



# OFFICE OF INSPECTOR GENERAL

## UNITED STATES POSTAL SERVICE

## Mobile System Review

### Audit Report

Report Number  
IT-AR-17-009

September 21, 2017





# OFFICE OF INSPECTOR GENERAL

## UNITED STATES POSTAL SERVICE

### Highlights

***The Postal Service did not manage the mPOS devices and application in accordance with its policies and best practices.***

### Background

In 2016, the U.S. Postal Service managed 31,585 retail offices serving 877 million customers. To reduce wait-time-in-line and expedite customer transactions, the Postal Service developed the mobile Point-of-Sale (mPOS) system. mPOS is a mobile system that allows retail associates to accept credit card and non-PIN debit card payments for customers' retail transactions. In fiscal year (FY) 2016, the mPOS system processed over 26 million transactions totaling about [REDACTED] million in revenue. As of May 2017, there were a total of 3,037 mPOS devices at high-volume retail units.

Like other retail systems, mobile retail systems are vulnerable to the same malware attacks as traditional payment systems, laptops, and other electronic devices.

Our objective was to determine if the mPOS devices and application are managed in accordance with Postal Service policy and best practices.

### What the OIG Found

The Postal Service did not manage the mPOS devices and application in accordance with its policies and best practices. We reviewed access to the mPOS application and found that management should have disabled or removed accounts due to inactivity according to Postal Service policy. Specifically, [REDACTED] of 39,112 active accounts ([REDACTED] percent) have not been

accessed in over [REDACTED] days. This occurred because management bulk-loaded accounts into mPOS based on user access to the lobby retail system and did not regularly review and validate users' need for mPOS access.

We also determined that all mPOS devices are running on [REDACTED]. This occurred because management did not have a process to ensure that they updated all mPOS devices when new operating system versions are available. Additionally, the Postal Service was unable to upgrade some devices [REDACTED]. In FY 2016, management approved the upgrade of all mPOS devices to the latest hardware by February 2018.

When system access, devices, and the application are not properly managed, there is an increased risk that the mPOS system could be exploited. For example, a [REDACTED]

Management also does not adequately train mPOS users. Specifically, [REDACTED] of 26,786 ([REDACTED] percent) active mPOS users with transaction activity did not receive mandatory mPOS user training. Management does not have a process to ensure that employees have completed mandatory training prior to using



# OFFICE OF INSPECTOR GENERAL

## UNITED STATES POSTAL SERVICE

the mPOS application. Improperly trained employees could lead to errors resulting in (1) reduced confidence in the Postal Service brand, (2) increased customer wait-time-in-line causing customers to use a competitor, or (3) unintentionally mishandled customer data and credit card information.

Finally, approved security standards for the mPOS devices and application did not exist. This occurred because the CISO recently re-established a dedicated security standards team and has been working through a backlog of outdated standards.

[REDACTED]

### What the OIG Recommended

We recommended management:

- Disable or delete unnecessary mPOS application user accounts and implement a process to ensure accounts are maintained in accordance with Postal Service policies.
- Upgrade mPOS devices as described in the approved decision analysis report, and develop a process to ensure all mPOS devices are updated to current [REDACTED].
- Develop and implement a process to ensure that employees receive mPOS training prior to granting them access to the mPOS application.
- Implement security standards for the mPOS devices and application.

# Transmittal Letter



OFFICE OF INSPECTOR GENERAL  
UNITED STATES POSTAL SERVICE

September 21, 2017

**MEMORANDUM FOR:** MICHAEL J. AMATO  
VICE PRESIDENT, ENGINEERING SYSTEMS

KELLY M. SIGMON  
VICE PRESIDENT, RETAIL & CUSTOMER SERVICE  
OPERATIONS

GREGORY S. CRABB  
VICE PRESIDENT, CHIEF INFORMATION SECURITY  
OFFICER

E-Signed by Kimberly Benoit  
VERIFY authenticity with eSign Desktop

A handwritten signature in cursive script, appearing to read "Kimberly F. Benoit", is overlaid on a grey rectangular background.

**FROM:** Kimberly F. Benoit  
Deputy Assistant Inspector General

**SUBJECT:** Audit Report – Mobile System Review  
(Report Number IT-AR-17-009)

This report presents the results of our audit of the U.S. Postal Service's Mobile System Review (Project Number 17TG005IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Jason Yovich, Director, Information Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General  
Corporate Audit and Response Management



# Table of Contents

Cover	
Highlights.....	1
Background.....	1
What the OIG Found.....	1
What the OIG Recommended.....	2
Transmittal Letter.....	3
Findings.....	5
Introduction.....	5
Summary.....	5
Application User Access.....	6
Configuration and Compliance Management.....	7
User Training.....	7
Security Standards.....	8
Other Matters.....	8
Recommendations.....	9
Management’s Comments.....	9
Evaluation of Management’s Comments.....	10
Appendices.....	11
Appendix A: Additional Information.....	12
Background.....	12
Objective, Scope, and Methodology.....	12
Prior Audit Coverage.....	13
Appendix B: Management’s Comments.....	14
Contact Information.....	18

# Findings

**Specifically, [REDACTED] of 39,112 [REDACTED] percent) active accounts have not been accessed in over 90 days.**

## Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's mobile system review (Project Number 17TG005IT000). Our objective was to determine if the mPOS devices and application are managed in accordance with Postal Service policy and best practices. See [Appendix A](#) for additional information about this audit.

In 2016, the Postal Service managed 31,585 retail offices serving 877.4 million customers. To reduce wait-time-in-line (WTIL) and expedite customer transactions, the Postal Service developed the mobile Point-of-Sale (mPOS) system — a mobile system that allows retail associates to accept credit card and non-PIN debit card payments for customers' transactions. As of May 2017, there were a total of 3,037 mPOS devices at high-volume retail units. In fiscal year (FY) 2016, the mPOS system processed over 26 million transactions totaling about [REDACTED] million in revenue. Mobile retail systems are vulnerable to the same malware attacks as traditional payment systems, laptops, and other electronic devices.

The goal of the mPOS system is to enhance the customer experience, decrease customer WTIL, and improve lobby management. To achieve this goal, the Postal Service has approved two decision analysis reports (DAR) for the creation and update of the mPOS system through the investment review process. In FY 2014, the Postal Service approved a DAR of [REDACTED] million to develop and implement the initial mPOS system over a seven-year period at 3,100 retail units. Management approved a second DAR in FY 2016 to update mPOS hardware and increase the number of mPOS sites by 1,003. This DAR requested the acquisition and deployment of 4,109 new mPOS devices, kits, receipt printers, and label printers.

## Summary

The Postal Service did not manage the mPOS devices and application in accordance with Postal Service policy and best practices. We reviewed access to the mPOS application and found that the Postal Service should have removed or disabled many accounts due to inactivity according to Postal Service policy. Specifically, [REDACTED] of 39,112 ([REDACTED] percent) active accounts have not been accessed in over 90 days. This occurred because management bulk-loaded accounts into mPOS based on user access to the lobby retail system and [REDACTED] for mPOS access.

We also determined that all of the mPOS devices are using [REDACTED]. This occurred because management did not have a process to ensure that it updated all mPOS devices when [REDACTED] are available. Additionally, management was unable to upgrade some devices [REDACTED]. In FY 2016, management approved a DAR to upgrade all mPOS devices to the latest hardware by February 2018.

When system access, devices, and the application are not properly managed, there is an increased risk that the mPOS system could be exploited. For example, a malicious individual could [REDACTED]

Management also does not adequately train mPOS users. Specifically, 20,803 of 26,786 (77.6 percent) active mPOS users with transaction activity did not receive mandatory mPOS user training. Management does not have a process to ensure that employees have completed mandatory training prior to using the mPOS application. Improperly trained employees could lead to errors resulting in (1) reduced confidence in the Postal Service brand, (2) increased customer WTIL causing customers to use a competitor, or (3) unintentional mishandling of customer data and credit card information.

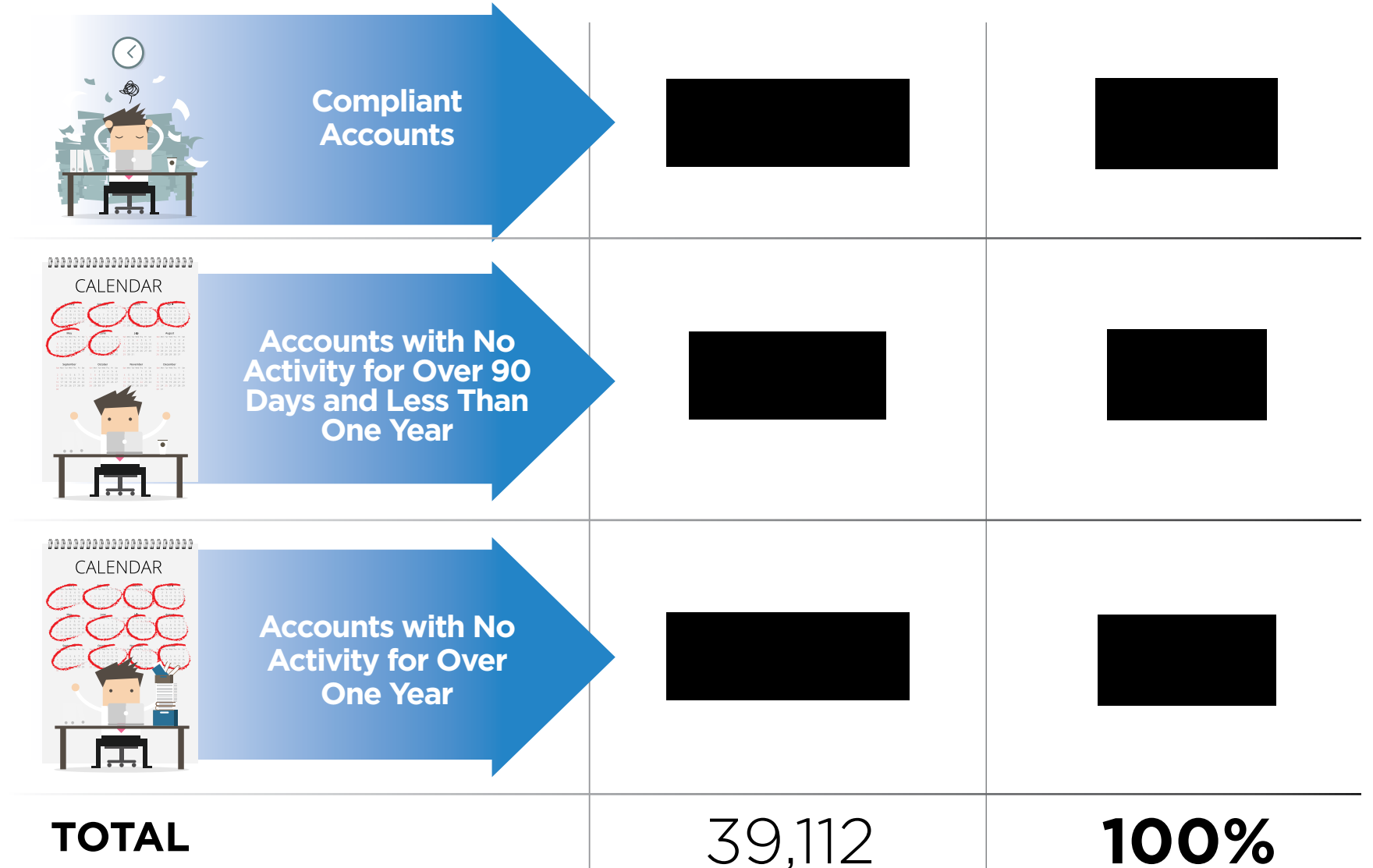
Finally, approved security standards for the mPOS devices and application did not exist because the CISO recently re-established a dedicated security standards team and have been working through a backlog of outdated standards. Without approved documented security standards, devices may not be [REDACTED]

**Postal Service policy states that accounts not used in the last 90 days must be disabled and accounts not used for over one year must be deleted.**

### Application User Access

We identified an excessive number of accounts with access to the mPOS application. Postal Service policy<sup>1</sup> states that accounts not used in the last 90 days must be disabled and accounts not used for over one year must be deleted. We reviewed 39,112 active and approved user accounts and determined that [REDACTED] ([REDACTED] percent) should have been disabled or deleted. See Figure 1 for mPOS user account activity.

**Figure 1: mPOS User Account Activity**



Source: U.S. Postal Service Office of Inspector General (OIG) analysis of active and approved accounts as of June 7, 2017.

<sup>1</sup> Handbook AS-805, *Information Security*, Section 9-4.3, Account Management, dated November 2016.

**Postal Service management did not ensure that [REDACTED] of 26,786 ([REDACTED] percent) active mPOS users with transaction activity received the required training.**

This occurred because Engineering Systems management bulk-loaded users into mPOS based on user access to the lobby retail terminal system and did [REDACTED] for mPOS access. When system access is not appropriately managed, there is an increased risk of unauthorized access to the mPOS device and application, which [REDACTED]

## Configuration and Compliance Management

We determined that the Postal Service is running the mPOS application on devices using [REDACTED]. Specifically, management cannot upgrade [REDACTED] devices currently in use to [REDACTED] because the hardware was out of date. In addition, management configured the mPOS application session to time out after [REDACTED] minutes of inactivity.

Postal Service policy<sup>4</sup> states that all Postal Service information resources must use approved vendor-supported operating systems, including all approved updates and patches. In addition, the application session time out must be set to [REDACTED] minutes.<sup>5</sup> This occurred because Engineering Systems does not have a process to ensure all mPOS devices are [REDACTED] become available. In addition, Retail and Customer Service Operations management configured the system to time out after [REDACTED] minutes, instead of [REDACTED] minutes, so that the retail clerk's efficiency would not be hindered. However, management did not provide a risk acceptance letter for the approved deviation.

[REDACTED] addition, when the application session time out is not set to appropriate limits, there is a [REDACTED]

In FY 2016, Postal Service management approved a requested DAR from Engineering Systems to purchase new mPOS devices that they could [REDACTED]. The upgrade process is scheduled to be completed by February 2018.

During our audit, Engineering Systems initiated a process to change the application session time-out from [REDACTED] minutes to [REDACTED] minutes. The Postal Service should complete this implementation into production by October 2017; therefore, we are not making a recommendation regarding the session time-out issue.

## User Training

Postal Service management did not ensure that [REDACTED] of 26,786<sup>6</sup> ([REDACTED] percent) active mPOS users with transaction activity received the required training. Retail and Customer Service Operations notifies new mPOS retail locations via email of the procedures that need to be completed prior to receiving the mPOS device. This email states that clerks must complete the mPOS training. Based on our interviews with Retail and Customer Service Operations and Engineering Systems, mPOS users are required to take mPOS *User Guide*<sup>7</sup> training in the Learning Management System<sup>8</sup> (LMS).

<sup>2</sup> The number of devices is based on data retrieved from a scan performed May 2, 2017.

<sup>3</sup> [REDACTED] at the time of this audit.

<sup>4</sup> Handbook AS-805, Section 10-3.5, Operating Systems, dated November 2016.

<sup>5</sup> Handbook AS-805, Section 9-4.3.3, Configuring Account Time Outs, dated November 2016.

<sup>6</sup> There were 12,326 users who have never accessed the mPOS application. We subtracted this amount from the total universe of 39,112 to come up with 26,786 users with transaction activity.

<sup>7</sup> The mPOS *User Guide* training covers functionality of the mPOS device, lobby assistance and processes related to mPOS, and accountability and responsibility for handling the stamps and mPOS device.

<sup>8</sup> LMS manages and integrates the full range of training administration processes.



***During our audit, the CISO documented security standards for Postal Service mobile devices. Therefore, we will not be issuing a recommendation for documenting security standards.***



Postal Service management did not ensure that [REDACTED] of 26,786 ([REDACTED] percent) active mPOS users with transaction activity received the required training.

This occurred because Retail and Customer Service Operations management does not have a process to ensure that retail employees have completed mandatory mPOS training prior to approving access to the application.

Improperly trained employees could cause an increase in customer WTIL, which would defeat the purpose of the mPOS program. Additionally, untrained employees could become frustrated and not use the mPOS system or unintentionally mishandle the mPOS device which could result in lost, stolen, or wiped devices.

### **Security Standards**

Postal Service management did not have approved security standards (i.e., hardening standards) for the mPOS devices and application. Postal Service policy<sup>9</sup> states that hardware and system software must be hardened to Postal Service information security requirements. This occurred because the CISO recently re-established a dedicated security standards team and has been working through a backlog of outdated standards. Without approved security standards, [REDACTED]

During our audit, the CISO documented security standards for Postal Service mobile devices. Therefore, we will not be issuing a recommendation for documenting security standards.

### **Other Matters**

Mobile devices have changed business and everyday life in the field of communication and now in the way financial transactions of all types are made. By 2020, 90 percent of mobile users will have made a mobile payment. Mobile payment technologies in the retail industry include options such as Apple Pay, Samsung Pay, and Google Wallet. Some benefits of these mobile payment options include the ability to learn about customer needs, speedier customer transactions, and more payment options for customers.

As payment technologies evolve, it is important for the Postal Service to continue keeping pace with these emerging retail technologies. Using these and other emerging mobile payment technologies will continue to decrease WTIL, improve the overall customer experience, and support promotion of the Postal Service brand image.

<sup>9</sup> Handbook AS-805, Section 8-5.4.2, Hardening Information Resources, dated November 2016.

# Recommendations

***We recommend management develop a process to ensure that all mPOS devices are updated to the [REDACTED].***

We recommend the Vice President, Retail & Customer Service Operations:

1. Review user accounts with access to the mobile Point-of-Sale application and disable or remove any unnecessary accounts; and implement a process to ensure accounts are maintained in accordance with Postal Service policy.
2. Document and implement a process to ensure that employees receive mobile Point-of-Sale (mPOS) training prior to granting access to the mPOS application.

We recommend the Vice President, Engineering Systems:

3. Complete the mobile Point-of-Sale (mPOS) device upgrade in accordance with the fiscal year 2016 Decision Analysis Report to include purchasing new mPOS devices that can be upgraded to [REDACTED].
4. Develop a process to ensure that all mobile Point-of-Sale devices are updated to the [REDACTED].

We recommend the Vice President, Engineering Systems, in coordination with the Vice President, Chief Information Security Officer:

5. Implement security standards for the mobile Point-of-Sale devices and application.

## Management's Comments

Management generally agreed with three of the five findings and their corresponding recommendations in the report. See [Appendix B](#) for management's comments in their entirety.

Regarding recommendation 1, management stated they already have a semiannual process that ensures they remove any unnecessary accounts in accordance with Postal Service policy. Additionally, all retail employees need mPOS access to quickly assist customers when necessary. Many mPOS users only use it during peak holiday periods or vacation coverage periods; therefore, management believes these users need access even if they have not used it in a 90-day period. Management also stated that these accounts meet Handbook AS-805 policy for unused accounts of 90 days or longer because they are part of the user's Active Directory account.

Regarding recommendation 2, management stated they prefer LMS training but developed it as part of a tool kit that also includes the mPOS user guide, job aides, and on-the-job quick guide handouts to provide several training tools for new users to learn mPOS functionality. Management believes the mPOS device is intuitive, simple to use, and comparable to current USPS hand-held scanners clerks already use. Additionally, management stated that the mPOS device poses minimal risk to the Postal Service because it does not have assigned individual accountability, handle cash transactions, require financial reporting, or provide direct access to the Postal Service network or the Internet. Finally, mPOS training is not mandatory per USPS Labor and Human Resources because it does not require a pass/fail score.

Regarding recommendation 3, management agrees to complete the mPOS device upgrade in accordance with the FY 2016 DAR. The target implementation date is [REDACTED].

Regarding recommendation 4, management stated they have an established process for evaluating pre-release/beta iOS builds against various USPS mobility programs. Engineering Systems will continue to work with the relevant application teams to ensure new Apple iOS versions are tested on the mPOS hardware so updates with critical security content are not deferred. The target implementation date is [REDACTED].

Regarding recommendation 5, management stated that the CISO develops hardening standards for platforms and relevant infrastructure components. As of August 30, 2017, the CISO organization has published standards for [REDACTED]. Incorporating the new standards into the mPOS program is a priority for management. The target implementation date is [REDACTED].

## Evaluation of Management's Comments

The OIG considers management's comments responsive for recommendations 3, 4, and 5.

Regarding recommendation 1, management has not met the intent of this recommendation. We found mPOS users with titles such as garage man, body and fender repairman, and motor vehicle operator who had access to the mPOS application. We also found over 13,000 accounts with no mPOS activity in over a year. Some of these accounts are over two years old and have never accessed the mPOS application. Furthermore, Handbook AS-805 section 1-10.1 outlines an exception process to Postal Service policy. The process involves completing a risk assessment, documenting that assessment in a risk acceptance letter, and receiving management approval.

Management stated that the mPOS user role is part of the user's Active Directory account and meets the 90-day policy requirement as long as the user accesses this account within a 90-day period. However, an employee accessing their Active Directory account does not necessarily result in the employee accessing the mPOS system. Employees use their Active Directory account to access many Postal Service network resources, such as email, application servers, and printers. The mPOS application does not have a separate control to track when an employee accesses the mPOS system, and therefore does not meet the 90- and 120-day requirement, as defined in Handbook AS-805 Section 9-4.3.

Regarding recommendation 2, management has not met the intent of this recommendation. The documented procedures for obtaining access to mPOS entails training prior to being granted access. According to their mPOS Information Guide, the purpose of the training is to ensure that users understand the functionality of the mPOS and the accountability and responsibility of handling the mPOS device. The OIG recommends that the Postal Service require this training for all new mPOS users, when appropriate, to reduce the risk of unwanted consequences of misuse or unsecured devices.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations 3, 4, and 5 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. Recommendations 1 and 2 will remain open as we coordinate resolution with management.

# Appendices

*Click on the appendix title  
to the right to navigate  
to the section content.*

Appendix A: Additional Information .....	12
Background.....	12
Objective, Scope, and Methodology .....	12
Prior Audit Coverage.....	13
Appendix B: Management's Comments.....	14



## Appendix A: Additional Information

***With the growth of mPOS system usage, organizations must focus on security and privacy issues related to mPOS, which are vulnerable to the same malware attacks as traditional payment systems, laptops, or other electronic devices.***

### Background

In 2016, the Postal Service managed 31,585 retail offices serving 877.4 million retail customers. To reduce WTIL and expedite customer transactions, the Postal Service uses the mPOS system — a fifth generation Apple iPod touch that allows a retail associate to accept electronic payments by swiping credit cards and non-PIN debit cards.

The Postal Service originally deployed mPOS devices and printers in 2014 to high-traffic locations, after retail research highlighted their ability to reduce WTIL and improve the customer experience. As of May 2017, there were 3,037 mPOS devices deployed at high-traffic retail units. mPOS allows a retail employee to assist in the post office lobby and interact with customers without being tied to conventional retail equipment. Retail employees equipped with mPOS devices are also able to promote the use of on-site self-service kiosks by providing technology-cautious customers with the information, confidence, and support they need to successfully complete transactions with the automated technology.

The Postal Service has approved two DARs for the mPOS system. In FY 2014, the Postal Service approved a DAR of █████ million. The return on investment (ROI) was measured in customer experience, reduced WTIL, and improved lobby management. Management approved the second DAR in 2016 to replace outdated mPOS hardware and increase the number of mPOS sites by 1,003.

With the growth of mPOS system usage, organizations must focus on security and privacy issues related to mPOS, which are vulnerable to the same malware attacks as traditional payment systems, laptops, or other electronic devices. It is important for the Postal Service to secure the mPOS system from unauthorized access to ensure it protects customer credit card information.

### Objective, Scope, and Methodology

Our objective was to determine if the mPOS devices and application are managed in accordance with Postal Service policy and best practices. The scope of our audit was the mPOS devices and application. To accomplish our objective we:

- Interviewed key personnel who manage, support, and use mPOS to determine their roles and responsibilities as they relate to mPOS and gain an understanding of the functionality and integration of mPOS devices.
- Determined if the Postal Service uses a mobile device management platform to lock and wipe lost or stolen devices.
- Reviewed policies on inventory management and obtained an inventory list for mPOS devices to determine if the Postal Service tracks and accounts for them.
- Obtained and reviewed mandatory annual training records and determined if all employees who use mPOS devices have had the mandatory training.
- Evaluated physical access to mPOS devices.
- Evaluated access controls to the mPOS application, determined whether there is accountability when using the application, and determined if only appropriate employees are authorized to use the application.

- Performed a vulnerability scan on the [REDACTED] platform to determine if mPOS devices have any vulnerabilities and are configured according to best practices and internal hardening standards.
- Determined if mPOS devices and the application are patched and updated regularly.

We conducted this performance audit from March through September 2017, 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 August 7, 2017, and included their comments where appropriate.

We assessed the reliability of computer-generated data by reviewing existing information about the data and the system that produced them, and interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

### **Prior Audit Coverage**

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

## Appendix B: Management's Comments



August 30, 2017

LORI LAU DILLARD  
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Mobile System Review (Report Number IT-AR-17-DRAFT)

HQ Management is providing the following response to address the findings and recommendations cited in the Mobile System Review Report IT-AR-17-DRAFT.

The OIG recommends that the Vice President, Retail & Customer Service Operations:

**Recommendation #1**

Review user accounts with access to the [REDACTED] application and disable or remove any unnecessary accounts; and implement a process to ensure accounts are maintained in accordance with Postal Service policy.

**Management Response/Action Plan: Management Disagrees**

Management already has a current process in place that ensures any unnecessary accounts are removed in accordance with Postal Service policy. All user accounts are consistently reviewed by local management as part of a 6 month semi-annual review process. During that review, all employee roles are evaluated by local management and any roles deemed unnecessary are removed at that time.

As lobby assistant duties and line busting may be rotated among employees, mPOS access is needed for all retail employees to be able to quickly assist customers when necessary. In addition, many mPOS users may only use the device during peak holiday periods or during vacation coverage periods. Therefore, all retail employees need the ability to access the mPOS any time they may be called to the lobby to assist customers, even if they haven't used it within a 90 day period.

While the OIG supports their stance of disabling/removing roles by referencing the AS 805 section 9-4.3 for unused accounts of 90 days or longer, the mPOS role is in fact, a part of the user Active Directory account. Therefore, as long as an mPOS user's Active Directory account has been accessed within a 90 day period. It would meet the 90 day access requirement per Postal Policy. (Per the AS 805 section 9-4.3.4 "All access to information resources will be through Active Directory accounts/passwords")

**Target Implementation Date:** NA

**Responsible Official:**

Kelly M. Sigmon, Vice President, Retail & Customer Service Operations

1

**Recommendation #2**

Document and implement a process to ensure that employees receive mobile Point-of-Sale (mPOS) training prior to granting access to the [REDACTED] application.

**Management Response/Action Plan: Management Disagrees**

Although LMS training is preferable, it was developed as part of a tool kit that also included the mPOS user guide, job aids, On the Job instruction and quick guide handouts to provide several training formats for a new user to learn the mPOS functionality. We believe the mPOS device is intuitive and simple to use and is comparable to the current USPS hand-held scanners already used by clerks. The device poses a minimal risk for the Postal Service as it does not have an assigned individual accountability, handle cash transactions, require financial reporting by employees or provide direct access by the user to the Postal network or internet. In addition, it does not store credit card information, receipts or paperwork - making it low risk for customer information as well.

Despite the device's easy-to-use features, OIG assumes that a lack of training could potentially lead to an increase in customer WTIL, user frustration or the mishandling of devices. However, this claim is unsubstantiated and antidotal with no data provided by the OIG to support their claim. Lobby assistants who use mPOS devices are typically RSS and Retail Window trained clerks who are already knowledgeable in conducting customer transactions and handling retail technology as part of their normal duties.

The OIG recommendation that "mandating" training be a prerequisite for mPOS access is not consistent with normal policy nor with training policies for similar devices in use. Furthermore no anticipated benefits, inclusive of cost, have been identified or proven by the OIG report.

Finally, this training is not considered "mandatory" per USPS Labor and Human Resources, since the training does not require or result in a pass/fail score for the user's position.

**Target Implementation Date: NA**

**Responsible Official:**

Kelly M. Sigmon, Vice President, Retail & Customer Service Operations

The OIG recommends that the Vice President, Engineering Systems:

**Recommendation #3**

Complete the mobile Point-of-Sale (mPOS) device upgrade in accordance with the fiscal year 2016 Decision Analysis Report to include purchasing new mPOS devices that can be upgraded to the [REDACTED]

**Management Response/Action Plan: Management Agrees**

Management generally agrees with the recommendation. The current plan is to complete the mPOS device [REDACTED]

**Target Implementation Date**

[REDACTED]

**Responsible Official:**

Michael Amato, Vice President, Engineering Systems



**Recommendation #4**

Develop a process to ensure that all mobile Point-of-Sale devices are updated to the latest [REDACTED]

**Management Response/Action Plan: Management Agrees**

Management generally agrees with the intent of this recommendation. We have an established process for evaluating pre-release/beta iOS builds against various USPS mobility programs (e.g. mPOS and general user iPhones). Engineering Systems will continue to work with the relevant application teams to ensure betas are fully regression-tested on the mPOS hardware so updates with critical security content do not need to be unnecessarily deferred to prevent an operational disruption.

**Target Implementation Date**  
[REDACTED]

**Responsible Official:**

Michael Amato, Vice President Engineering Systems

The OIG recommends that the Vice President, Engineering Systems, in coordination with the Vice President, Chief Information Security Officer:

**Recommendation #5**

Implement security standards for the mobile Point-of-Sale devices and application.

**Management Response/Action Plan: Management Agrees**

Management agrees with the intent of this recommendation. CISO develops hardening standards for platforms and relevant infrastructure components. The applicable hardening standards for mPOS include [REDACTED]. CISO will support both Engineering Systems and Information Technology in the implementation of the applicable hardening standards through validation that standards for [REDACTED] are accurately applied.

As of August 30, 2017, the below standards have been published by the USPS CISO organization. Incorporation into the new mPOS program is a priority for Management and it was in the process of being updated parallel to the audit fieldwork phase.

#	Standard	Release Version	Status (as of 8/30/17)
1	Apple iOS	iOS Security Standard - Apple Mobile Devices-V 1 0, dated 10/3/2012 8:45 AM	Released
2	Wi-Fi	Wi-Fi ISS Security Standard, dated 5/31/2017 1:00 PM	Released
3	[REDACTED]	MobileIron Hardening Standard__V2.0, dated 6/15/2017 12:16 PM	Released

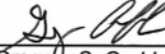
**Target Implementation Date**  
[REDACTED]

**Responsible Official:**

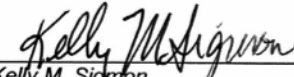
Michael Amato, Vice President Engineering Systems  
Gregory S. Crabb, Vice President, Chief Information Security Officer



Michael J. Amato  
Vice President, Engineering Systems



Gregory S. Crabb  
Vice President, Chief Information Security Officer



Kelly M. Sigmon  
Vice President, Retail & Customer Service Operations



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