Counterfeit Stamps

AUDIT REPORT

Report Number 25-121-R26 | June 16, 2026

Table of Contents

Highlights

Background

The U.S. Postal Service delivers over 108 billion pieces of mail annually, and each piece requires an approved stamp or other payment indicator. Bad actors, however, are increasingly selling, printing, or distributing counterfeit stamps. To combat this threat to its finances and customers, the Postal Service and its primary law enforcement arm, the U.S. Postal Inspection Service, focus on preventing counterfeit stamps from entering the mail system through public education, removing online fraud schemes, or partnering with other federal law enforcement to interdict illicit inbound shipments.

What We Did

Our objective was to evaluate the Postal Service and Postal Inspection Service's efforts to mitigate the threat of counterfeit stamps. We reviewed related policies, initiatives, and data; engaged a contractor to assess online threats; and tested equipment.

What We Found

Postal Service and Postal Inspection Service mitigation efforts are limited, with no substantive approach to identify counterfeit stamps in the Postal Service network. While the Postal Service and the Postal Inspection Service have increased prevention-related efforts, the quantity of counterfeit stamps in the network remains unknown.

The Postal Service has not developed a comprehensive, risk-based strategy for identifying and mitigating counterfeit stamps. Developing such a strategy would help coordinate efforts across the organization, putting the Postal Service in a stronger position to protect its revenues and customers. The urgency of this threat also necessitates immediate actions to address other mitigation shortfalls. First, the Postal Service did not set mail processing equipment's detection capabilities to a level to sufficiently detect counterfeit stamps or conduct sample testing to quantify the potential revenue loss. Second, the Postal Service has no identification capabilities across any other points of mail entry, such as through [redacted]. We estimate these shortfalls resulted in over $349 million in revenue loss and $1.7 billion of revenue at risk in fiscal year 2026. Lastly, the Postal Service takes more than twice as long as comparable companies to disable online threats due to legal considerations.

Recommendations and Management's Comments

We made four recommendations to address the issues identified in the report, and management agreed with all four. We consider management's comments responsive, as corrective actions should resolve the issues. Management's comments and our evaluation are at the end of each finding and recommendation. See Appendix B for management's comments in their entirety.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

June 16, 2026

MEMORANDUM FOR: GARY BARKSDALE
CHIEF POSTAL INSPECTOR

KEITH WEIDNER
GENERAL COUNSEL AND EXECUTIVE VICE PRESIDENT

AMIT CHOLKAR
VICE PRESIDENT, ENGINEERING SYSTEMS

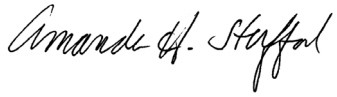
STEPHEN DEARING
VICE PRESIDENT, CHIEF DATA AND ANALYTICS OFFICER

JASON DECHAMBEAU
VICE PRESIDENT, PROCESSING OPERATIONS

CARA GREENE
VICE PRESIDENT, CONTROLLER

JENNIFER VO
VICE PRESIDENT, RETAIL AND POST OFFICE OPERATIONS

GREGORY WHITE
VICE PRESIDENT, NETWORK SOLUTIONS AND PERFORMANCE EXCELLENCE



FROM: Amanda H. Stafford
Deputy Assistant Inspector General
for Retail, Marketing, & Supply Management

SUBJECT: Audit Report – Counterfeit Stamps
(Report Number 25-121-R26)

This report presents the results of our audit to address the efforts the Postal Service and Postal Inspection Service are making to combat counterfeit stamps.

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. Recommendations 1, 2, and 3 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 consider recommendation 4 closed with issuance of this report.

We appreciate the cooperation and courtesy provided by your staff. If you have any questions or need additional information, please contact Josh Bartzen, Director, Retail & Infrastructure, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of counterfeit stamps[1] (Project Number 25-121). Our objective was to evaluate the U.S. Postal Service and Postal Inspection Service's efforts to mitigate the threat of counterfeit stamps. See Appendix A for additional information about this audit.

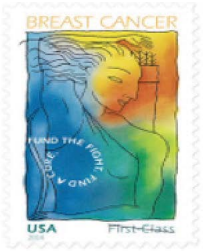
Background

The Postal Service delivers more than 108 billion pieces of mail each year. Each piece should contain an approved Postal Service stamp — such as a Forever stamp — or other postage payment indicator (see sidebar Figure 1). The Postal Service recorded revenues of over $4.4 billion from the sale of stamps in fiscal year (FY) 2025, most of which was from Forever stamps ($3.8 billion).

This revenue stream, however, is threatened by domestic and international bad actors attempting to commit fraud against the Postal Service and its customers by printing, marketing, selling, or using counterfeit stamps. In 2018, the Universal Postal Union[2] estimated related annual losses of over $500 million to postal administrations and customers throughout the world. Today the threat of counterfeit stamps continues to grow due to advances in printing technology and increased prevalence of online marketplaces and social media. Consumers who use counterfeit stamps can face legal penalties, and even if used unknowingly, the Postal Service will dispose of the mailpiece.

Figure 1. Stamps and Other Postage

The Postal Service provides customers a variety of postage options in accordance with Postal Service rates and requirements (see examples below):



Commemorative Stamp

Forever Stamp

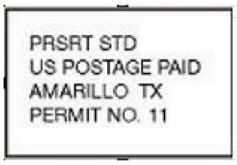
Postcard Stamp

Priority Mail Stamp

International Stamp

Precanceled Stamp

Picture Permit



Permit Imprint

Precanceled Postmark

Source: Stamp images found on USPS.com.

1 Those stamps produced other than by postal administrations, post offices, or their authorized suppliers, with the primary purpose of deceiving or defrauding customers. They are often copies of stamps issued by postal administrators.

2 This is a specialized agency of the United Nations that coordinates postal policies among member nations and facilitates a uniform worldwide postal system. It has 192 member states and is headquartered in Bern, Switzerland.

The U.S. Postal Service Office of Inspector General (OIG) enlisted a contractor to gauge online counterfeit stamp threats, and it found multiple websites, phishing sites, dark web activity, and social media postings.[3] It identified 8,895 instances of marketing or selling counterfeit stamps over a nearly two-month period. The contractor also noted many of these threats originate from outside of the United States, are printed "on demand,"[4] typically mimic Forever stamps, and are frequently sold in bulk quantities at steep discounts — from 20 to 50 percent below face value. Although some counterfeit stamps displayed noticeable defects, the overall quality of most fake stamps makes it increasingly difficult for the Postal Service and the average consumer to distinguish them from genuine stamps.

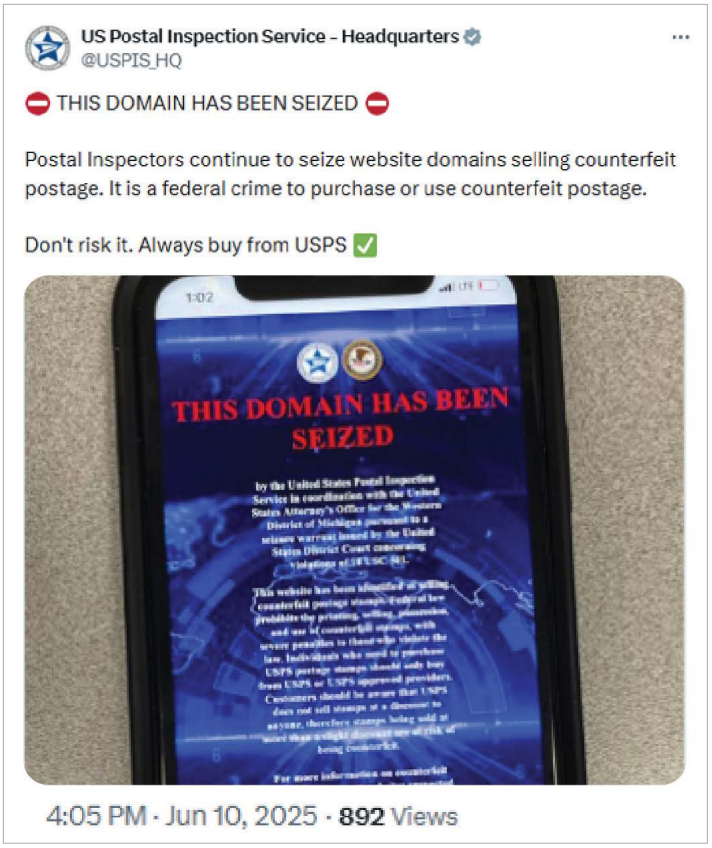
Postal Service Mitigation Efforts

Multiple Postal Service groups share responsibility for combating counterfeit stamps. The Postal Inspection Service leads related investigations, the Law Department provides legal and law enforcement support, and other groups, such as Engineering and Digital Communications, support identification, testing, and customer and employee education. In FY 2025, the Postal Inspection Service created a new Cyber-Enabled Group intended to target counterfeit stamp activity on online marketplaces and digital platforms.

The Postal Service and Postal Inspection Service take the following actions to help prevent or address counterfeit stamps:

- **Educating and Involving the Public.** The Postal Service issues press releases, blog posts, and other social media campaigns to raise awareness around the growing threat of counterfeit stamps. It urges customers to purchase stamps only from official Postal Service approved sources or vendors and warns against heavily discounted stamps sold online. The Postal Inspection Service also hosts the Counterfeit Postage Reporting System, which allows consumers to report suspected counterfeit stamps and related fraud.
- **Identifying and Removing Fraudulent Online Retailers.** The Postal Inspection Service uses artificial intelligence and machine learning to identify counterfeit stamp websites to pursue seizure or removal.[5] For website seizures,[6] the Postal Inspection Service serves a warrant to the host, then places a "splash page" on the website to notify visitors of the seizure (see Figure 2). Postal Inspection Service officials stated that site seizures are a lengthy process requiring a court order. In 2025, the Postal Inspection Service reported seizing 11 websites.

Figure 2. Example of a Seized Website



Source: Postal Inspection Service post on X (formerly known as Twitter), June 10, 2025.

3 We contracted with a leading cyber- and information-security firm to analyze the online threat of counterfeit stamps. Phishing websites impersonated USPS.com to get access to user financial details. The dark web is part of the World Wide Web that allows users and website operators to remain anonymous or untraceable.
4 Now that counterfeit stamps can be mass produced quickly and easily, it is difficult to trace bad actors.
5 The Postal Inspection Service often coordinates with other parties, such as the Postal Service's General Counsel, a U.S. Attorney's Office, or other law enforcement entities on these investigative or removal actions.
6 Lawful temporary or permanent takeover of a web address to prevent its use in illegal, postal-related commerce.

For website removals, the Postal Inspection Service sends the site registrar a letter requesting it take down the site. The Postal Inspection Service took down nearly 190 websites between October and December 2025. Postal Inspection Service officials stated the investigative actions and coordination with the site registrars can be time consuming, sometimes taking months to solidify action.

- **Interdicting Inbound Shipments.** The Postal Inspection Service, in coordination with U.S. Customs and Border Protection (CBP), interdicts or intercepts packages suspected of containing counterfeit stamps entering the United States. In FY 2025, the Postal Inspection Service stated it had seized over 21.6 million stamps worth approximately $18.1 million. Figure 3 shows results of an interdiction at a local sorting facility in Birmingham, AL, uncovering over 200,000 counterfeit Forever stamps originating from Hong Kong.
- **In-Network Identification – Leveraging Employees and Equipment.** The Postal Service and Postal Inspection Service stated that they identify counterfeit stamps through employee training and detection technologies integrated into mail processing operations. The primary detection tool is the Advanced Facer Canceller System (AFCS 200), with roughly 500 units deployed nationwide. In FY 2025, nearly 7 billion mailpieces were run on AFCS 200 machines.

  The AFCS 200 evaluates stamp authenticity by analyzing and testing the accuracy of the image and luminescence.[7] A stamp would "fail" the image test if the machine did not detect the stamp in the Postal Service's image database. A stamp would "fail" the luminescence test if the machine detected the luminescence (phosphor) level to be less than the required threshold. The machines can be run in the following operational modes:

  - High-revenue protection mode, which rejects mail if a stamp fails **either** the image or luminescence test, or
  - Low-revenue protection mode, which rejects mail only if a stamp fails **both** tests.

  The Postal Service's Engineering group determines the operational modes for the AFCS 200 machines throughout the network.

Figure 3. Example of a Counterfeit Stamp Interdiction

The Postal Inspection Service and CBP found over 200,000 counterfeit Forever stamps originating from Hong Kong at a sorting facility in Birmingham, AL.

Source: CBP News Release, February 21, 2025.

7 The AFCS 200 utilizes a high-resolution color imaging camera system designed to identify stamps, metered indicia, and barcode patterns based on their visual characteristics and an Optical Character Reader that can compare stamp images to a database of valid stamps and detect inconsistencies or discrepancies that suggest a stamp is not genuine.

- **Law Enforcement and Legal Actions.** After the Postal Service or the Postal Inspection Service identify issues, they may conduct a law enforcement investigation or action. For example, the Postal Inspection Service can decide to open cases when presented with evidence of the usage, marketing, or selling of counterfeit stamps. The Postal Inspection Service closed 31 counterfeit stamp cases across the country between FY 2020 and FY 2025, which identified nearly $21 million in "known losses."[8] As of December 2025, the Postal Inspection Service had 35 open, ongoing cases. Further, in April 2026, the Postal Inspection Service and OIG completed an investigation in which an owner of a direct-mail marketing business pleaded guilty in federal court after authorities say he used nearly 400,000 counterfeit Forever stamps in a scheme that caused more than $441,000 in losses to the Postal Service.

  The Postal Inspection Service uses two primary options to deter the sale and marketing of counterfeit stamps. First, a Cease-and-Desist order is a formal directive that can be issued by the Postal Inspection Service and the Postal Service Law Department to require the person or business involved to immediately stop the activity in question. The second, less-time intensive option is to secure a Voluntary Discontinuance agreement with the party involved to freely stop the activity in question. A violation of either a Cease-and-Desist order or a Voluntary Discontinuance agreement can be referred to a U.S. Attorney's Office for prosecutorial consideration. During FYs 2023 and 2025, the Postal Inspection Service issued one Cease-and-Desist order and secured 538 Voluntary Discontinuance agreements — most of them (416, or 71 percent) in FY 2025.

Recent Postal Service Counterfeit Concerns

Starting in October 2025, the OIG alerted Postal Service management to multiple revenue risks related to counterfeit package labels and insufficient controls within a system by which mailers can obtain and pay for Postal Service package labels (the Enterprise Payment Account system).[9] Across the three reports, we identified more than $666 million in revenue losses and projected additional potential losses exceeding $1.7 billion if corrective actions were not taken. Given the scale and nature of these vulnerabilities, this risk profile warranted a closer examination of similar threats involving stamps to ensure comprehensive revenue protection.

8 Losses identified during an investigation in which a monetary value can be determined based on available evidence pertaining to a specific scheme and/or financial instrument (such as cash, credit cards, or checks).

9 U.S. Postal Service OIG, *Management Alert – Emerging Counterfeit Label Trend*, Report Number 25-072-3-R26, issued April 8, 2026; U.S. Postal Service OIG, *Management Alert – Enterprise Payment Account Fraud*, Report Number 25-072-2-R26, issued February 10, 2026; and U.S. Postal Service OIG, *Management Alert – Issues Identified with Counterfeit Postage*, Report Number 25-072-1-R26, issued October 15, 2025.

Finding: Counterfeit Stamps Pose Significant Revenue Risk

While the Postal Service and Postal Inspection Service increased prevention-related efforts, they did not identify any counterfeit stamps within the network or quantify the associated revenue implications. This occurred due to a combination of reasons.

Counterfeit Identification Flaws Associated with the AFCS 200

For mail processed on the AFCS 200, we coordinated with the Postal Inspection Service to test the counterfeit stamp identification capabilities on a machine in [redacted] using 800 stamps that we placed on individual pieces of First-Class Mail.[10] While our test indicated the machine correctly identified all stamps with [redacted], it was unable to accurately identify any counterfeit stamps with [redacted]. The machines' inability to identify counterfeit stamps with [redacted] becomes problematic when the machine is run in the low-revenue protection mode because the machine rejects mail only when it identifies stamps that [redacted]. Since all the counterfeit stamps in our test incorrectly "passed" the [redacted], the associated mailpieces would continue in the network when the machines are operating in low-revenue protection mode.

Postal Service officials stated they choose to operate these machines in the low-revenue protection mode based on cost and service considerations. They stated there is a sizeable difference in the amount of mail that is rejected in each mode, with initial estimates that about 3–4 percent of mail is rejected in low-revenue protection mode and upwards of 20 percent in high-revenue protection mode.[11] However, our test results raise questions as to whether any of the 3–4 percent of mail rejected in the "low" setting include counterfeit stamps. Officials stated that implementation of the "high" mode would require extra resources and time to investigate each rejected mailpiece and could impact service if rejected mailpieces had proper stamps. While the OIG understands the justification behind this decision, the Postal Service failed to implement other interim controls for this mail volume, such as sample testing of mailings to quantify or mitigate the threat of counterfeit stamps.

Accordingly, a substantial risk remains of counterfeit stamps not being sufficiently identified in the Postal Service network using the AFCS 200. We estimate a potential revenue loss of $337 million in FY 2026 due to the AFCS 200's limited performance and selected operational setting, which reduces its ability to detect counterfeit stamps.[12]

Counterfeit Detection Concerns Across Other Mail Processing Points

The Postal Service [redacted] for counterfeit stamps across any other points of mail entry or processing, such as stamped mail processed on the [redacted] or mail with [redacted][13] These channels handled about 1.1 and 3.4 billion pieces, respectively, in FY 2025.

Postal Service and Postal Inspection Service staff acknowledged these gaps and confirmed [redacted] We assessed the potential financial impact of these verification shortfalls. For the segment of stamped mail processed on the [redacted], we estimated $1.7 billion in

10 The OIG obtained the counterfeit stamps from the Postal Inspection Service for testing purposes, and all counterfeit mailpieces were handled in a controlled environment and returned to the Postal Inspection Service upon completion.

11 The Postal Service subsequently tested over 327 million pieces on AFCS 200 machines nationwide between April 14-30, 2026, and reported overall rejection rates of 7 (low-revenue protection mode) and 22 percent (high-revenue protection mode), respectively. They then further assessed the rejected volumes to identify what portion of them were attributable to stamps failing the luminescence and/or image tests. For the 7 percent rejected in low-revenue mode, nearly 3 percent failed both the luminescence and image tests. For the 22 percent rejected in high-revenue mode, nearly 6.5 percent failed either the luminescence or image test.

12 Revenue loss applies to funds such as postage, retail sales, rent leases, or fees the Postal Service is entitled to receive but was underpaid or not realized because policies, procedures, agreements, or requirements were lacking or not followed. Our revenue loss estimate was based on 20 percent of the mail volume processed on the AFCS 200 during FY 2026, which the Postal Service estimated would be rejected if the machines were operated in high-revenue protection mode.

13 [redacted] are an area of a Postal Service facility where [redacted] for acceptance. While stamped letters and packages can enter and be processed in the Postal Service network in a variety of manners, we focused on the [redacted] because it processes large amounts of stamped mail and has comparable cancellation operations to the [redacted] and the [redacted] because of the [redacted] The Postal Service also has equipment and processes to detect mail with counterfeit labels in other parts of its network.

revenue at risk for FY 2026.[14] For the segment of mail entered at [redacted], we estimate a potential revenue loss of about $19 million between FYs 2024 and 2025, and project $28 million in FYs 2026 and 2027.[15]

Concerns About the Timeliness of Disabling Online Counterfeit Stamp Threats

The Postal Service took more than twice as long to disable online threats compared to other companies — over 30 days as reported by the Postal Service versus eight days as presented by our contractor.[16] Postal Inspection Service officials stated that their mitigation efforts can take additional time due to various legal and regulatory requirements.[17] They also stated that staff and resource limitations hinder their ability to be more proactive in these efforts, and that they typically conduct online investigative actions only after receiving tips and referrals. While we acknowledge these challenges, increasing online threats will continue to pressure Postal Service mitigation efforts.

Our research indicates the Postal Service could expedite takedowns from online threats by using additional legal tools, such as trademark enforcement under the Lanham Act.[18] Although management has used the Lanham Act regularly to take legal action against bad actors that sell merchandise like t-shirts and hats using unauthorized Postal Service logos and trademarks, it has applied this approach less often to online sellers of counterfeit stamps, even when they misuse Postal Service logos. Leveraging this, or other legal and administrative tools, could possibly help the Postal Service disable additional online counterfeit stamp threats more quickly.

Lack of a Comprehensive, Risk-Based Mitigation Strategy

The Postal Service has not developed a comprehensive, risk-based strategy for identifying and mitigating counterfeit stamps. Such a strategy could include the following:

- **Analyzing and Documenting Vulnerabilities and Risks.** As the Postal Service and Postal Inspection Service face threats across multiple environments — online, cross-border, and during mail acceptance and processing operations — it would be helpful to analyze and document the magnitude of these associated vulnerabilities and risks to Postal Service revenue and customers. Such an analysis could include sampling mailpieces in the current network being run on the AFCS 200s or on other equipment or operations (such as the [redacted]), as well as those entered through the [redacted].
- **Establishing Priorities and Initiatives.** As the Postal Service and Postal Inspection Service have limited resources and other competing demands, it would be useful to identify and document the key priorities and initiatives needed to best address the vulnerabilities and risks associated with counterfeit stamps. Potential initiatives could also consider the future applicability and costs-and-benefits of innovations and technologies, such as artificial intelligence, security ink, or other printing or security features.
- **Clarifying Roles and Responsibilities.** As counterfeit stamps analysis, identification, prevention, interdiction, handling, prosecution, and communication touch on multiple groups in the Postal Service and the Postal Inspection Service, it would be useful to clearly define and delineate

14 Revenue the Postal Service is at risk of losing (for example, a mailer loss because of fraud, inappropriate or unauthorized disclosure of sensitive data, or disruption of critical Postal Service operations and services). Our revenue at risk estimate was based on a projection of about 977 million mailpieces being processed on these machines in FY 2026.
15 Our revenue loss estimate was based on comparing the revenues from precanceled stamps sold and used.
16 Our contractor has experience with 1,000 global clients across many different industries, including education, financial services, healthcare, insurance partners, legal firms, media and entertainment, retail, public sector, and technology.
17 18 U.S. Code § 501 states the Postal Inspection Service must prove the seller knows the stamps being sold are counterfeit.
18 The Lanham Act (Public Law 79-489) is the primary federal statute governing trademark law, service marks, and unfair competition in the U.S. It provides a national system for trademark registration and protects owners against infringement, dilution, false advertising, and cybersquatting.

key roles and responsibilities throughout the organization, including which key group or groups would champion these efforts and be responsible for revenue protection outcomes.

- **Creating Performance Tracking Mechanisms.** As the Postal Service and the Postal Inspection Service dedicate staff, equipment, and other resources to mitigating the threat of counterfeit stamps, it will be essential to track the performance of key efforts and initiatives.

Developing this strategy aligns with leading practices and would help coordinate counterfeit stamp mitigation efforts across the organization, putting the Postal Service in a stronger position to protect its revenues and customers. The urgency of this threat, however, also necessitates immediate actions to supplement key identification and prevention efforts. For example, efforts to increase counterfeit stamp testing and/or sampling of mail (a) processed on AFCS 200s or through other equipment or operations (such as the [redacted]) and (b) entered through [redacted], should be taken to quantify the extent to which mail with counterfeit stamps is already being processed in the Postal Service network. This fundamental information underpins the *Vulnerabilities and Risk* section of the proposed risk mitigation strategy.

Further, the growth of online marketplaces and social media may result in customers unknowingly purchasing counterfeit stamps and experiencing financial loss and/or delayed or rejected mail, which would erode confidence in the Postal Service and its reputation as a secure and trusted entity. Disabling these online threats in a more timely manner would allow the Postal Service an opportunity to focus on other online threats or pursue the most impactful initiatives as identified in the *Priorities and Initiatives* section of the proposed risk mitigation strategy.

Counterfeit stamps will continue to threaten Postal Service revenues and customers without a broader, coordinated action. Developing a risk-based mitigation strategy, paired with immediate corrective actions, would enable the Postal Service and Postal Inspection Service to respond more quickly and effectively to this evolving global threat at a time when revenue protection is paramount for a financially strapped Postal Service.

Recommendation #1

We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Processing Operations; Vice President, Retail and Post Office Operations; Vice President, Engineering Systems; Vice President, Chief Data and Analytics Officer**; and **Vice President, Controller**, develop and implement a risk-based counterfeit stamp identification and mitigation strategy with documented vulnerabilities and risks; initiatives and priorities; roles and responsibilities, including a revenue assurance champion; and performance tracking mechanisms.

Recommendation #2

We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Processing Operations** and **Vice President, Engineering Systems**, take immediate action to enhance counterfeit stamp testing of mail processed on Advanced Facer Canceller System 200 machines, such as by more targeted or sample testing using the high-revenue protection mode.

Recommendation #3

We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Processing Operations** and **Vice President, Network Solutions and Performance Excellence**, take immediate action to assess vulnerabilities of potential counterfeit stamps entered through [redacted] or processed outside of the [redacted], and provide more targeted or sample testing if assessment deems appropriate.

Recommendation #4

We recommend the **Chief Postal Inspector**, in coordination with the **General Counsel and Executive Vice President**, consider other avenues to disable online counterfeit stamp threats more expediently, such as through the Lanham Act.

Postal Service Response

Management partially agreed with the finding, agreed with the recommendations, and disagreed with the monetary impacts. Regarding the finding, while management acknowledged there were counterfeit identification flaws with the AFCS 200 and a risk-based mitigation strategy was lacking, it stated that the Postal Inspection Service mitigates loss risk from counterfeit stamps with well-documented methods, and that there is no evidence of significant loss across other mail processing platforms. Further, it stated the cost to develop and operate systems to sample all stamps would far exceed the realistic benefit.

Regarding recommendation 1, management noted it has begun working on an enterprise-wide Counterfeit Postage National Strategy and will work with Postal Service stakeholders on security control initiatives. This multi-prong approach will include prevention, analytics, technology, awareness, investigations, and tracking mechanisms to gauge progress. The target implementation date is May 31, 2027.

Regarding recommendation 2, management stated that the manual labor required to perform additional verification in high-revenue protection mode presents a mail processing burden. Therefore, the planned solution is to enhance surveillance of mail processed on AFCS 200s through analysis of a real-time machine data "dashboard." If further evaluations are required, Engineering can provide additional manual mail validation support. The target implementation date is November 30, 2026.

Regarding recommendation 3, management stated that although there have been no recent confirmed cases of counterfeit precanceled stamps, it would perform a regular assessment of the precanceled stamps program to assess vulnerabilities and provide targeted follow-up, as appropriate. This financial risk assessment will be conducted on an annual basis by the Product Acceptance and Support senior director. The FY 2026 assessment of precanceled volume showed a low risk, and it will be conducted again in FY 2027. The target implementation date is November 30, 2026.

Regarding recommendation 4, management stated that the Postal Service has used several avenues to disable online counterfeit stamp threats and will continue to do so. Its goal is to disable threats expeditiously, recognizing that some threats require judicial interventions that are not expeditious. In subsequent conversations, management confirmed it is considering various legal, regulatory, and technical options. The target implementation date is June 30, 2026.

Regarding the monetary impacts, management agreed with both calculations but noted additional considerations. For the $336 million revenue loss estimate associated with recommendation 2 (AFCS 200 machine testing), management indicated that efforts to capture fraud volume will offset a portion of the projected revenue loss. Regarding the $47 million revenue loss estimate associated with recommendation 3 (other mail entry points), management disagreed with that level of revenue protection, stating that mailers will typically hold on to unused stamps for future precanceled mailings. As such, the total value of precanceled stamps purchased in a given fiscal year would always have some variance from the postage affixed revenue.

OIG Evaluation

We consider management's comments responsive to the recommendations as the corrective actions should resolve the issues identified in the report and help mitigate the threat of counterfeit stamps. Regarding the partial disagreement with the finding, we reported that the Postal Service and Postal Inspection Service did not identify any counterfeit stamps within the network or quantify the associated revenue implications — gaps that put Postal Service revenues at risk. While

we recognize the potential operating costs associated with stamp sampling efforts, determining the magnitude of the vulnerabilities can provide a roadmap to guide cost effective mitigation efforts that reduce the significant revenue risk to the Postal Service and its customers.

Regarding the monetary impact disagreements, we agree that increased sampling has cost implications and that some customers hold on to precanceled stamps for future mailings. However, considering the lack of detailed Postal Service data on the revenue implications associated with counterfeit stamps, we factored in Postal Service data, related operations, and staff insights, and arrived at reasonable estimates of potential revenue losses and risks from the limited mitigation efforts.

Appendices

Appendix A: Additional Information

Scope and Methodology

Our objective was to evaluate the Postal Service and the Postal Inspection Service's efforts to mitigate the threat of counterfeit stamps. To accomplish our objective, we:

- Reviewed Postal Service and Postal Inspection Service policies, procedures, guidance, and manuals related to counterfeit stamps.
- Reviewed and analyzed applicable laws and regulations.
- Analyzed FY 2022 through 2025 counterfeit stamp data from the Postal Inspection Service, machine processing data from the Postal Service's Web End of Run (WebEOR) system, and PostalOne! data.
- Interviewed Postal Service and Postal Inspection Service officials, such as Forensic Laboratory, Stamp Design, Engineering, Digital Communications, and Law Department responsible for key aspects of mitigating counterfeit stamps.
- Engaged a contractor[19] with subject matter expertise to monitor general and industry threat intelligence. It provided specific insights into the recent attacker techniques, tactics, and procedures and new risks or concerns in the legal or regulatory environment.
- Coordinated with Postal Service and Postal Inspection Service officials to conduct testing of the counterfeit stamp-related detection capabilities of the AFCS 200 machine in [redacted]. This involved running tests of mail with authentic stamps (purchased by OIG) and counterfeit stamps (obtained from the Postal Inspection Service) on both the low– and high-revenue protection modes.

We conducted this performance audit from August 2025 through June 2026 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on May 13, 2026, and included their comments where appropriate.

In planning and conducting the audit, we obtained an understanding of the counterfeit stamp-related 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. We also assessed the internal control components and underlying principles, and we determined that the following five components were significant to our audit objective:

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

We developed audit work to ensure that we assessed these controls. Based on the work performed, we identified deficiencies for each of these five internal control components that were significant within the context of our objectives. Our recommendations, if implemented, should correct the weaknesses we identified.

19 The contractor provided advisory and analytical services to identify and remediate targeted phishing attacks, credential compromise, data exfiltration, brand hijacking, and executive and location threats.

We assessed the reliability of WebEOR, PostalOne! and Enterprise Data Warehouse data by interviewing knowledgeable agency officials, testing for completeness, reviewing related documentation, and comparing data to other related data. We determined that the data was sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
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	4/8/2026	$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 fraud.	25-072-2-R26	2/10/2026	$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	10/15/2025	$485.9 million

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

June 8, 2026

Laura Lozon
Director, Audit Services
Office of the Inspector General

SUBJECT: Management Response: *Counterfeit Stamps* (25-121-DRAFT)

Thank you for providing the Postal Service with an opportunity to review and comment on the findings, recommendations, and monetary impact statement contained in the draft audit report, *Counterfeit Stamps*.

Finding: Counterfeit Stamps Post Significant Revenue Risk

- **Counterfeit Identification Flaws Associated with the AFCS 200**
  Management Response:
  Management **agrees** with -
  The first two paragraphs.

  Management **agrees** with -.
  The last paragraph -The estimated $1 billion in revenue risk is based on the 20 percent rejected mail. For the mail rejected when operating in high-revenue mode, this rejected mail includes those not meeting the high-revenue mode criteria but also includes mechanical rejects, double-feeds, missing indicia, failed dual-verifiers, unfaced mail, and bypasses. When evaluating the 20% rejected mail, approximately 6.47% (of total volume processed) could be considered not meeting the high-revenue mode criteria. The total mail volume at 6.47% is 431,492,824 pieces "at risk". At the current First-Class Single-Piece stamp price (as of October 2025, $0.78), the estimated revenue at risk for FY2026 is $336,564,403. However, this full amount will never be capturable as there will be monies spent on manual processes to capture the fraud volume.

- **Counterfeit Detection Concerns Across Other Mail Processing Points**
  Management Response:
  Management **disagrees** with this finding.

  The Inspection Service mitigates the risk of loss from counterfeit stamps using well documented methods. There is no evidence of any significant loss on the indicated platforms. The cost to develop and operate systems to sample all stamps would far exceed the realistic benefit.

- **Concerns About the Timeliness of Disabling Online Counterfeit Stamp Threats**
  Management Response:
  Management **agrees** with this finding.

  The Inspection Service prioritizes the identification, monitoring, and shutdown of online vendors responsible for selling counterfeit stamps. However, certain threats require judicial intervention, and USPS has limited control over the timeline for removing the threat in those instances.

- **Lack of Comprehensive, Risk-Based Mitigation Strategy**
  Management Response:
  Management **agrees** with this finding.

  The Inspection Service is developing a comprehensive, risk-based mitigation strategy to address counterfeit postage (stamps and shipping labels).

Monetary Impact Statement:

- **OIG estimates the revenue loss associated with recommendation #2 is $336,564,403.**
  Management Response:
  Management **disagrees** with this finding.

  Management agrees with the calculation however, there will be monies spent in capturing this fraud volume which will reduce the revenue loss mentioned above.

- **OIG estimates the revenue loss associated with recommendation #3 is $46,875,103.**
  Management Response:
  Management **disagrees** with this finding.

  Management understands and agrees with the calculation. However, this is a calculation of potential risk and cannot be defined with certainty as revenue loss. The calculation was done by taking the difference between the total value of precanceled stamps purchased versus the PostalOne! postage affixed revenue. The net was $8.1M (2.43%) in 2024 and $11.2M (3.96%). This was then extrapolated to calculate the $46,875,103.

  Management has no concern with this calculation but does not agree that the recommended changes will yield revenue protection of $46,875,103. As outlined in the management response to recommendation 3, mailers will typically hold on to unused stamps for future pre-canceled mailings; therefore, the total value of precanceled stamps purchased in a given fiscal year will always have some variance from the postage affixed revenue.

The following are our comments on each of the four recommendations.

Recommendation #1:
We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Processing Operations**; **Vice President, Retail and Post Office Operations**; **Vice President, Engineering Systems**; **Vice President, Chief Data and Analytics Officer**; and **Vice President, Controller**, develop and implement a risk-based counterfeit stamp identification and mitigation strategy with documented vulnerabilities and risks; initiatives and priorities; roles and responsibilities, including a revenue assurance champion; and performance tracking mechanisms.

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

The Inspection Service has begun working on a Counterfeit Postage National Strategy that will be enterprise wide in the mitigation of counterfeit postage. The Inspection Service will work with Postal Service stakeholders on security control initiatives. This will be part of a multi-prong approach that will include initiatives in prevention, analytics, technology, awareness, and investigations. Once implemented, we will have tracking mechanisms to gauge the progress of the strategy.

Target Implementation Date: 05/31/2027

Responsible Official: Chief Postal Inspector

Recommendation #2:
We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Processing Operations** and **Vice President, Engineering Systems**, take immediate action to enhance counterfeit stamp testing of mail processed on Advanced Facer Canceller System 200 machines, such as by more targeted or sample testing using the high-revenue protection mode.

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

The AFCS 200 has technology to support verification for the presence of a stamp on letter mail. This technology includes a check for luminescence and a check of the stamp image against a stamp database. A recent targeted test conducted with USPIS in 2022, with high-revenue mode enabled, resulted in approximately 20% of mail rejected go to Manual Processing (only one bin of twelve assigned for rejects). This 20%, rejected mail included those not meeting the high-revenue mode criteria but also included mechanical rejects, double-feeds, missing indicia, failed dual-verifiers, unfaced mail, and bypasses. When evaluating the 20% rejected mail, approximately 6.47% could be considered not meeting the high-revenue mode criteria. This 6.47% mail then required manual labor to perform additional

verification for valid postage. The manual labor presents a burden to mail processing operations when supporting a targeted sample test effort.

A planned solution is to enhance counterfeit stamp surveillance of mail processed on the AFCS 200 machines through analysis of high-revenue protection mode machine data that would allow for near real-time view via "dashboard" without disrupting mail processing operations. This provides the dashboard viewer with information for each AFCS 200 machine in their geographic location and would allow for a more strategic resource planning when conducting further mail evaluation. If further evaluation is required, engineering can provide support to enable high-revenue protection mode and reject bin separations to allow improved manual mail validation. A go-live date for an initial dashboard version is estimated for end of November 2026.

Target Implementation Date: 11/30/2026

Responsible Official: Exec. Mgr. Sortation Systems Technology

Recommendation #3:
We recommend the **Chief Postal Inspector**, in coordination with the **Vice President, Processing Operations** and **Vice President, Networking Solutions and Performance Excellence**, take immediate action to assess vulnerabilities of potential counterfeit stamps entered through [redacted] or processed outside of the [redacted] and provide more targeted or sample testing if assessment deems appropriate.

Management Response/Action Plan:
While there have been no recent confirmed cases of counterfeit pre-canceled stamps, we **agree** with regular assessment of the pre-canceled stamps program to assess vulnerabilities and provide targeted follow up as appropriate. Financial risk assessment will be conducted on an annual basis by the Senior Director, Product Acceptance and Support.

The difference between the total value of precanceled stamps purchased versus the PostalOne! postage affixed revenue was $8.1M (2.43%) in 2024 and $11.2M (3.96%). This calculated to a difference of 3.14% for the two years combined. Mailers will typically hold on to unused stamps for future pre-canceled mailings; therefore, the sold versus used calculation will always have variance. In conclusion, our assessment of pre-canceled volume has been conducted for FY26 with a result of low risk. This assessment will be conducted again in FY2027.

Target Implementation Date: 11/30/2026

Responsible Official: Senior Director, Product Acceptance and Support

Recommendation #4:
We recommend the **Chief Postal Inspector**, in coordination with the **General Counsel and Executive Vice President**, consider other avenues to disable online counterfeit stamp threats more expediently, such as through the Lanham Act.

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

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 some threats require judicial interventions and are not expeditious. The Postal Service management understands the OIG will close this recommendation with the issuance of the Final Report.

Target Implementation Date: 06/30/2026

Responsible Official: Chief Postal Inspector and General Counsel and Executive Vice President

Sincerely,

E-SIGNED by GARY.R BARKSDALE
on 2026-06-08 14:26:51 EDT

Gary R. Barksdale
Chief Postal Inspector

E-SIGNED by AMIT CHOLKAR
on 2026-06-06 05:49:30 EDT

Amit Cholkar
Vice President, Engineering Systems

E-SIGNED by GREGORY.T WHITE
on 2026-06-08 16:54:24 EDT

Gregory White
Vice President, Network Solutions and Performance Excellence

E-SIGNED by Keith.E Weidner
on 2026-06-05 13:50:01 EDT

Keith Weidner
General Counsel and Executive Vice President

cc: Corporate Audit & Response Management

Contact us via our Hotline and FOIA forms. Follow us on social networks. Stay informed.

1735 North Lynn Street, Arlington, VA 22209-2020
(703) 248-2100

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

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