Service employees or technology. The other half were mail entry errors by customers who did not timely transmit payment records to the Postal Service.[19] Policy requires payment records to be submitted timely and prior to mail entry.[20]

Postal Service management stated it is working internally to resolve the manual and technical errors while also working collaboratively with customers to resolve payment file transmission issues.

The Postal Service incurred unnecessary costs to transport these paid packages for re-processing at the [redacted] where they were ultimately re-entered into the mailstream and delivered. We estimate these costs total $7.2 million from December 2024 through February 2026. If errors persist, we forecast the Postal Service will incur an additional $11.9 million in unnecessary re-processing costs from March 2026 through May 2027.

We found an opportunity for the Postal Service to recover costs related to retrieval fees paid to the [redacted]. In certain cases, mailers who failed to submit payment files on time asked the Postal Service to retrieve their packages, which resulted in the Postal Service paying a fee to the [redacted] for each retrieval. Currently, mailers are not charged for these retrievals. The Postal Service incurred more than $548,000 in retrieval costs from April 2025 through April 2026. In April 2026 alone, the Postal Service paid $51,700 in retrieval fees, and 52 percent of these fees ($26,884) were directly due to mailers' late payment submissions. While these costs are minimal, management stated it is coordinating with the Postal Service Law Department to explore the possibility of recouping these funds from mailers, which could set a positive precedent for mailers to submit payment records timely and prior to mail entry.

**Recommendation #3**

We recommend the **Vice President, Chief Information Security Officer**, establish an acceptable threshold for mistaken intercepts and resolve the manual and technical errors until the threshold is met.

**Recommendation #4**

We recommend the **Vice President, Chief Information Security Officer**, in coordination with the **General Counsel and Executive Vice President**, determine a strategy and mechanism for recouping retrieval costs from mailers who did not timely transmit payment records.

**Postal Service Response**

Management agreed with recommendations 3 and 4.

18 Management conducted an analysis limited to April 2026 volume.
19 Management determined that in April 2026 47 percent of mistakenly routed volume was due to an employee or technical error. 52 percent was due to mail entry errors by customers.
20 U.S. Postal Service Publication 199, *Intelligent Mail Package Barcode (IMpb) Implementation Guide for Confirmation Services and Electronic Payment Systems*, section 3.1, dated February 7, 2025.

In response to recommendation 3, management stated that the CISO monitors the frequency and root causes of all false positives and works to reduce disruption to good mail volume. Additionally, the CISO FAM team rolled out the [redacted] nationwide. Further, the CISO FAM, Chief Technology Officer and Engineering teams continue to collaborate so that they can take action on machines that are having issues. CISO provided an internal target of reducing the rate of false positives to [redacted] percent of properly redirected package volume. The target implementation date is August 31, 2027.

In response to recommendation 4, management agreed to seek opportunities to recoup retrieval costs. It stated its efforts will require communication and teamwork with multiple parties across the organization. CISO is working with Strategic Sales to ensure payments are made on time. Additionally, management stated that shippers who persistently submit late payments and fail to correct their behavior will be required to sign the Do Not Intercept agreement. By doing so, they will assume full responsibility for all package volume associated with their Mailer IDs, regardless of whether payment has been made. The target implementation date is August 31, 2027.

### OIG Evaluation

The OIG considers management's comments responsive to recommendations 3 and 4, as corrective actions should resolve the issues identified in the report.

## Insufficient Mail Entry Point [redacted] Controls

In addition to the unaddressed vulnerabilities in the Intercept Process, the Postal Service has not established sufficient controls at entry points — including retail and delivery units, and mail processing facilities — to check that labels were prepaid according to policy.[21] As of December 2025, the Postal Service estimated that [redacted] percent of packages with counterfeit labels were [redacted] at mail processing facilities,[22] while [redacted] percent were [redacted] at retail and delivery units[23] for processing and delivery. Entry points lacked adequate [redacted] controls because the Postal Service initially focused on the Intercept Process as its main mitigating control.

Postal Service management stated that counterfeit labels enter mail processing facilities [redacted] We observed suspected counterfeit labels at mail processing facilities (see Figure 3) and also observed suspected counterfeit labels [redacted] retail and delivery units at all points of entry visited during the audit. This included at the [redacted], as shown in Figure 4.

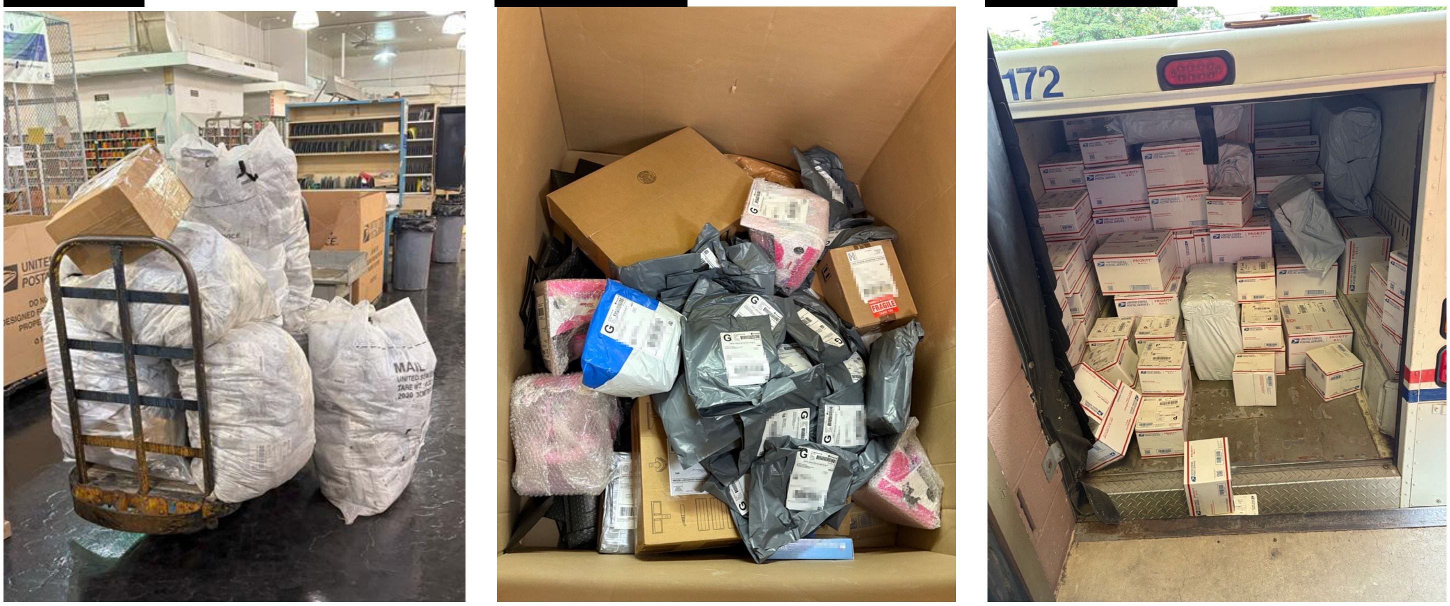
**Figure 3. Packages With Suspected Counterfeit Labels Observed in a Mail Processing Facility**

Source: OIG photograph taken at the [redacted] on August 27, 2025.

21 U.S. Postal Service *Domestic Mail Manual*, Section 604.6.1.
22 This includes [redacted] percent at mail processing facility [redacted] and [redacted] percent [redacted].
23 Percentages are rounded.

**Figure 4. Examples of Packages With Suspected Counterfeit Labels [redacted] via Retail and Delivery Units**

[redacted]




[redacted]

Source: OIG photographs and observations.

Postal Service employees had no tools to [redacted] during our observations at 27 retail and delivery units, and Postal Service management at 10 of the units (or 37 percent) said it was unaware of the counterfeit labels [redacted] through the facility. At the time of our site visits, headquarters management instructed retail and delivery unit employees [redacted] because the Intercept Process [redacted].

> “Employees had access to scanners that could scan for [redacted], but employees were not always aware of this functionality.”

During observations at 20 mail processing facilities, we further noted that dock employees had access to scanners that could scan for [redacted] but employees were not always aware of this functionality, and they did not always use it. Further, Postal Service management noted that drivers either did not have scanning equipment, or their equipment did not have the capability to scan and [redacted]

The Postal Service started implementing new preventative controls in January 2026 and issued guidance to retail units on how to identify and handle [redacted]. In February 2026, management [redacted] and other devices to give retail and delivery unit employees the ability to scan for [redacted]. Management also stated it may [redacted]

[redacted] In May 2026, management stated that it implemented or planned to implement several additional efforts, [redacted]

Without the ability to [redacted] at entry points, the Postal Service is unable to stop it at its source and may incur unnecessary transportation and delivery costs. By implementing controls at all entry points, the Postal Service could better prevent the [redacted] of packages with counterfeit labels and reduce future revenue loss.

### Recommendation #5

We recommend the **Vice President, Chief Information Security Officer**, in coordination with the **Vice President, Retail and Post Office Operations**, the **Vice President, Delivery Operations**, and the **Vice President, Logistics**, establish [redacted] on all package points of entry.

### Postal Service Response

Management agreed with recommendation 5.

In response to recommendation 5, management stated that CISO and other key teams are collaborating to strengthen security and control over package entry points. Their ongoing efforts include [redacted] The target implementation date is August 31, 2027.

### OIG Evaluation

The OIG considers management's comments responsive to recommendation 5, as corrective action should resolve the issues identified in the report.

# Finding #3: Potential for New Technology

To improve label security and reduce the risk of counterfeiting, there is opportunity for the Postal Service to collaborate with the broader mailing industry on potential technological solutions. We spoke with various companies that sell package labels on behalf of the Postal Service, and many expressed interest in working with the Postal Service on solutions, such as new label technology.

Other logistics companies have introduced new technology into their labels, including (1) specialized barcodes and (2) radio frequency identification (RFID) technology. Specialized barcodes [redacted] and can store more information on the label than the Postal Service's current barcode, providing more data points for the Intercept Process to check. The same is true for RFID-embedded labels, both of which could be additional layers of security against counterfeit. Further, companies that provide shipping labels on behalf of the Postal Service advocated advanced barcodes. One label provider questioned why the Postal Service, which at one point required a more advanced barcode on labels, had removed that requirement.

The Postal Service itself has considered its own long-term technological approach to hardening its label technology but has not yet fully considered industry alternatives, such as specialized barcodes. However, with its exploration in specialized barcodes, Postal Service management stated its processing equipment had difficulty reading barcode information, and that package processing speeds would be reduced as a result. Currently, the Postal Service allows legitimate labels to be created through various means. For example, customers can obtain labels directly from Postal Service systems or through a third-party label provider, which transmits information about the labels to the Postal Service.

Having many ways to obtain labels legitimately has made it impossible to implement a one-size-fits-all counterfeit response. Further, the methodology for constructing Postal Service [redacted] Using these [redacted] Therefore, to reduce the risk of counterfeit labels, management stated it plans to [redacted]

During our review, we did not identify one piece of technology that would be a clear catch-all solution to counterfeit labels. We encourage the Postal Service to work collaboratively with its industry partners on potential technological solutions as doing so may enable the Postal Service to strengthen its counterfeit mitigation capabilities.

### Recommendation #6

We recommend the **Vice President, Chief Information Security Officer**, in coordination with the **Vice President, Applied Engineering**, and the **Vice President, Technology Applications** collaborate with industry partners to establish a strategy on potential technological solutions for mitigating counterfeit postage.

### Postal Service Response

Management agreed with finding 3 and recommendation 6.

In response to recommendation 6, management stated that the Postal Service is working with industry partners through various groups, including regular meetings and advisory committees, to address fraud. They are evaluating solutions based on cost, effort, and benefit before implementation. The target implementation date is August 31, 2027.

### OIG Evaluation

The OIG considers management's comments responsive to recommendations 6, as corrective action should resolve the issues identified in the report.

# Finding #4: Challenges in Prosecuting Counterfeit Label Cases

The Postal Inspection Service has also taken steps to address counterfeit labels, making it a top mission priority in its strategic plan and collaborating with partners to combat the issue. Despite these actions, the Postal Inspection Service faces challenges in referring cases to the Department of Justice (DOJ) for prosecution, in recovering funds from related cases, and in managing counterfeit label tips and referrals. We identified opportunities where progress can be made, such as enhancing oversight of referrals, considering other methods to recover lost revenue and secure prosecution of offenders, and improving analysis of tips and referrals related to counterfeit labels.

## Criminal and Administrative Action Available to the Postal Inspection Service

We found that the Postal Inspection Service faced difficulty securing criminal action against counterfeiters. Between March 2020 and March 2025, only nine of 44 cases presented to the DOJ were accepted for prosecution,[24] but all nine resulted in successful convictions. Management noted that the DOJ may not consider a case for reasons outside its control. For example, a particular DOJ office may have minimum thresholds for revenue loss or may prioritize other cases. Enhanced oversight and exploration of nontraditional legal pathways for prosecution could improve case acceptance and outcomes from cases if not accepted.

Regarding oversight, we found opportunities to enhance the Postal Inspection Service's Case Management System to track which cases are referred to the DOJ and document reasons for acceptance or rejection. Currently, Inspectors can enter this information in a free-form text field with other case-related information. However, the information in this field cannot be queried or analyzed, and it is not a required entry. A best practice in federal law enforcement is to use data to inform decision making.[25] Standardizing this information in a structured data field could allow the Postal Inspection Service to identify strategies to strengthen future cases and increase DOJ acceptance.

There is also an opportunity to explore legal pathways that do not require DOJ involvement. We identified two potential paths the Postal Inspection Service could use to attempt to recoup funds from counterfeit label cases and/or secure prosecution of offenders:

1. **Coordinate with the Postal Service to utilize the Revenue Deficiency Process,** an administrative action in which the Postal Service issues a notice for unpaid revenue.[26] The Domestic Mail Manual, backed by federal regulation, allows the Postal Service to issue a written notice or bill to recover revenue from mailers responsible for deficiencies due to fraud, misrepresentation, or misuse of postage systems.[27] If payment is not received within 30 days, barring appeal, debt collection procedures may begin. Postal Service officials noted that, historically, this process applied to mailers who shortpaid postage, not those using counterfeit labels. However, due to significant revenue loss from counterfeit labels, the Postal Inspection Service and Postal Service should consider utilizing this option.
2. **Taking cases to state and local prosecutors for prosecution.** Although there are no mandates to pursue state or local prosecution, these options can serve as alternatives when federal prosecutors decline a case. To date, Postal Inspection Service management stated that it has not taken counterfeit label cases to state and local prosecutors because it views counterfeit label cases as federal cases and believe these cases would face similar barriers

24 The Postal Inspection Service must present evidence to the DOJ, which must agree to accept the case and move forward with prosecution.
25 U.S. Department of Justice, *Law Enforcement Best Practices: Lessons Learned from the Field,* published 2019, accessed at https://portal.cops.usdoj.gov/ResourceCenter/content.ashx/cops-w0875-pub.pdf.
26 This must occur in conjunction with the Postal Service.
27 U.S. Postal Service *Domestic Mail Manual*, Section 607.3.

at the state and local levels. However, state criminal statutes — such as forgery, theft, and other related offenses — cover illegal conduct similar to federal offenses traditionally pursued by the Postal Inspection Service for counterfeit label cases.[28] We recognize there are challenges with state or local prosecution not faced at the federal level, as criminal statutes vary significantly in terms of severity and penalties; nonetheless, seeking prosecution at the state and local levels for counterfeit label cases is yet untapped by the Postal Inspection Service.

Pursuing administrative remedies or criminal charges may be worthwhile when the potential recovery of losses through court-ordered restitution to the Postal Service outweighs the cost of investigation, or when there are no other legal pathways.

### Recommendation #7

We recommend the **Chief Postal Inspector** enhance the Case Management System with a data field to enter whether a case was accepted by the Department of Justice for prosecution, track the trends of acceptance, and pursue further discussion with the Department of Justice where the trends show lack of acceptance.

### Recommendation #8

We recommend the **Chief Postal Inspector** in collaboration with the **General Counsel and Executive Vice President** and the **Vice President, Controller**, explore alternate options for legal action against counterfeit label operations, including utilizing the Revenue Deficiency Process and state and local prosecution.

### Postal Service Response

Management disagreed with finding 4 and recommendations 7 and 8.

Regarding the finding, management stated that while it agreed there are challenges to obtaining counterfeit label case prosecution, overall the Postal Inspection Service has a method to track prosecutive efforts, and postal inspectors have used state and local prosecution methods when federal prosecution is not feasible.

Regarding recommendation 7, management stated that the Case Management System can already track cases presented to the U.S. Attorney's Office but would be unable to capture the reason cases are accepted or declined because that information is not provided.

Regarding recommendation 8, management referred to a separate titled *Counterfeit Stamps*, which recommended management consider other avenues for disabling online counterfeit stamp threats. It agreed with the previous audit's recommendation, and will continue to use several avenues to disable online counterfeit stamp threats. Management further stated the prior recommendation was closed with report issuance and asked the same consideration for recommendation 8, as it continuously explores options for legal action and seeks state and local prosecution in postage fraud cases.

### OIG Evaluation

We consider management's comments unresponsive to recommendations 7 and 8, and will pursue the disagreements through the audit resolution process.

Regarding recommendation 7, we noted in our finding that while postal inspectors can enter acceptance or declination in a free-form text field within the Case Management System, this field is not required and cannot be queried. Therefore, we believe standardizing this information as a structured and required data field can better inform strategies on future cases and improve acceptance of cases for prosecution. Further, the OIG maintains that coordination with the U.S. Attorney's Office would be prudent to obtain and track feedback on declined cases to strengthen future cases presented.

28 We focused this review on the following states: California, New York, New Jersey, Illinois, Texas, and Michigan.

Regarding recommendation 8, we recognize a previous OIG report recommended considering avenues to disable online counterfeit stamp threats, such as the Lanham Act. However, this recommendation offers additional avenues, such as the Revenue Deficiency Process, which may be specifically leveraged for counterfeit labels. The OIG believes this is an alternate option for legal action in counterfeit label cases that management should consider. Further, management's claims that the Postal Inspection Service has used state and local prosecution methods contradicts an interview during the audit in which management stated that it has not taken counterfeit label cases to state and local prosecutors because it views these cases as federal matters.

### Inability to Recover Funds

We found the Postal Inspection Service was unable to recover most of the losses associated with counterfeit labels identified through investigations.[29] Specifically, between March 2020 and March 2025, the Postal Inspection Service identified $57 million in losses related to counterfeit labels cases but recovered only $572,250 (about 1 percent).

Postal Inspection Service management said that it recovered such a small amount of funds because there is a four-to-five-month delay between obtaining the subpoena and subsequently obtaining the search and seizure warrants necessary to recover funds. First, the Postal Inspection Service needs a subpoena to gather evidence to obtain a search warrant, which allows them to obtain the suspect's bank statements from their bank. At the issuance of the subpoena, some banks may notify the suspect of the inquiry. Next, the Postal Inspection Service uses the information obtained to identify the amount of funds available for seizure. Lastly, the Postal Inspection Service needs a seizure warrant to seize the funds in the bank account.

In the time between the execution of the search warrant and the seizure warrant, funds are not frozen, and suspects may withdraw the funds. The delay can be caused by various factors, such as the bank's processing time, the identification of additional accounts that require separate subpoenas, additional investigative steps, time needed to secure seizure warrants from a court, or other factors. Once a court finally issues the seizure warrant, the suspect may have already withdrawn the remaining funds.

According to Postal Inspection Service management, in limited circumstances, the search and the seizure warrant can be issued simultaneously. However, under these circumstances, the Postal Inspection Service would have to be able to identify the specific bank accounts and funds to be seized without an initial search warrant, which in most cases is difficult.

Therefore, there are no clear options available to improve funds recovery, as the process is largely outside the control of the Postal Inspection Service. As such, we will not make a recommendation on this issue but encourage the Postal Inspection Service to look for opportunities, when possible and appropriate, to improve its ability to recover funds.

### Insufficient Tracking of Counterfeit Label Tips and Referrals

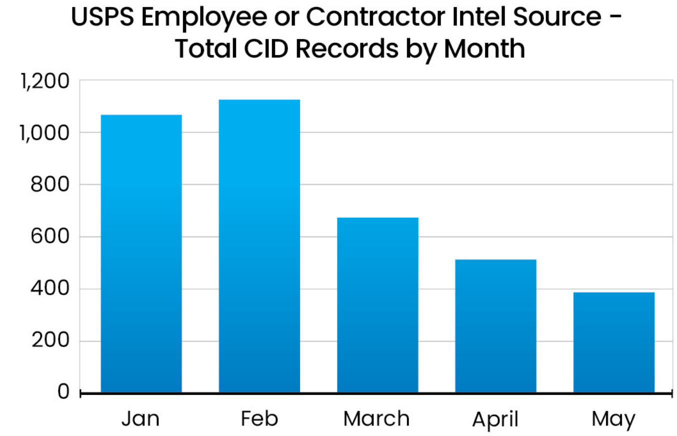
The Postal Inspection Service does not employ a comprehensive method for managing tips and referrals related to counterfeit labels. Prior to September 2025, the Postal Inspection Service processed tips and referrals by email. In September 2025, the agency enhanced its procedures by introducing the Counterfeit Postage Reporting System ("reporting system"), which tracks submissions from both external and internal sources. The reporting system automatically generates daily spreadsheets and weekly reports, delivered to revenue fraud analysts according to the ZIP Code associated with each tip or referral.

29 39 CFR § 233.1 authorizes the Postal Inspection Service to make seizures of property as provided by law.

Law enforcement best practices suggest that agencies should use data to inform decision-making, including identifying hotspots and predicting patterns.[30] Management stated they review the total number of complaints received monthly from internal employees and contractors (see Figure 5), and they generate a report of the total number of complaints by month and postage type (Figure 6).

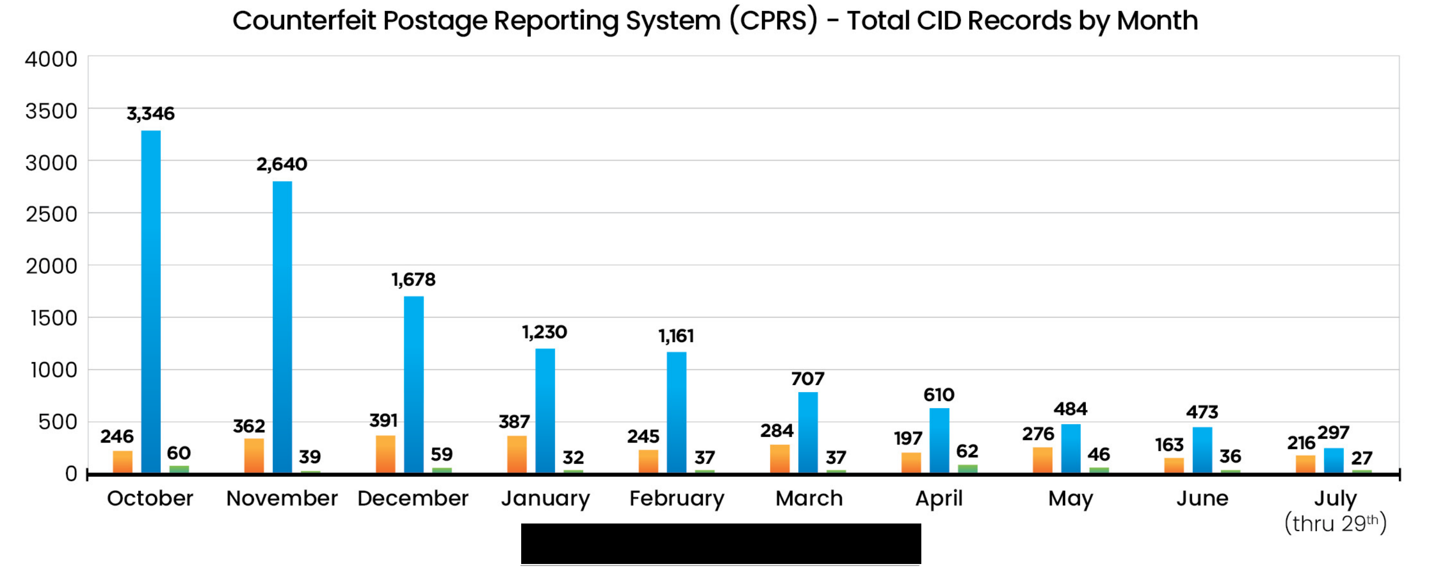
However, these reports only summarize overall tips volume and do not provide meaningful insights which align with best practices. For example, the Inspection Service could enhance reporting to show geographic areas where the most tips surface or identify patterns in fraud vectors reported. Conducting continuous trend analysis could provide Inspectors with valuable insights for initiating investigations.

### Figure 5. Postal Inspection Service Analysis of Internal CPRS Tips and Referrals by Month




Source: Provided by Postal Inspection Service management by email on August 3, 2026.

### Figure 6. Postal Inspection Service Analysis of Total CPRS Tips and Referrals by Month and Postage Type




Source: Provided by Postal Inspection Service management by email on August 3, 2026.

30 U.S. Department of Justice, *Law Enforcement Best Practices: Lessons Learned from the Field*, published 2019, accessed at https://portal.cops.usdoj.gov/ResourceCenter/content.ashx/cops-w0875-pub.pdf.

**Recommendation #9**

We recommend the **Chief Postal Inspector** perform a continuous trend analysis on counterfeit postage tips and referrals, including identification of geographic hotspots and patterns in fraud vectors reported.

**Postal Service Response**

Management disagreed with recommendation 9.

Regarding recommendation 9, management stated that it submitted documentation that showed trend analysis performed on Counterfeit Postage Reporting System data and, as such, viewed the recommendation unnecessary.

**OIG Evaluation**

We consider management's comments unresponsive to recommendation 9 and will pursue the disagreement through the audit resolution process.

Regarding recommendation 9, we recognize that management provided two figures showing limited analysis of Counterfeit Postage Reporting System data: (1) the total number of complaints received monthly from internal employees and contractors; and (2) the total number of complaints by month and postage type. However, we noted that these figures summarize only overall tip volume and do not provide meaningful insights, such as identification of geographic hotspots and fraud vector patterns.

# Finding #5: Challenges in Addressing Counterfeit Label Sales on Social Media Platforms and eCommerce Websites

The Postal Inspection Service encountered difficulties in removing advertisements and sales of counterfeit labels from social media platforms and eCommerce websites. These labels are widely accessible on these sites and often promoted at low prices, as illustrated in Figure 7 and Figure 8. Despite ongoing challenges, the Postal Inspection Service has managed to successfully shut down some websites dedicated to selling counterfeit labels.

In its FY 2025–2027 strategic plan, the Postal Inspection Service set goals to collaborate with eCommerce marketplaces to identify root causes of counterfeit postage and to introduce counterfeit postage messaging and warnings on customer sites. However, the plan did not establish comparable goals for social media companies, despite their platforms being a significant source of counterfeit label sales.

While the Postal Inspection Service has had some success in addressing the sale of counterfeit labels through eCommerce websites, it encounters difficulties in getting social media companies to remove counterfeit label listings. The law provides broad immunity to social media companies from what users do on their platforms. Therefore, the agencies' primary option to address the issue is to work directly with social media stakeholders to implement safeguards. Postal Inspection Service management stated it has attempted to work with these companies to stop the advertising and sale of counterfeit labels; however, cooperation has been inconsistent. Without the cooperation of social media companies, the Postal Service and the Postal Inspection Service have limited legal options to remove postings advertising counterfeit labels.

**Figure 7. Examples of Counterfeit Label Advertisements on Social Media**

[redacted]

Source: OIG screenshots of label advertisements on a social media website, obtained January 23, 2026.

**Figure 8. Counterfeit Label Advertisements on an eCommerce Website**

[redacted]

Source: OIG screenshots of label advertisements on an eCommerce website, obtained January 23, 2026.

Counterfeit label advertisements may have been prevalent, in part, because Postal Inspection Service communications focused more on informing the public about counterfeit stamps, not labels, as of January 2026. The Postal Inspection Service and Corporate Communications shared documentation of eight public communications relating to counterfeit postage dating back to February 2023.[31] All eight communications mentioned counterfeit stamps; however, only five mentioned counterfeit labels. This indicates an opportunity for the Postal Inspection Service to expand its public messaging to better reflect the current counterfeit label issue.

Without addressing these challenges, consumers remain at risk of inadvertently purchasing counterfeit labels, which could further harm the Postal Service reputation, reduce consumer confidence, and prolong financial losses.

### Recommendation #10

We recommend the **Vice President, Chief Information Security Officer**, in coordination with the **General Counsel and Executive Vice President**, **Vice President, Government Relations and Public Policy**, and the **Chief Postal Inspector**, establish a strategy to enable the removal of counterfeit label posts and advertisements from social media websites, and/or advocate with lawmakers for such changes.

### Recommendation #11

We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Corporate Communications**, develop a strategy to effectively communicate to the public the risks of purchasing or using counterfeit labels.

### Postal Service Response

Management agreed with finding 5 and recommendations 10 and 11.

In response to recommendation 10, management stated that both CISO and the Postal Inspection Service agree to collaborate with internal and external partners to develop unified strategies for preventing and removing counterfeit label advertisements on social media. The Postal Inspection Service will also collaborate with both internal and external parties to pursue removal and prosecute efforts, when appropriate. The Postal Inspection Service will also identify outside vendors to conduct site assessments and facilitate administrative removals. The target implementation date is May 31, 2027.

In response to recommendation 11, management stated that it will include a section on prevention communication in its national strategy for counterfeit postage and it has begun social media boosting on Postal Inspection Service national channels. The target implementation date is May 31, 2027.

### OIG Evaluation

The OIG considers management's comments responsive to recommendations 10 and 11, as corrective actions should resolve the issues identified in the report.

## Looking Forward

We recognize and acknowledge the Postal Service has taken actions and made progress toward reducing counterfeit label volumes. As the Postal Service takes additional steps to address this complex challenge, there may be opportunities for it to collaborate with its competitors in the logistics industry to identify broader solutions to the issue. Counterfeit labels are not a challenge faced solely by the Postal Service; counterfeit and fraud of all kinds can affect any organization. Commercial mail services and other courier companies also experience financial losses due to these deceptive practices, which adversely affect their shareholders and employees. It is essential for the Postal Service to implement a multifaceted strategy and allocate sufficient resources to mitigate the considerable risks posed by counterfeit labels, thereby supporting its objective of ensuring long-term financial stability.

31 The earliest communication was February 2023. Not all were dated.

# Appendices

**Appendix A: Additional Information** .......... 27
Scope and Methodology .......... 27
Prior Audit Coverage .......... 29
**Appendix B: The Counterfeit Label Lifecycle** .......... 30
**Appendix C: Management's Comments** .......... 31

# Appendix A: Additional Information

## Scope and Methodology

Our objective was to evaluate the Postal Service’s and the U.S. Postal Inspection Service's efforts to address counterfeit postage. We focused our review on counterfeit postage, which for the purposes of this report we defined as “unpaid USPS shipping labels and the packages which these labels are on.” We excluded counterfeit stamps, which is addressed in a separate report.[32]

To accomplish our objective, we:

- Interviewed Postal Service Headquarters management to obtain information on counterfeit labels and the Counterfeit Postage Intercept Program.
- Interviewed U.S. Postal Inspection Service Headquarters and division management to understand their operations related to counterfeit labels.
- Interviewed and observed the contracted handling facility involved in the Counterfeit Postage Intercept Program to understand their roles and responsibilities, operations, and controls.
- Researched, identified, and obtained laws, policies, and procedures regarding counterfeit label crimes.
- Analyzed data regarding counterfeit labels volumes, estimated revenue losses, and investigations.
- Judgmentally selected and conducted site visits at mail processing facilities and retail and delivery units nationwide, as shown in Table 2. On-site, we interviewed Postal Service officials, conducted observations of mail intake, and tested Intercept Process controls.

**Table 2. Judgmentally Selected Site Visit Locations**

| Facility | City, State | Date Visited |
|---|---|---|
| **Mail Processing Plants** | | |
| [redacted] | [redacted] | 05/13/2025 |
| [redacted] | [redacted] | 05/15/2025 |
| [redacted] | [redacted] | 05/15/2025 |
| [redacted] | [redacted] | 05/15/2025 |
| [redacted] | [redacted] | 06/03/2025 |
| [redacted] | [redacted] | 06/24/2025 |
| [redacted] | [redacted] | 06/24/2025 |
| [redacted] | [redacted] | 06/25/2025 |
| [redacted] | [redacted] | 06/26/2025 |
| [redacted] | [redacted] | 07/28/2025 |
| [redacted] | [redacted] | 07/29/2025 |
| [redacted] | [redacted] | 08/12/2025 |
| [redacted] | [redacted] | 08/12/2025 |
| [redacted] | [redacted] | 08/13/2025 |
| [redacted] | [redacted] | 08/13/2025 |
| [redacted] | [redacted] | 08/14/2025 |

32 *Counterfeit Stamps* (Report Number 25-121-R26, dated June 16, 2026).

| Facility | City, State | Date Visited |
|---|---|---|
| [redacted] | [redacted] | 08/14/2025 |
| [redacted] | [redacted] | 08/26/2025 |
| [redacted] | [redacted] | 08/27/2025 |
| [redacted] | [redacted] | 08/28/2025 |
| **Retail and Delivery Units** | | |
| [redacted] | [redacted] | 06/24/2025 |
| [redacted] | [redacted] | 06/24/2025 |
| [redacted] | [redacted] | 06/26/2025 |
| [redacted] | [redacted] | 06/24/2025 |
| [redacted] | [redacted] | 06/25/2025 |
| [redacted] | [redacted] | 06/25/2025 |
| [redacted] | [redacted] | 06/25/2025 |
| [redacted] | [redacted] | 06/26/2025 |
| [redacted] | [redacted] | 06/26/2025 |
| [redacted] | [redacted] | 07/24/2025 |
| [redacted] | [redacted] | 07/28/2025 |
| [redacted] | [redacted] | 07/31/2025 |
| [redacted] | [redacted] | 07/31/2025 |
| [redacted] | [redacted] | 07/31/2025 |
| [redacted] | [redacted] | 07/31/2025 |
| [redacted] | [redacted] | 08/05/2025 |
| [redacted] | [redacted] | 08/05/2025 |
| [redacted] | [redacted] | 08/05/2025 |
| [redacted] | [redacted] | 08/12/2025 |
| [redacted] | [redacted] | 08/12/2025 |
| [redacted] | [redacted] | 08/13/2025 |
| [redacted] | [redacted] | 08/13/2025 |
| [redacted] | [redacted] | 08/13/2025 |
| [redacted] | [redacted] | 08/14/2025 |
| [redacted] | [redacted] | 08/26/2025 |
| [redacted] | [redacted] | 08/27/2025 |
| [redacted] | [redacted] | 08/28/2025 |

We conducted this performance audit from March 2025 through September 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management on

August 5, 2026, and included its comments where appropriate.

In planning and conducting the audit, we obtained an understanding of counterfeit labels and the Counterfeit Postage Intercept Program 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 following five components were significant to our audit objective:

- Risk Assessment
- Control Environment
- Control Activities
- Information and Communication
- Monitoring

We developed audit work to ensure that we assessed these controls. Based on the work performed, we identified internal control deficiencies related to all five components 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 and Product Tracking & 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

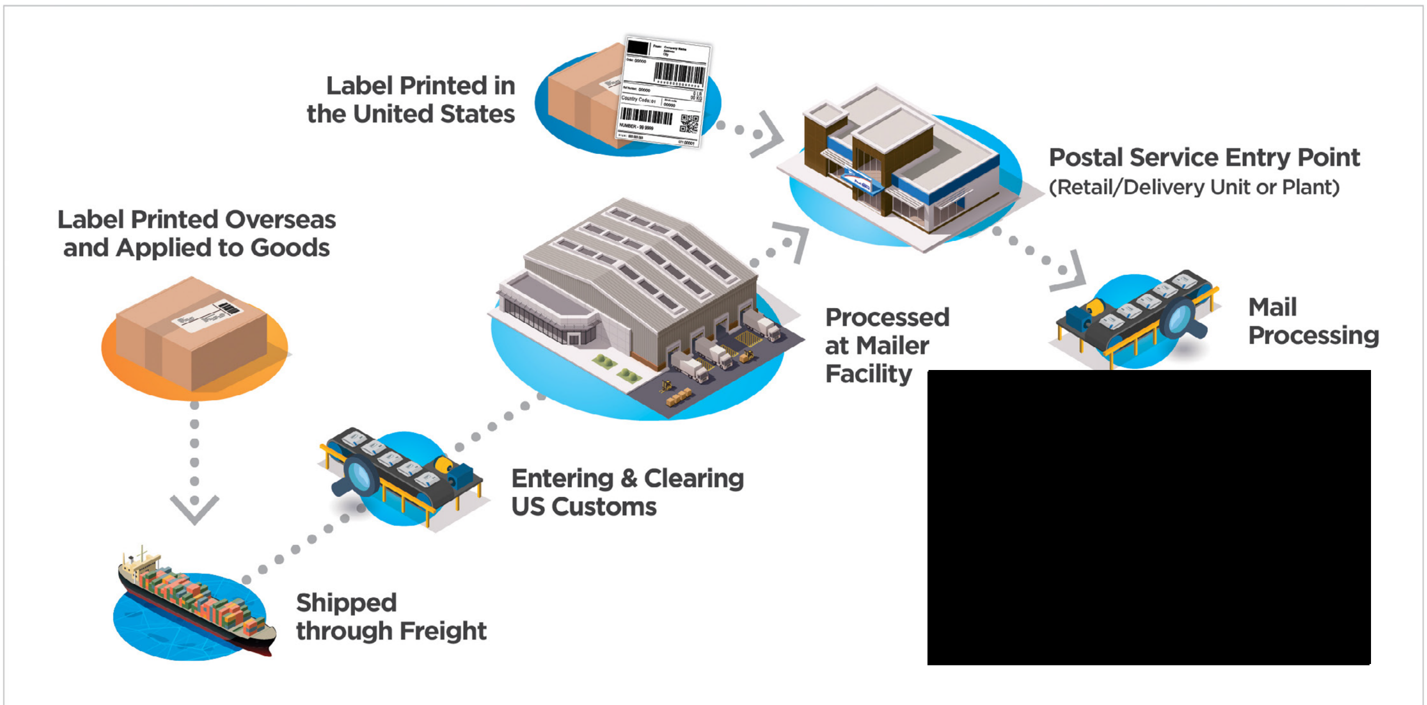
| Report Title | Objective | Report Number | Final Report Date | Monetary Impact |
|---|---|---|---|---|
| *Counterfeit Stamps* | To evaluate the Postal Service's and the Postal Inspection Service's efforts to mitigate the threat of counterfeit stamps. | 25-121-R26 | June 16, 2026 | $383.4 million |
| *Management Alert – Emerging Counterfeit Label Trend* | To promptly notify the U.S. Postal Service about an identified deficiency in the detection of counterfeit package labels with [redacted]. | 25-072-3-R26 | April 8, 2026 | $92.6 million |
| *Management Alert – Enterprise Payment Account Fraud* | To provide immediate notification of issues related to an identified deficiency in the prevention of Enterprise Payment Account (EPA) fraud. | 25-072-2-R26 | February 10, 2026 | $1.8 billion |
| *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 |

# Appendix B: The Counterfeit Label Lifecycle

Postal Service and Postal Inspection Service management stated counterfeit labels most often originate through [redacted] actors, but not necessarily exclusively. Bad actors who create counterfeit labels may either [redacted] who then enter them into the mailstream; or [redacted] who apply the labels to packages domestically. At ports of entry, the Postal Inspection Service works with U.S. Customs and Border Protection to identify packages with counterfeit labels. If a counterfeit label is not caught during customs inspection, the package continues to a domestic mailer facility where it is then entered into the mailstream.

Mailers may enter packages with counterfeit labels at any Postal Service entry point, including retail locations, delivery units, or mail processing facilities. Packages can be dropped off at a retail counter, package chute, self-service kiosk, delivery facility dock, or scheduled for carrier pickup. At mail processing facilities, mailers can drop off packages at the docks or schedule Postal Service pick-up from their location. Once packages enter the mailstream, the Intercept Process [redacted] Otherwise, packages will be processed and transported for delivery. See Figure 9 for a map of this process.

### Figure 9. The Counterfeit Label Journey




Source: OIG generated image based on interviews and observations conducted with the Postal Service and Postal Inspection Service.

# Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

August 31, 2026

LAURA LOZON
DIRECTOR, AUDIT SERVICES

SUBJECT: Management Response: Efforts to Mitigate Counterfeit Postage (Audit 25-072-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, *Efforts to Mitigate Counterfeit Postage*

**Monetary Impact**
Management agrees with the monetary impact and calculations used.

**Finding #1: Lack of Comprehensive Oversight and Formal Decision Authority to Address Counterfeit Postage Fraud**
While management agrees with the finding that official documentation may not have been sent out to the entire organization when the fraud program was established, the other components have been addressed.

**Finding #2: Ineffective Controls to Combat Counterfeit Labels Fraud**
Management agrees with this finding.

**Finding #3: Potential for New Technology**
Management agrees with this finding.

**Finding #4: Challenges in Prosecuting Counterfeit Label Cases**
Management disagrees with this finding. Management agrees that there are challenges related to obtaining prosecution in counterfeit label cases, management disagrees with many of the recommendations made below. Each recommendation is addressed individually below. Overall, the Inspection Service has a method in Case Management to track prosecutive efforts; postal inspectors have used state and local prosecution methods when federal prosecution is not feasible. The Postal Inspection Service is already conducting trend analysis related to tips and referrals as well as using Postal Service data to identify patterns and drive investigative responses based on data analytics.

**Finding #5: Challenges in Addressing Counterfeit Label Sales on Social Media Platforms and eCommerce Websites**
Management agrees with this finding.

The following are our comments on the eleven recommendations:

Recommendation 1:
We recommend the **Vice President, Chief Information Security Officer**, establish key programmatics across counterfeit postage efforts, upon final approval, to include:
a) a documented program charter signed by an executive sponsor,
b) a defined program scope that includes coverage of all types of counterfeit postage,
c) clearly defined roles and responsibilities, including voting rights, approval gates, and signatory authority, and
d) documentation of key decisions and approvals.

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

During the audit, the FAM team submitted a written response to an OIG request for an organization chart and mission statement. Both were provided on December 2, 2025. The information included clearly defined roles and responsibilities for all the groups involved in fraud prevention. Additionally, the mission statement aligns with suggestions to cover all types of counterfeit postage. That statement is as follows: *The overall goal of the Fraud Program is to reduce the amount of unpaid volume entering and flowing through the USPS network. The written goal of the program, as per Get it Right (GIR) 841 is to reduce fraud to* [redacted] *of all volume by the end of FY26.*

Management and the OIG have a difference of opinion on what constitutes effective program management. For example, while a formalized project charter that documents key decisions and approvals might be a useful tool, the Postal Service already has established decision processes in place that include all relevant stakeholders prior to operational execution and investments. Modern technology and the nature of fraud necessitate quick action that balances risks and benefits to the Postal Service as opposed to administrative red tape. Program success is ultimately measured by the demonstrated fraud rate.

Management agrees that it did not formally obtain signatures from all stakeholders on the documentation referenced in this recommendation.

Target Implementation Date:
N/A

Responsible Official:
VP, Chief Information Security Officer

Recommendation 2:
We recommend the **Vice President, Chief Information Security Officer**, conduct a review to identify known vulnerabilities not yet addressed by mitigation efforts and develop a plan, with dedicated milestones, to address these vulnerabilities.

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

Management has already acknowledged that a constant review to identify vulnerabilities not addressed must occur. Once such vectors are discovered, a plan is developed with dedicated milestones to address the vulnerabilities, dependent on the scope of work required. Known vectors are included below with expected completion dates.

[redacted]

Target Implementation Date:
8/31/2027

Responsible Official:
VP, Chief Information Security Officer

Recommendation 3:
We recommend the **Vice President, Chief Information Security Officer**, establish an acceptable threshold for mistaken intercepts and resolve the manual and technical errors until the threshold is met.

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

The CISO agrees with the OIG regarding acceptable thresholds for pieces that are intercepted and ultimately released. Today, CISO monitors the frequency and root causes of all false positives and continues to work to reduce disruption to good standing volume through the network.

To enhance visibility, the CISO FAM team rolled out the [redacted] for every configured and configurable equipment nationwide. CISO FAM continues to collaborate alongside CTO and Engineering teams so that they can act on sites or machines that are having issues.

Based on the current available data, for 7/1/2026 - 7/27/2026 the overall redirect rate is [redacted] with a precision rate of [redacted]

CISO has set an internal target of reducing the rate of false positives within the network to [redacted] of properly redirected package volume.

Target Implementation Date:
8/31/2027

Responsible Official:
VP, Chief Information Security Officer
VP, Engineering Systems

Recommendation 4:
We recommend the **Vice President, Chief Information Security Officer**, in coordination with the **General Counsel and Executive Vice President,** determine a strategy and mechanism for recouping retrieval costs from mailers who did not timely transmit payment records.

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

The CISO agrees with seeking opportunity to recoup retrieval costs and has been in contact with Postal Service Law Department for this effort. This effort will require collaboration with multiple parties across the organization and the CISO believes in finding a solution that continues to work in the interest and fairness of all parties. As such, CISO is working with Strategic Sales to ensure that shippers who pay late are aware of this behavior so they can improve upon it.

Additionally, shippers who continue to pay late and do not improve their behavior will be asked to sign the Do Not Intercept (DNI) agreement and take full responsibility for all volume on their MID(s), regardless of payment status.

Target Implementation Date
8/31/2027

Responsible Official:
VP, Chief Information Security Officer
General Counsel and Executive Vice President

Recommendation 5:
We recommend the **Vice President, Chief Information Security Officer**, in coordination with the **Vice President, Retail and Post Office Operations**, the **Vice President, Delivery Operations**, and the **Vice President, Logistics**, establish [redacted] on all package points of entry.

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

The CISO agrees with this recommendation and has been communicating to the OIG, for at least the last 9 months, a strategy to address the points of entry. In prioritizing greater security around volume and payment control on all package points of entry, the CISO, CSSO, CRDO, CLO, CFO, and CPDO are working together to establish a full line of defense at all entry points.

[redacted]

Target Implementation Date:
8/31/2027

Responsible Official:
VP, Chief Information Security Officer
VP, Logistics
VP, Retail & Post Office Operations

Recommendation 6:
We recommend the **Vice President, Chief Information Security Officer**, in coordination with the **Vice President, Applied Engineering**, and the **Vice President, Technology Applications** collaborate with industry partners to establish a strategy on potential technological solutions for mitigating counterfeit postage.

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

The Postal Service has several workstreams and industry focus groups that cover a variety of topics and initiatives. In addition, the CISO and US Postal Inspection Service meet regularly with stakeholders to discuss current fraud trends, remediation strategies, and indicators of compromise. In addition, there is a Mailer's Technical Advisory Committee (MTAC) workgroup chaired by the VP, Applied Engineering and has members of the VP, Technology Applications group and CISO group.

There is also a small task team made of several industry partners and CISO to discuss fraud, this is a Chatham House Rules group. Any solutions will be evaluated to weigh the cost, implementation effort, and benefit.

Target Implementation Date:
8/31/2027

Responsible Official:
VP, Technology Application
VP Applied Engineering
VP, Chief Information Security Officer

Recommendation 7:
We recommend the **Chief Postal Inspector** enhance the Case Management System with a data field to enter whether a case was accepted by the Department of Justice for prosecution, track the trends of acceptance, and pursue further discussion with the Department of Justice where the trends show lack of acceptance.

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

The ability to track cases presented to the United States Attorney's Office (USAO) already exists within Case Management under subject presentation. Therefore, that data is already being captured. As for the second portion of the recommendation, the USAO does not provide a justification for acceptance or declination of a case presented by the Postal Inspection Service and, therefore, the Postal Inspection Service would be unable to capture this information in Case Management as specified in the recommendation.

Target Implementation Date:
N/A

Responsible Official:
N/A

Recommendation 8:
We recommend the **Chief Postal Inspector** in collaboration with the **General Counsel and Executive Vice President** and the **Vice President, Controller**, explore alternate options for legal action against counterfeit label operations, including utilizing the Revenue Deficiency Process and state and local prosecution.

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

On June 16, 2026, OIG issued audit report #25-121-R26 titled *Counterfeit Stamps*. OIG assigned recommendation 4 to the Chief Postal Inspector, in coordination with the General Counsel and Executive Vice President, to consider other avenues to disable online counterfeit stamp threats more expediently, such as through the Lanham Act.

In response, management agreed with recommendation 4 and stated the Postal Service has used several avenues to disable online counterfeit stamp threats and will continue to do so. The Postal Service shares a goal of disabling threats expeditiously, recognizing that some threats require judicial intervention and are not expeditious.

With the issuance of the final report, OIG considered recommendation 4 closed. The Postal Inspection Service would ask for the same consideration for this recommendation as we continually explore alternate options for legal action. Moreover, postal inspectors are currently using state and local prosecution efforts in their postage fraud cases.

Target Implementation Date:
N/A

Responsible Official:
N/A

Recommendation 9:
We recommend the **Chief Postal Inspector** perform a continuous trend analysis on counterfeit postage tips and referrals, including identification of geographic hotspots and patterns in fraud vectors reported.

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

The Counterfeit Postage Reporting System (CPRS) is a database used to collect data (counterfeit postage tips and referrals). Currently, the Postal Inspection Service extracts the data from the CPRS and conducts trend analysis on it. In addition to the trend analysis done from the CPRS data, the Postal Inspection Service also works with several USPS groups including CISO Analytics, and Engineering to conduct continuous trend analysis related to counterfeit postage.

On August 3, 2026, the Postal Inspection Service submitted documentation to USPS OIG demonstrating the trend analysis presently being completed utilizing counterfeit postage tips and referrals from CPRS. Based on the trend analysis performed by the Postal Inspection Service, the recommendation provided is unnecessary, since said work is already being conducted.

Target Implementation Date:
N/A

Responsible Official:
N/A

Recommendation 10:
We recommend the **Vice President, Chief Information Security Officer,** in coordination with the **General Counsel and Executive Vice President**, **Vice President, Government Relations and Public Policy,** and the **Chief Postal Inspector**, establish a strategy to enable the removal of counterfeit label posts and advertisements from social media websites, and/or advocate with lawmakers for such changes.

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

The CISO agrees and will continue to collaborate with USPIS and lean on other qualifying teams to determine a unified strategy for prevention and removal of counterfeit label promotion on social media sites. Due to the prolific nature of such advertising schemes and anonymity related to associated accounts, this will demand continuous commitment and advocacy by other invested parties.

The Postal Inspection Service agrees with this recommendation and will collaborate with other invested parties, both internal and external, to determine appropriate strategies for removal and/or prosecutive efforts when appropriate. The Postal Inspection Service is also attempting to identify external vendors that may be able to support larger-scale site evaluations and administrative takedowns.

Target Implementation Date:
5/31/2027

Responsible Official:
VP, Chief Information Security Officer
Chief Postal Inspector

Recommendation 11:
We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Corporate Communications,** develop a strategy to effectively communicate to the public the risks of purchasing or using counterfeit labels.

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

As part of the National Strategy for counterfeit postage, there will be a section on prevention communication to the public and Postal Service employees.

Social Media Boosting has already begun on Postal Inspection Service national channels.

Target Implementation Date:
5/31/2027

Responsible Official:
Chief Postal Inspector

E-SIGNED by HEATHER.L DYER
on 2026-09-02 13:30:18 EDT

Heather Dyer
Vice President, Chief Information and Security Officer

E-SIGNED by Robert.B Wemyss
on 2026-09-01 11:48:19 EDT

Robert Wemyss *for Gary Barksdale*
Deputy Chief Inspector

E-SIGNED by Keith.E Weidner
on 2026-09-01 15:51:43 EDT

Keith Weidner
General Counsel and EVP

E-SIGNED by Jennifer.T Vo
on 2026-09-01 11:48:12 EDT

Jennifer Vo
Vice President, Retail & Post Office Operations

E-SIGNED by JOHN.S MORGAN
on 2026-09-01 15:27:34 EDT

John Morgan
Vice President, Delivery Operations

E-SIGNED by ROBERT CINTRON
on 2026-09-01 11:38:19 EDT

Robert Cintron
Vice President, Logistics

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.