



Office of Inspector General | United States Postal Service

Audit Report

Deposit by Mail Controls at the U.S. Postal Service

Report Number 22-034-R22 | March 30, 2022



Table of Contents

- Cover
- Transmittal Letter 1
- Results..... 2
 - Background..... 2
 - Objective, Scope, and Methodology..... 4
 - Finding #1: Security Deficiencies Not Addressed..... 4
 - Recommendation #1..... 6
 - Finding #2: Costs for Providing Deposit by Mail Service 7
 - Recommendation #2..... 8
- Management’s Comments..... 8
- Evaluation of Management’s Comments 8
- Appendix A: Management’s Comments..... 9
- Contact Information 11

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

March 30, 2022

MEMORANDUM FOR: LARRY P. MUNOZ, JR
VICE PRESIDENT, REGIONAL PROCESSING
OPERATIONS, WESTERN

TODD S. HAWKINS
SENIOR DIRECTOR, DISTRIBUTION PROCESSING
OPERATIONS, LAKESHORES DIVISION

THOMAS J. FOTI
VICE PRESIDENT, PRODUCT SOLUTIONS

A handwritten signature in cursive script that reads "Todd J. Watson".

FROM: Todd J. Watson
Director, Network Processing

SUBJECT: Audit Report – Deposit by Mail Controls at the U.S.
Postal Service (Report Number 22-034-R22)

This report presents the results of our audit of Deposit by Mail Controls at the U.S. Postal Service.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact please contact Victoria Dixon, Operational Manager, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit and Response Management

Results

Background

This report presents the results of our self-initiated audit of Deposit by Mail (DBM) Controls at the U.S. Postal Service's [REDACTED] (Project Number 22-234). The [REDACTED] is in the Lakeshores division of the Western Processing region of the Postal Service. This audit was designed to provide Postal Service management with timely information on potential financial and security risks related to DBM service at the [REDACTED].

In February 2015, the Postal Service and a bank initiated the DBM service to allow cash and high-value mailings to be sent to the bank from retail customers through the Postal Service Priority Mail¹ system. The bank has [REDACTED] retail customers that participate in the DBM service.² The Postal Service receives only the revenue from postage paid on the Priority Mail pieces as high-value DBM mail is handled and processed like any other Priority Mail. DBM mail is processed at [REDACTED] —for delivery to the bank. The U.S. Postal Inspection Service and Postal Service personnel are responsible for security at these [REDACTED]. Our review focused on DBM mail service routed through the [REDACTED].

This is a follow-up to our *Deposit by Mail Controls at Selected Mail Processing Facilities* audit (Report Number [NO-AR-19-007](#), dated September 12, 2019). In that audit, we found the Postal Service did not properly address the 10³ high-risk security deficiencies the Postal Inspection Service identified for the [REDACTED]. We recommended management:

- Establish standard operating procedures (SOP) for DBM service, including the use of security cameras, secured doors and staged mail, and adequate rewrap procedures.
- Instruct plant management to properly address security deficiencies identified by the Postal Inspection Service in a timely manner.

Management agreed with and implemented the recommendations. Specifically, in January 2020, they developed a DBM SOP outlining sortation and rewrap procedures and coordinated with the U.S. Postal Service Office of Inspector General (OIG) Office of Investigations (OI) to relocate security cameras. Postal Service management also conducted service talks with employees that noted personal items were prohibited on the workroom floor and installed new exterior building doors in February 2020 for enhanced security.

Since that audit, the Postal Inspection Service conducted a vulnerability and risk assessment at the [REDACTED] and identified four high-risk security deficiencies.⁴ Further, in October 2021, the OIG OI conducted a follow-up review and found that management did not sufficiently address the 10 high-risk security deficiencies found in our prior audit (see [Table 1](#)).

The [REDACTED] processed about [REDACTED] DBM mailpieces for the bank, generating [REDACTED] in postage revenue. We estimate business customers mailed over [REDACTED] in cash to the bank through the DBM service in the last year.⁶

1 Priority Mail is an expedited service of mailable matter weighing no more than 70 pounds with a service objective for delivery of one to three days.

2 Report Number [NO-AR-19-007](#), dated September 12, 2019.

3 There were 17 deficiencies identified overall — 10 at the [REDACTED], five at the [REDACTED] and two at the [REDACTED].

4 Two deficiencies were repeated from the previous assessment and two were newly identified deficiencies.

5 The bank estimated the average DBM cash deposit in 2021 was [REDACTED]. We calculated the total value of these deposits was [REDACTED] based on the number of DBM mailpieces [REDACTED] multiplied by the average cash deposit [REDACTED].

6 Between January 18, 2021, and January 17, 2022.

Table 1. High-Risk Deficiencies Identified

Item	High-Risk Security Deficiency	2019 OIG Report/Postal Inspection Service Vulnerability and Risk Assessment	2020 Postal Inspection Service Vulnerability and Risk Assessment	2021 OIG-OI Follow-up Review
1	Not enough cameras in place to monitor and observe the movement and separation of DBM mail throughout the facility. The ability to view and record transactions of DBM mail is limited because dedicated cameras are not in place to obtain a clear view of the arrival and unloading process.	✓		✓
2	DBM mail is not staged in a secure area after being processed.	✓		✓
3	Employees placed personal bags or items on the workroom floor.	✓		✓
4	Exterior facility doors did not lock mechanically. They are equipped with emergency exit panic bars, which disengage when the doors are opened from the outside, allowing entrance into the building.	✓	✓	✓
5	Not all doors have the access control system; it is only at the main entrance.	✓	✓	✓
6	The entrance to the rewrap area is not restricted to only two assigned personnel.	✓		✓
7	Items were in the damaged mail area that should not have been, obstructing cameras from observing employees working in the damaged mail area.	✓		✓
8	The damaged mail area does not have a secure place to stage DBM mailings.	✓		✓
9	DBM mail is not moved around the workroom floor in a secure container.	✓		✓
10	The incoming and outgoing recording method detailing the final resolution of rewrapped mail has not been updated.	✓		✓
11	During our walkthrough of the facility, 50 employees were seen wearing badges that were not clearly visible.		✓	
12	Numerous leaking parcels were outside the HAZMAT room on a leak table but were not addressed quickly so were being stacked on one another without considering whether the leaking substances would be reactive with one another.		✓	

Source: OIG Report Number [NO-AR-19-007](#), dated September 12, 2019; Postal Inspection Service Vulnerability Risk Assessment, dated August 25, 2020; and OIG analysis.

Objective, Scope, and Methodology

Our objective was to follow-up on controls implemented and actions taken by the Postal Service to address identified security deficiencies surrounding DBM mail service at the [REDACTED].

The scope of this project included following up on high-risk security deficiencies reported in the *Deposit by Mail Controls at Selected Mail Processing Facilities* audit,⁷ security deficiencies the Postal Inspection Service reported between October 1, 2019, and September 30, 2021, at the [REDACTED]; and security deficiencies identified during fieldwork.

To accomplish our objective, we reviewed the high-risk security deficiencies identified in the prior audit, a Postal Inspection Service Vulnerability Risk Assessment Tool security review,⁸ and the OIG OI's memorandum of activity summarizing the status of the Postal Service deficiencies.⁹ We also observed the DBM mail service on December 7-8, 2021, at the [REDACTED] and interviewed managers from that facility and the Lakeshores division.

We relied on computer-generated data from the Vulnerability Risk Assessment Tool system.¹⁰ We did not test the validity of controls over this system; however, we verified the accuracy of the data by reviewing related documentation, tracing selected information to supporting source records, and interviewing knowledgeable Postal Service employees. We also assessed the reliability of DBM package volume data and revenue by interviewing agency officials knowledgeable about the data. We determined the data were sufficiently reliable for the purposes of this report.

We conducted this audit from November 2021 through March 2022 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 objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusion based on our audit objective. We discussed our observations and conclusions with management on March 11, 2022, and included their comments where appropriate.

Finding #1: Security Deficiencies Not Addressed

The Postal Service did not fully address all security deficiencies surrounding DBM mail service at the [REDACTED]. Specifically, we observed in December 2021 that management did not properly address the following five high-risk security deficiencies identified in prior OIG and Postal Inspection Service reviews:

- Security cameras were not in place and active to observe all DBM mail service throughout the facility. However, after our visit, the Postal Inspection Service installed temporary cameras to record those areas where DBM mail is processed and secured. Postal Service management stated they are planning to install permanent cameras throughout the [REDACTED].
- Physical access controls designed to monitor personnel access to the rewrap area¹¹ where DBM mail is repaired are not effective. We observed two employees enter and leave the rewrap area without signing in or out, as required and posted on a large sign attached to the entry gate (see [Figure 1](#)). On December 10, 2021, [REDACTED] management submitted a request to the Postal Inspection Service for security upgrades and secured a contractor to assess the feasibility of adding badge readers to the rewrap area entrance to limit access.

⁷ Report Number [NO-AR-19-007](#) dated September 12, 2019.

⁸ Vulnerability Risk Assessment Tool review dated August 25, 2020.

⁹ OI MOA dated November 2, 2021.

¹⁰ The Vulnerability Risk Assessment Tool system maintains the data recorded as part of the risk assessment tool the Postal Inspection Service uses to identify facility security risks and vulnerabilities.

¹¹ The rewrap area is where damaged or broken mailpieces are repaired.

Figure 1. Rewrap Area Entry Point



Source: OIG photograph taken December 8, 2021, at 10:47 a.m.

- Damaged DBM mail is not repaired in a secure space in the rewrap area, which exposes DBM mail to a higher risk of theft. Postal Service management's request for security upgrades on December 10, 2021, included improvements to the rewrap area and securing DBM mail.
- Secure badge readers are not installed on exterior doors to restrict access to the building. Management stated that they will install badge readers on

designated entry points near outside break areas to allow employees to re-enter the workroom floor (see Figure 2).

Figure 2. Exterior Door Without a Secure Access Badge Reader



Source: Postal Service photograph taken January 26, 2022, at 3:32 p.m.

- Employee personal items were observed on the workroom floor. Although plant management previously conducted a service talk for employees prohibiting personal items on the workroom floor, we observed personal items still present on the workroom floor (see Figure 3). Management stated

that they conducted a second employee service talk on January 8, 2022. Management also secured a contractor to redesign the employee entrance to require employees to enter the locker room before entering the workroom floor and plan to station an employee at the locker room exit to ensure personal items are not taken to the workroom floor.

Figure 3. Personal Items on the Workroom Floor



Source: OIG photograph taken December 8, 2021, at 10:30 a.m.

12 Administrative Support Manual 13, Section 273.114, dated July 2021.

We also observed that controls designed to record incoming and outgoing DBM mail in the rewrap area were not in place. However, during our audit, plant management updated the DBM SOP to require the recording of incoming and outgoing DBM mail; therefore, we are not making a recommendation regarding this issue.

These conditions occurred because management officials did not coordinate with the Postal Inspection Service to address security deficiencies and ensure DBM mail was processed correctly in the rewrap area. According to Postal Service policy, management must remediate deficiencies identified in Postal Inspection Service reviews within 30 working days.¹²

“Inadequate physical protection increases mail theft risk and could also impact the safety and security of employees.”

When management does not properly address security deficiencies, there is an increased risk of mail theft. According to DBM customer records, nearly [REDACTED] and over [REDACTED] for 2020 and 2021, respectively, were reported missing from DBM service mail. Further, the OIG is currently investigating a DBM mail theft totaling approximately [REDACTED] that occurred on November 28, 2021. Inadequate physical protection increases mail theft risk and could also impact the safety and security of employees.

Recommendation #1

We recommend the Senior Director, Distribution Processing Operations, Lakeshores Division, in coordination with the Vice President, Regional Processing Operations, Western, properly address all remaining security deficiencies identified by the Postal Inspection Service within 30 working days of identification, as required by Postal Service policy.

Finding #2: Costs for Providing Deposit by Mail Service

The Postal Service does not know how much it spends to provide DBM service for the bank. While the Postal Service receives revenue from the postage customers pay to send deposits via Priority Mail, it spends additional money on resources to safeguard those deposits. Specifically, the Postal Service converted a maintenance area at the [REDACTED] into a secure caged staging area to hold DBM mail while it awaits armored vehicle transport to the bank (see Figure 4). Employees must enter the secured cage and manually sort some types of DBM mail when an automated processing machine cannot sort it from other Priority Mail, which increases costs. In addition, the Postal Service is planning to add further measures to secure DBM mail at the [REDACTED]. Postal Service management stated these measures will enhance facility security overall. Specifically, Postal Service management has budgeted about \$1.7 million for the following security measures and related improvements:

- Repair and/or replace perimeter fencing around the [REDACTED] facility;
- Install an automated security gate at the employee parking lot entrance;
- Install badge readers for entry into the employee parking lot, exterior doors near designated outside break areas, and throughout the facility;
- Upgrade the badge reader control system throughout the main, storage, and vehicle maintenance buildings;
- Install additional cameras throughout the workroom floor, stairwells, and employee parking lot; and

“While the Postal Service receives revenue from the postage customers pay to send deposits via Priority Mail, it spends additional money on resources to safeguard those deposits.”

- Redesign the employee entrance to require employees to enter the locker room before entering the workroom floor.

Figure 4. Deposit by Mail Cage



Source: OIG photograph taken December 8, 2021, at 10:43 a.m.

In addition, the Postal Inspection Service has contracted with a security company to provide 24-hour armed security guards for the [REDACTED]¹³ (at a cost of about \$200,000) to restrict facility access to authorized personnel until they complete security improvements.

[REDACTED] management stated that headquarters management had not fully considered the additional costs associated with securing the increased DBM volume and the security risks associated with storing a large amount of high-value mail. Further, when DBM mail is lost or stolen, neither the bank nor the Postal Service is responsible for replacing the amount sent. Lost or stolen mail reflects poorly on the Postal Service's brand and public image and leaves the agency open to further customer complaints.

Recommendation #2

We recommend the Vice President, Product Solutions, conduct a cost-benefit analysis of the Deposit by Mail (DBM) program. This analysis should include, at a minimum, an evaluation of anticipated future DBM volume, costs incurred to secure DBM within the [REDACTED] compared to revenue earned, employee safety, and security risks.

Management's Comments

Management agreed with both findings and both recommendations in the report. See [Appendix A](#) for management's comments in their entirety.

Regarding recommendation 1, management stated they will correct deficiencies within 30 working days pending security equipment availability. The target implementation date is April 30, 2022.

Regarding recommendation 2, management stated they will conduct a cost benefit analysis of the [REDACTED] Deposit by Mail program within 6 months to assess customer market demand, anticipated volume, and a cost and risk analysis. The target implementation date is September 23, 2022.

Evaluation of Management's Comments

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

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. The recommendations should not be closed in the Postal Service's follow-up tracking system until we provide written confirmation that the recommendations can be closed.

¹³ The armed security service contract is from December 27, 2021, to February 20, 2022.

Appendix A: Management's Comments



3/24/2022

JOHN CIHOTA
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Management Response: Deposit by Mail Controls at the U.S. Postal Service's [REDACTED] (Project Report Number 22-034-DRAFT)

Thank you for providing the Postal Service with an opportunity to review and comment on the findings and recommendations containing in the draft audit report, Deposit by Mail Controls at the U.S. Postal Service's [REDACTED]

Management agrees with Finding #1: Security Deficiencies Not Addressed.

Management agrees with Finding #2: Costs for Providing Deposit by Mail Service.

Following are our comments for each of the four recommendations.

Recommendation [1]:

We recommend the **Senior Director, Distribution Processing Operations, Lakeshores Division**, in coordination with the **Vice President, Regional Processing Operations, Western**, properly address all remaining security deficiencies identified by the Postal Inspection Service within 30 working days of identification, as required by Postal Service policy.

Management Response/Action Plan:

Management **agrees** with this recommendation. Management will correct deficiencies within 30 working days barring no supply chain issues for materials/issues for security items being addressed.

Target Implementation Date: 04/31/2022

Responsible Official: Vice President, Regional Processing Operations, Western

Recommendation [2]:

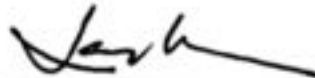
We recommend the **Vice President, Product Solutions**, conduct a cost-benefit analysis of the Deposit by Mail (DBM) program. This analysis should include, at a minimum, an evaluation of anticipated future DBM volume, costs incurred to secure DBM within the [REDACTED] compared to revenue earned, employee safety, and security risks.

Management Response/Action Plan:

Management **agrees** with this recommendation. Product Management will conduct a cost benefit analysis of the Deposit by Mail program in the [REDACTED] area within the next six months to determine customer market demand, anticipated volume, cost and risk analysis.

Target Implementation Date: 09/23/2022

Responsible Official: Vice President Product Solutions



Larry Munoz, VP, Regional Processing Operations, Western


Thomas Fojt, VP, Product Solutions

cc: Manager, Corporate Audit Response Management

OFFICE OF
**INSPECTOR
GENERAL**
UNITED STATES POSTAL SERVICE

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