OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

September 11, 2015

MEMORANDUM FOR: ROBERT CINTRON
VICE PRESIDENT, ENTERPRISE ANALYTICS

E-Signed by Lorie Nelson
ERIFY authenticity with eSign Deskto
Lorie Nelson

for

FROM: John Cihota
Deputy Assistant Inspector General
for Finance and Supply Management

SUBJECT: Management Alert – Controls Over Credit Card Data at the National Customer Support Center
(Report Number SM-MA-15-003)

This management alert presents security and fraud risks associated with the U.S. Postal Service’s Controls Over Credit Card Data at the National Customer Support Center (Project Number 15BG004SM001).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Keshia L. Trafton, director, Supply Management and Facilities, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Introduction

During an ongoing U.S. Postal Service Office of Inspector General (OIG) audit of U.S. Postal Service address management licensing agreements, we identified security issues with the maintenance of credit card data at the Postal Service's National Customer Support Center (NCSC) in Memphis, TN. The Postal Service's Office of Address Management, located at the NCSC, provides value-added products and services that help business customers better manage the quality of their mailing lists while maximizing the Postal Service's ability to efficiently deliver mail as addressed. This management alert presents security and fraud risks associated with the Postal Service's Controls Over Credit Card Data at the NCSC (Project Number 15BG004SM001).

When we visited the NCSC, we observed that personnel there did not receive and maintain credit card payments and hardcopy payment records according to Payment Card Industry (PCI) requirements and Postal Service policy.[1] PCI compliance applies to all entities involved in payment card processing and all entities that store, process, and transmit cardholder data. In an attempt to adhere to PCI requirements, the Postal Service completed a Delivering Results, Innovation, Value, and Efficiency (DRIVE) initiative to position the Postal Service to pass an independent PCI data security standard audit.[2]

Although the DRIVE initiative was closed, we identified control weaknesses over credit card data. Because of the urgency and sensitivity associated with these weaknesses, we are issuing this alert to allow the Postal Service to take appropriate, timely action to strengthen controls at the NCSC.

Conclusion

The Postal Service needs to improve controls over credit card data at the NCSC. The NCSC did not follow PCI requirements and Postal Service policy for securing credit card information, specifically:

- The credit card numbers on payment records were not masked.[3]

- The facility did not require individuals entering the accounting room (where credit card payment information is received) to have identification access badges.

[1] Handbook AS-805, *Information Security*, dated May 2015, and PCI Data Security Standard (DSS) *Requirements and Security Assessment Procedures*, version 3.1, dated April 2015.
[2] DRIVE Initiative 21, *Payment Card Industry Compliance*, was created for the Postal Service to prepare for and pass an independent PCI audit.
[3] Masking is a method of concealing a segment of data when displayed or printed.

- Management did not protect video cameras surveilling the accounting room from possible tampering.

NCSC personnel stated that they believed they were in compliance with the PCI requirements and Postal Service policy based on an assessment the U.S. Postal Inspection Service (Inspection Service) conducted in 2012 to identify security weaknesses. However, based on our analysis, the assessment did not evaluate PCI controls. Without proper controls, the Postal Service is at risk of unauthorized use of credit card numbers.

We determined the potential impact of compromised payment records to be $52,276 from October 1, 2013, through May 13, 2015.[4]

Credit Card Control Weaknesses

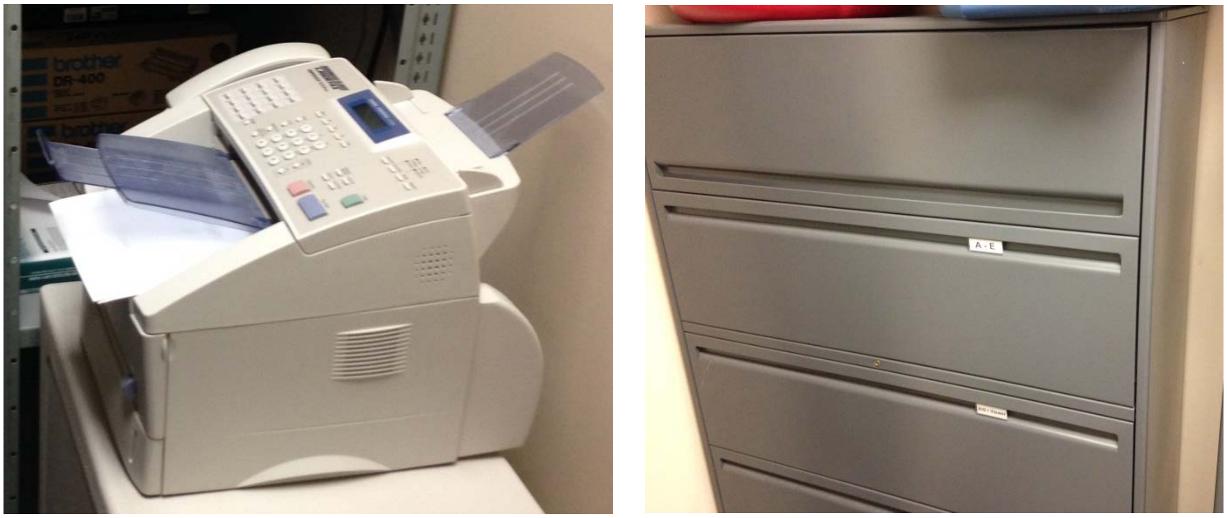
NCSC personnel did not receive and maintain credit card payments according to PCI requirements and Postal Service policy. The credit card numbers on payment records were not masked; the facility did not require employees entering the accounting room (where credit card payment information is received) to have identification access badges; and management did not protect video cameras surveilling the accounting room from possible tampering. Specifically:

- **Credit Card Numbers**. Credit card numbers received via fax were not masked. The accounting room contains a fax machine that receives customer credit card payments, filing cabinets that store hard copies of payment documents for the current fiscal year, and compact disks containing copies of the previous 2 fiscal years (FY). At least 3,687 payments were received during that time.[5]

  Credit card payment information displayed full primary account numbers[6] (PAN) which were stored in filing cabinets (see Figure 1 for photos of the fax machine and filing cabinets in the accounting room). Although the cabinets were secured with keyed locks, Postal Service policy states that PANs must be masked to allow a maximum of the first six or last four digits to be displayed or printed.[7]

[4] We used the Ponemon Institute's *2015 Cost of Data Breach Study: United States,* version SEW03055-USEN-00, dated May 2015, to determine the value of customer records at risk.
[5] The number of payment transactions was provided by NCSC personnel.
[6] Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
[7] Handbook AS-805, Section 3-5.2.f.

Figure 1. Accounting Room



Source: OIG photographs taken May 12, 2015. The accounting room contains a fax machine, which receives credit card payment information, and storage cabinets maintaining credit card payment forms displaying full PANs.

- **Access Control Identification**. Management did not properly secure the accounting room where credit card transactions are stored. The room was secured by a combination lock door, but employee identification access badges[8] should have been required for entry. According to Postal Service policy, the accounting room contains sensitive-enhanced information[9] and must be secured as a controlled area.[10] Personnel authorized to access controlled areas must always use their identification access badge or device for entry, and management must maintain a record of access.[11] See Figure 2 for a photograph of the combination lock doors and the surveillance camera.

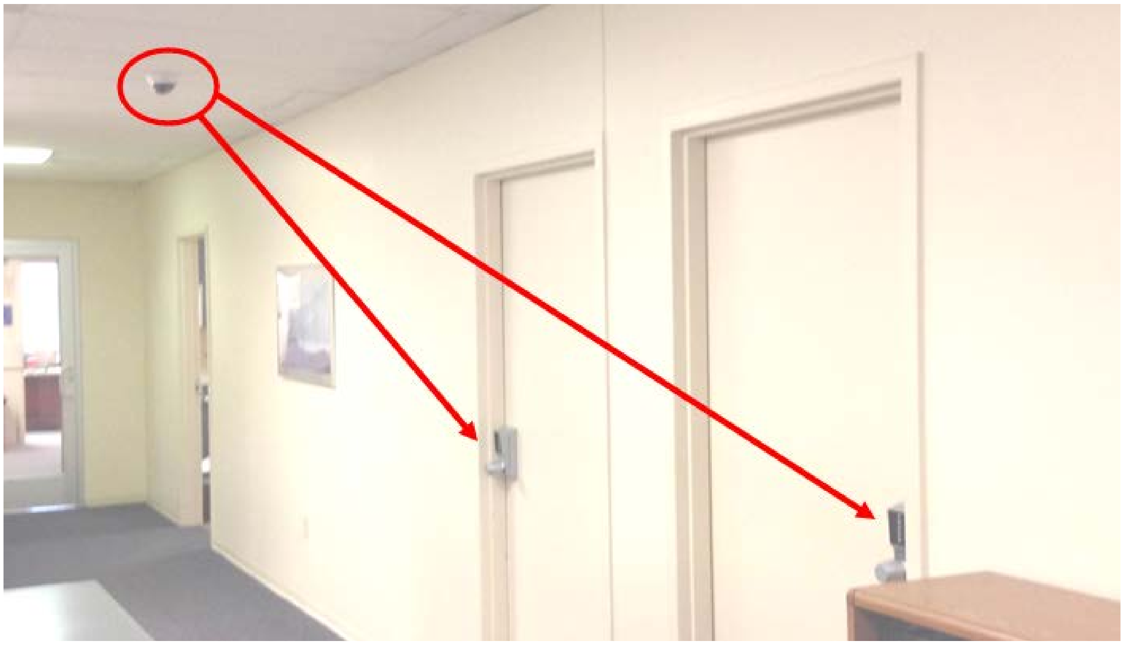
[8] An employee identification access badge is an assigned card key that allows access to a secure location when scanned by a card reader.

[9] Handbook AS-805, Section 3-2.3.2.b, states that full PANs are sensitive-enhanced information.

[10] Handbook AS-805, Section 7-2.3, states that information resources processing sensitive-enhanced information must be in a controlled area.

[11] Handbook AS-805, Section 7-2.1.b., states that access to controlled areas must be restricted by electromechanical means. Personnel authorized access to controlled areas must always use their access control identification badge or device to gain entrance to the controlled area. In addition, 7-2.1.c., states that a record of physical access, both authorized individuals and visitors, must be maintained. Automated mechanisms should be employed where feasible to facilitate the maintenance and review of access records.

Figure 2. Surveillance Camera Observing Combination Lock Doors

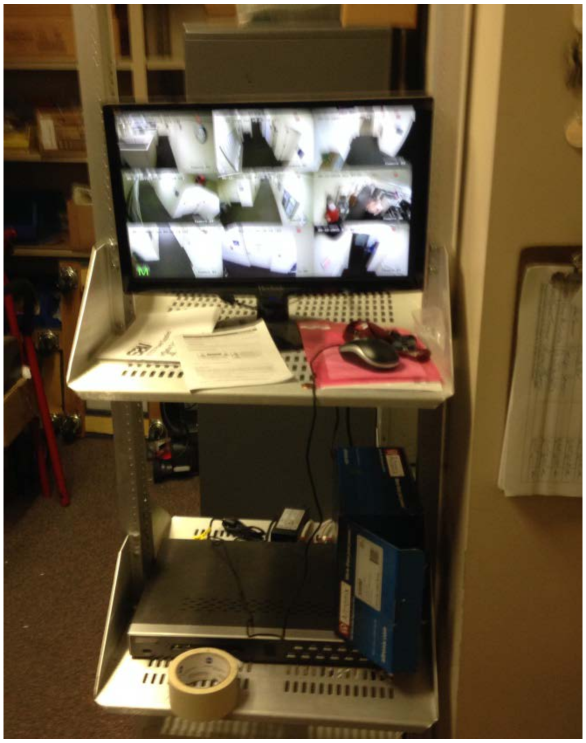


Source: OIG photograph taken February 25, 2015. The surveillance camera records personnel entering the accounting room on the right and the storage room on the left.

- **Video Footage**. A surveillance camera in the hall monitors personnel who enter and exit the accounting and storage rooms; however, the digital video recorder (DVR) that captures the footage is [redacted]. [redacted] According to PCI requirements, video cameras and access control mechanisms should be protected from tampering or disabling by malicious individuals. [redacted]. See Figure 3 for a photograph of the DVR located [redacted].

[12] As of May 19, 2015.
[13] PCI DSS, version 3.1, dated April 2105, Section 9.1.1.b., details requirements, testing procedures, and guidance relating to video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas.

Figure 3. [redacted]



[redacted]

NCSC management stated that they believed they were complying with PCI requirements and Postal Service policy. They relied on the results from an Inspection Service Vulnerability Risk Assessment Tool (VRAT) review conducted in 2012 to identify security weaknesses in their processes. However, we determined the VRAT review focused on security factors involving physical security, information technology security, personnel security, and policy compliance. The assessment did not evaluate PCI compliance.

Without proper controls over credit card data, the Postal Service is at risk of unauthorized use of customer credit card information. From FY 2013 through May 13, 2015, we determined the potential impact for compromised payment records to be $52,276. In addition to financial implications associated with a data breach, non-compliance with PCI standards could damage the Postal Service's reputation and affect its ability to process card transactions.[14]

[14] PCI Security Standards Council.

Recommendation

We recommend the vice president, Enterprise Analytics, direct the manager, Address Management, to:

1. Increase the security of customer information by masking credit card numbers when received and stored in the accounting room.

2. Replace combination locks with employee identification access badge readers or similar devices for the accounting and storage room doors.

3. Restrict personnel with access to the accounting room from being able to access the storage room to prevent tampering with the video surveillance system and having undetected access to primary account number information.

4. Complete periodic Payment Card Industry compliance reviews at the National Customer Support Center.

Management's Comments

Management neither agreed nor disagreed with the findings and recommendation 3.

Management agreed with recommendation 4 and disagreed with recommendations 1 and 2.

Management agreed that the findings and recommendations in this alert would enhance security at the NCSC; however, management stated that a PCI-qualified security assessor (QSA) reviewed the NCSC in August 2015, and found no PCI-related security issues. The QSA deemed the NCSC compliant with PCI rules concerning credit card information; therefore, management believes we should remove any reference to PCI, other than the one we made in recommendation 4, from this alert.

Regarding recommendation 1, management stated that they receive full PANs via fax and cannot mask the information when they receive PANS by this method. They need the information to process transactions. Management stated the Corporate Information Security Office will be updating its policy relating to masked PANs to allow them to be displayed or printed such that only personnel with a legitimate business need (for example, to process or manage transactions or chargebacks) can see the full PAN. Management plans to release the policy by June 30, 2016.

In subsequent correspondence regarding recommendation 1, management stated they now mask credit card numbers after they process payment information and prior to storing the information.

Although management disagreed with recommendation 2, they stated they will work with the Inspection Service to replace the accounting and storage room combination locks with employee identification badge readers. The target implementation date is December 31, 2015.

Regarding recommendation 3, management stated that only one person has access to both the accounting and storage rooms; however, to increase security around the DVR in the storage room, management will place the surveillance equipment in a tamper-proof cabinet. The target implementation date is December 31, 2015.

Regarding recommendation 4, management stated that a QSA has already completed a review of the NCSC for 2015 and that the NCSC will be reviewed again in 2016.

See Appendix A for management's comments, in their entirety.

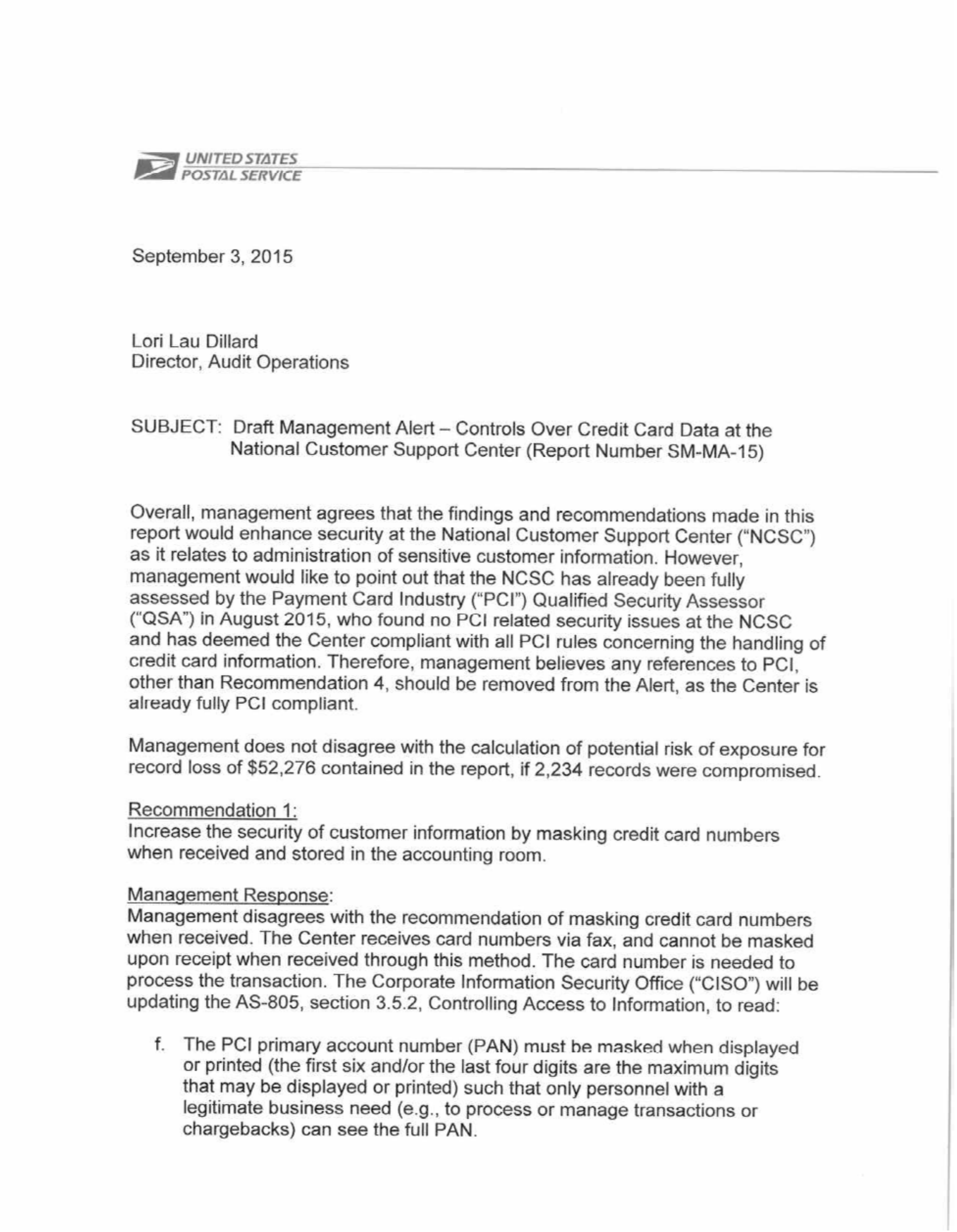
Evaluation of Management's Comments

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

Regarding references to PCI in this alert, management notified the OIG in a meeting subsequent to our fieldwork that a PCI review was in process and a QSA determined that the NCSC complied with PCI standards. Management did not provide the details of that review, as requested. Without this information, the OIG cannot assess the scope of the PCI controls tested. Based on our assessment, we determined that using PCI criteria was appropriate for the purpose of this alert. Therefore, we do not intend to remove any references to PCI.

The OIG considers all of the recommendations significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendix A. Management's Comments



UNITED STATES
POSTAL SERVICE

September 3, 2015

Lori Lau Dillard
Director, Audit Operations

SUBJECT: Draft Management Alert – Controls Over Credit Card Data at the National Customer Support Center (Report Number SM-MA-15)

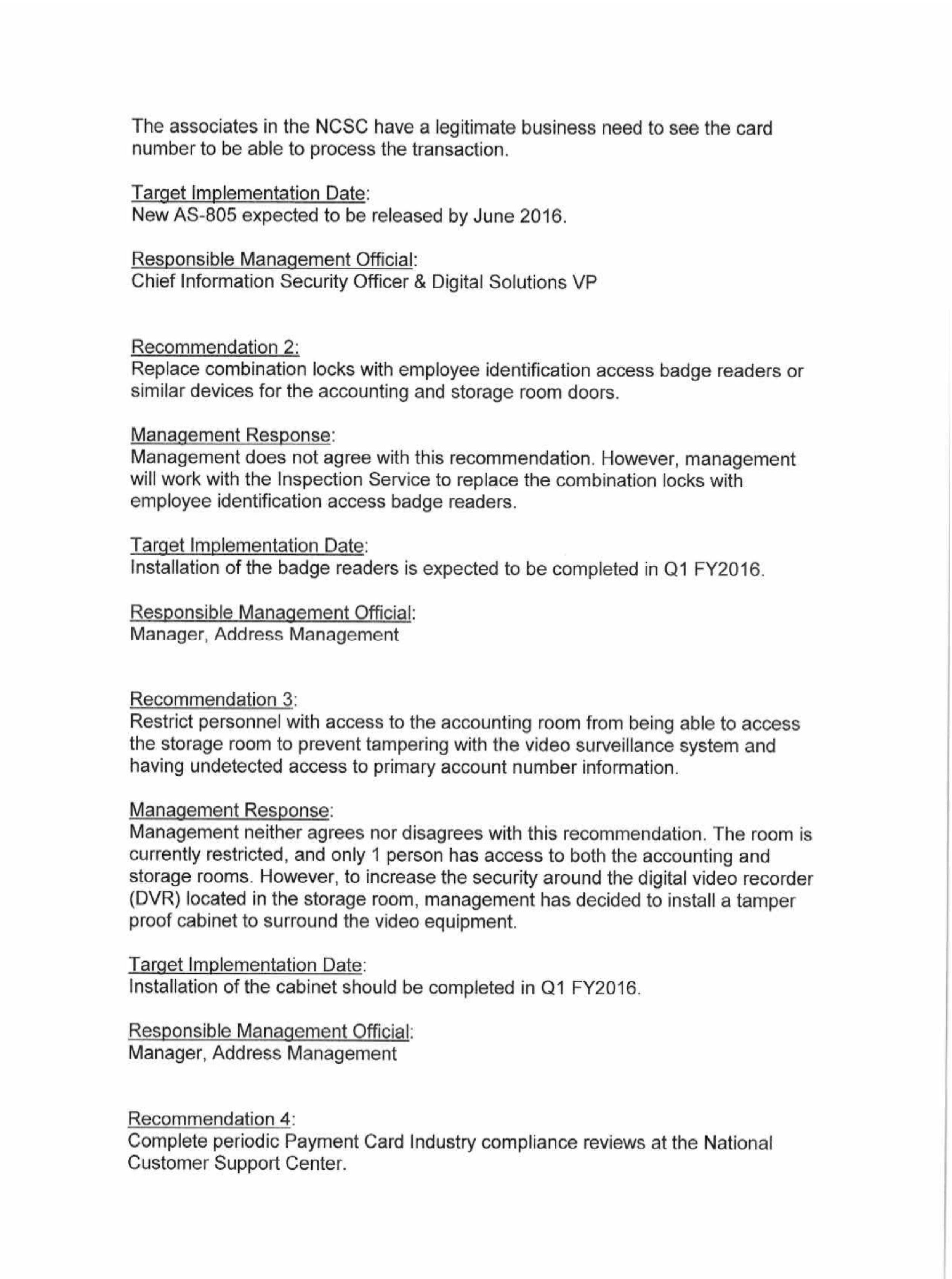
Overall, management agrees that the findings and recommendations made in this report would enhance security at the National Customer Support Center ("NCSC") as it relates to administration of sensitive customer information. However, management would like to point out that the NCSC has already been fully assessed by the Payment Card Industry ("PCI") Qualified Security Assessor ("QSA") in August 2015, who found no PCI related security issues at the NCSC and has deemed the Center compliant with all PCI rules concerning the handling of credit card information. Therefore, management believes any references to PCI, other than Recommendation 4, should be removed from the Alert, as the Center is already fully PCI compliant.

Management does not disagree with the calculation of potential risk of exposure for record loss of $52,276 contained in the report, if 2,234 records were compromised.

Recommendation 1:
Increase the security of customer information by masking credit card numbers when received and stored in the accounting room.

Management Response:
Management disagrees with the recommendation of masking credit card numbers when received. The Center receives card numbers via fax, and cannot be masked upon receipt when received through this method. The card number is needed to process the transaction. The Corporate Information Security Office ("CISO") will be updating the AS-805, section 3.5.2, Controlling Access to Information, to read:

f. The PCI primary account number (PAN) must be masked when displayed or printed (the first six and/or the last four digits are the maximum digits that may be displayed or printed) such that only personnel with a legitimate business need (e.g., to process or manage transactions or chargebacks) can see the full PAN.



The associates in the NCSC have a legitimate business need to see the card number to be able to process the transaction.

Target Implementation Date:
New AS-805 expected to be released by June 2016.

Responsible Management Official:
Chief Information Security Officer & Digital Solutions VP

Recommendation 2:
Replace combination locks with employee identification access badge readers or similar devices for the accounting and storage room doors.

Management Response:
Management does not agree with this recommendation. However, management will work with the Inspection Service to replace the combination locks with employee identification access badge readers.

Target Implementation Date:
Installation of the badge readers is expected to be completed in Q1 FY2016.

Responsible Management Official:
Manager, Address Management

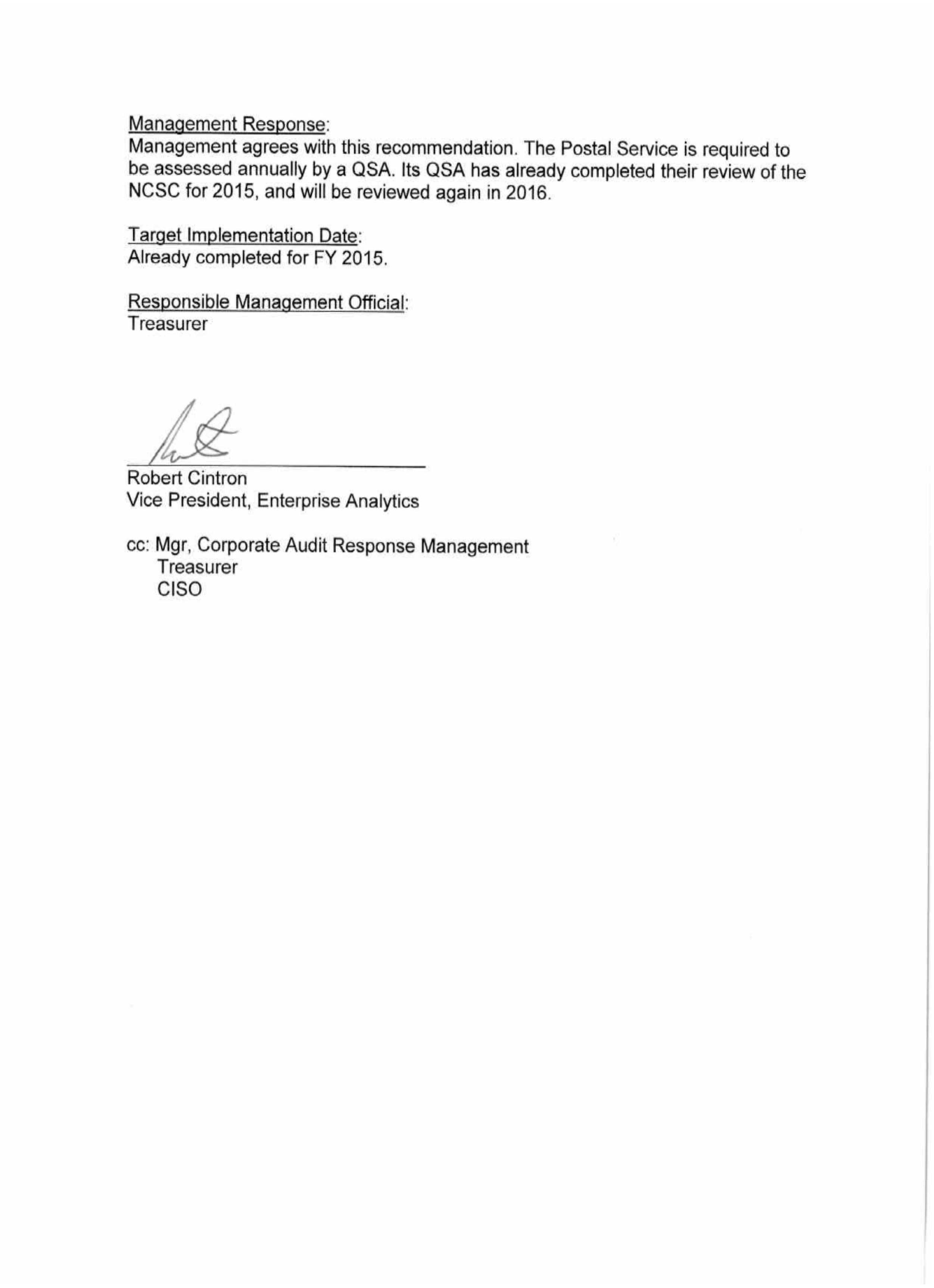
Recommendation 3:
Restrict personnel with access to the accounting room from being able to access the storage room to prevent tampering with the video surveillance system and having undetected access to primary account number information.

Management Response:
Management neither agrees nor disagrees with this recommendation. The room is currently restricted, and only 1 person has access to both the accounting and storage rooms. However, to increase the security around the digital video recorder (DVR) located in the storage room, management has decided to install a tamper proof cabinet to surround the video equipment.

Target Implementation Date:
Installation of the cabinet should be completed in Q1 FY2016.

Responsible Management Official:
Manager, Address Management

Recommendation 4:
Complete periodic Payment Card Industry compliance reviews at the National Customer Support Center.



Management Response:
Management agrees with this recommendation. The Postal Service is required to be assessed annually by a QSA. Its QSA has already completed their review of the NCSC for 2015, and will be reviewed again in 2016.

Target Implementation Date:
Already completed for FY 2015.

Responsible Management Official:
Treasurer

Robert Cintron
Vice President, Enterprise Analytics

cc: Mgr, Corporate Audit Response Management
Treasurer
CISO