OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 9, 2007

[redacted]
POSTMASTER, [redacted], [redacted]

SUBJECT: Audit Report – Voyager Card Program – [redacted] [redacted] [redacted]
Branches [redacted] [redacted] [redacted], [redacted] Post Office
(Report Number CA-AR-07-006)

This report presents the results of our Voyager Card audit at the [redacted] and [redacted] [redacted] Branches of the [redacted], [redacted] Post Office (Project Number 06YG043CA000). The Postmaster General requested we review the Postal Service's Voyager Card program, and the information in this report may be included in a nationwide capping report assessing Voyager Card controls and transactions.

Background

U.S. Postal Service employees use the Voyager Card like a credit card to pay for fuel, repairs, and maintenance for Postal Service vehicles. The government-wide General Services Administration SmartPay program administers Voyager Cards to simplify payment for vehicle fuel and service. The SmartPay contractor for the Postal Service is U.S. Bank Voyager Fleet Systems, Incorporated, or simply Voyager. The Postal Service began using Voyager in January 2000, and as of September 2006, had issued approximately 250,000 cards service-wide. In fiscal year 2006, there were approximately 9.8 million Voyager Card transactions nationwide totaling about $403.2 million.

Management assigns each Postal Service vehicle its own Voyager Card with the vehicle number listed on the front of the card. Management also issues each vehicle operator their own unique personal identification number (PIN) which they can use to authorize purchases on any Voyager Card.

Each facility with Postal Service-owned vehicles has a designated site manager. The site manager is responsible for assuring that someone at the site has access to the eFleet Card System (eFCS) and is familiar with the Voyager Card reconciliation process. Once a month, the site manager or other designated party is required to reconcile accounts online in the eFCS. This involves matching receipts against the invoice report displayed in the eFCS. After the online reconciliation is complete, the invoice report must be printed from the eFCS and filed with all supporting receipts for a 2-year period.

Objectives, Scope, and Methodology

Our overall audit objective was to determine whether the Postal Service implemented effective controls for Voyager Card use. Specifically, we determined whether managers established appropriate card procedures, reviewed and reconciled accounts monthly, and properly investigated and resolved questionable transactions. Additionally, we determined the propriety of Voyager Card purchases.

To accomplish our objectives, we reviewed Postal Service Voyager Card policies and procedures. In conjunction with the Postal Service Internal Control Group, we made site visits to the [redacted] and [redacted] [redacted] Branches of the [redacted], [redacted] Post Office to review controls over the Voyager Card. During our site visits, we interviewed managers and employees, observed operations, and tested security controls over Voyager Cards and PINs. We also reviewed supporting documentation for judgmentally selected Voyager Card transactions.[1]

We conducted this audit from November 2006 through July 2007 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. We discussed the results of our observations and conclusions with management officials on November 30, 2006, and included their comments where appropriate. We used data generated from the eFCS, but did not rely on the information in the system to support our findings. We obtained source documentation that validated the data we used from the system.

Prior Audit Coverage

The U.S. Postal Service Office of Inspector General (OIG) issued the following three reports on Voyager Cards:

Voyager Card Control Weaknesses – Chicago (Report Number TD-AR-02-004, dated September 26, 2002) and *Voyager Card Control Weaknesses – San Antonio District* (Report Number TD-AR-03-003, dated December 2, 2002) concluded that controls in these districts did not protect the Postal Service from improper, fraudulent, or questionable use of the Voyager Card. Our site visits to Postal Service facilities in these districts revealed that management did not properly protect or segregate cards and PINs, keep accurate card and PIN inventories, or cancel cards and PINs when necessary; cards were missing or lost; employees made unauthorized and questionable

[1] At each site, we reviewed transactions that occurred in November 2005, and February, May, August, and October 2006. For each of those months, we judgmentally selected a Voyager Card and reviewed all associated card activity.

transactions; and site managers did not reconcile accounts. We made two recommendations to management to address the issues we identified in each of our reports. Management agreed with all of our findings and recommendations in both reports.

Voyager Card Control Weaknesses – National Analysis (Report Number TD-AR-03-012, dated September 8, 2003) revealed that from September 2000 until March 2002, the Postal Service incurred more than $1.1 million in unnecessary food and premium fuel costs. In addition, the report identified at least $42 million in other questionable transactions. The transactions included miscellaneous purchases, multiple fuel purchases on the same day for the same vehicle, fuel purchases exceeding tank capacity, and purchases exceeding the $250 individual daily purchase limit. The Postal Service incurred these unnecessary and questionable costs because management did not protect Voyager Cards and PINs or properly segregate responsibility for purchase authorization and review. In addition, questionable purchases were not recognized, investigated, or disputed because site managers did not reconcile accounts. We made one recommendation to management to address the issues identified in our report. Management agreed with the recommendation but disagreed with our assessment of monetary impact. Management said the system of control was too unreliable to provide a reasonable basis for estimating monetary impact.

Results

Voyager Card Control Weaknesses at the [redacted] and [redacted] [redacted] Branches of the [redacted] Post Office

Managers at the [redacted] and [redacted] [redacted] Branches of the [redacted] Post Office did not always follow Voyager Card policies and procedures. Specifically, we identified control weaknesses in:

- Training
- Voyager Card security
- PIN security
- Missing receipts and documentation
- Organization of the files
- Vehicle numbers

These control weaknesses occurred because managers responsible for the Voyager Card program had other duties that took priority or they were unaware of the requirements. Although we did not identify any fraudulent transactions,[2] control weaknesses increased the risk of Voyager Card fraud or abuse at the [redacted] and [redacted] [redacted] Branches.

[2] We did not identify fraudulent transactions; however, we were not able to locate receipts to support seven transactions included in our samples.

Training. The site managers responsible for performing the monthly reconciliation at the [redacted] and [redacted] [redacted] Branches had not taken the required online Voyager Card training. This occurred because individuals were not aware of the training requirement. According to Postal Service policy, any individual responsible for reconciling Voyager Card activities is required to take this training. We brought this to the attention of management at both branches and recommend both branches use the online training available to address this issue.

Voyager Card Security. Management did not adequately secure Voyager Cards when they were not being used at the [redacted] and [redacted] [redacted] Branches. At the [redacted] Branch, management locked Voyager Cards in a cage; however, the location of the key to the cage was known throughout the post office. At the [redacted] [redacted] Branch, Voyager Cards were left unattended and out in the open during the day. In addition, the Z Card[3] was not adequately secured at the [redacted] [redacted] Branch. The Z Card was maintained in the Customer Service supervisor's desk drawer, which is kept unlocked and available for all employees to access. According to Postal Service policy, the site manager is responsible for maintaining security over Voyager Cards. The guidance further states that Voyager Cards should not be left in locations with unrestricted access. We brought these situations to the attention of management at both branches and they agreed to better safeguard card access.

PIN Security. PINs were written on the back of one of 23 Voyager Cards reviewed at the [redacted] Branch and one of 51 Voyager Cards reviewed at the [redacted] [redacted] Branch. At the [redacted] Branch, the mail carrier did not know this was against policy. Employees should memorize PINs and keep them private and secure, and should never write PINs on the Voyager Card. Branch management immediately agreed to obscure the PIN from view on the back of the card when we brought the issue to their attention.

Additionally, master PIN lists were not current at the [redacted] and [redacted] [redacted] Branches. PINs were maintained for individuals who were no longer employed by the Postal Service or were no longer assigned to one of the affected branches. Specifically, at the [redacted] Branch, seven of 57 individuals on the master PIN list had active PINs but were no longer assigned to the branch.[4] In addition, one employee had two active PINs. At the [redacted] [redacted] Branch, 21 of 87 individuals on the master PIN list had active PINs but were no longer assigned to the branch.[5] This occurred at both branches because managers had other duties that took priority over maintaining the PIN lists. According to Postal Service policy, site managers must notify Voyager when a driver is no longer assigned to their site or when a driver needs to be added to the roster. Postal Service policy further states that if an employee leaves the Postal Service, management must notify Voyager to cancel that employee's PIN.

[3] Z Cards are issued to the finance number of the site and are used to pay for washing numerous Postal Service vehicles at the same time and to temporarily pay for fuel or repairs for vehicles with lost, stolen or damaged cards.
[4] One of the seven individuals no longer worked for the Postal Service.
[5] Three of the 21 individuals no longer worked for the Postal Service.

Furthermore, management did not adequately secure the master PIN list at the [redacted] [redacted] Branch. The master PIN list was maintained on a shared drive where access was not limited. The manager did not realize the shared drive was not an appropriate place to store the master PIN list. According to Postal Service policy, the site manager is responsible for maintaining the site's PIN list and is responsible for its security.

Missing Receipts and Documentation. Receipts and documentation were not always maintained for Voyager Card purchases. This occurred at both branches because files were poorly organized and, as a result, receipts may have been lost or misplaced. Specifically, [redacted] Branch personnel did not maintain receipts for six of the 42 transactions reviewed. All six of these transactions were identified as questionable transactions[6] in the eFCS. According to the site manager, the drivers were questioned about the transactions and management determined the transactions were legitimate. However, the determinations were not annotated in the files, as required. In addition, supporting documentation was not maintained for transactions occurring in May and July of 2005.

[redacted] [redacted] Branch personnel did not maintain receipts for one of the 49 transactions we reviewed. In addition, invoice reports were not printed from the eFCS and maintained with supporting documentation as required. This occurred because the manager was unaware of the requirement to print the invoice report. According to Postal Service policy, a receipt or invoice must accompany every card purchase. In each instance where a receipt is not available, the manager must contact the appropriate individual to determine why there is no receipt, investigate the particular transaction to determine if it is a legitimate purchase or one which indicates potential fraud, document the results of their determination, and retain the documentation for 2 years. Furthermore, site managers or other responsible parties are required to reconcile accounts online monthly, print the invoice report, and file with all receipts and invoices for a 2-year period.

Organization of the Files. Voyager Card files at the [redacted] and [redacted] [redacted] Branches were not well organized. Receipts were generally thrown together in boxes and were not always in order. We could not determine if managers had properly reconciled Voyager Card transactions because of the inadequate recordkeeping. Managers did not always have time to organize the Voyager Card files because other duties took priority. Postal Service policy recommends management use an accordion-style file folder, large enough to contain every receipt and invoice generated by vehicles in the office for an entire month. The file can be arranged by vehicle number or day of the month. Every month, management can bundle the receipts together and place them in a suitable file folder for the 2-year retention period.

[6] The eFCS identifies certain transactions as questionable. Examples of questionable transactions include premium fuel purchases, food purchases, and number of gallons purchased exceeds tank capacity.

<u>Vehicle Numbers.</u> Employees did not always write vehicle numbers on receipts at the [redacted] and [redacted] [redacted] Branches. Below is an example of a receipt that did not have the vehicle number written on it.

Redacted

At both branches, sites managers were aware of the requirement to write vehicle numbers on receipts but did not enforce the policy because other duties took priority. Postal Service policy requires the vehicle number to be written on all receipts and invoices for tracking purposes.

Recommendation

We recommend the Postmaster, [redacted] [redacted] [redacted]:

1. Ensure that managers at the [redacted] and [redacted] [redacted] Branches are aware of and follow Voyager Card policies and procedures specified by the *Site Fleet Card Guide* for the United States Postal Service and the *Fleet Card Standard Operating Procedures Handbook*.

Management's Comments

Management's comments reflected agreement with our recommendation. They instructed managers at the [redacted] and [redacted] [redacted] Branches to review and follow the policies and procedures contained in the two referenced documents. Management's comments, in their entirety, are included in the appendix of this report**.**

Evaluation of Management's Comments

Management's comments are responsive to the recommendation. Management's actions taken should correct the issues identified in the finding.

Recommendation

We recommend the Postmaster, [redacted] [redacted] [redacted]:

2. Direct the managers responsible for Voyager at the [redacted] and [redacted] [redacted] Branches to:

    - Take the required online Voyager training class.
    - Adequately secure Voyager and Z Cards.
    - Ensure personal identification numbers are kept private and secure.
    - Maintain a current master personal identification number list.
    - Maintain receipts and supporting documentation for 2 years.
    - Properly annotate the file in instances where receipts are not available.
    - Maintain organized Voyager files.
    - Ensure vehicle numbers are written on receipts.

Management's Comments

Management's comments reflected agreement with our recommendation. Management took or planned corrective actions to address control weaknesses in training, Voyager Card security, PIN security, missing receipts and documentation, organization of the files, and vehicle numbers. Specifically, management took or planned the following actions:

Training - Supervisors at the [redacted] and [redacted] [redacted] Branches took the online Voyager Card training in May 2007. The manager at the [redacted] [redacted] took the training in June 2007, and the manager at the [redacted] Branch is planning to take the training in July 2007.

Voyager Card security – In May 2007, the [redacted] Branch began locking Voyager cards in the accountable cart, which is inside the cage, and access to the key is secured. In addition, in May 2007, the [redacted] [redacted] Branch began securing Voyager cards in a cabinet inside the cage. In June 2007, the branch placed a work order for a lock for the cabinet.

PIN security – In May 2007**,** management instructed employees at both branches to never write PINs on Voyager Cards and to memorize their PINs and keep them private and secure. In addition, in June 2007, both branches updated the master PIN lists by removing individuals who no longer worked for the Postal Service or were no longer assigned to one of the affected branches. In May 2007, the [redacted] [redacted] Branch removed the master PIN list from the shared drive and placed it in the manager's personal files. Also, in June 2007, management instructed managers at both branches that they were responsible for maintaining the site's PIN list and its security.

Missing receipts and documentation – In June 2007**,** management instructed managers at both branches that every card purchase must have a receipt or invoice. They were further instructed that, if a purchase does not have a receipt, they must contact the appropriate individual to determine why there is no receipt, investigate the particular transaction to determine if it is a legitimate purchase or one that indicates potential fraud, document the results of their determination, and retain the documentation for 2 years.

Organization of the files - In May 2007**,** both branches developed better filing systems for maintaining receipts.

Vehicle numbers – In May 2007, managers at both branches talked with all employees about the requirement to write vehicle numbers on receipts. The branches will also perform reviews to ensure compliance.

Evaluation of Management's Comments

Management's comments are responsive to the recommendation. Management's actions taken or planned should correct the issues identified in the finding.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Judy Leonhardt, Director, Supply Management or me at (703) 248-2100.

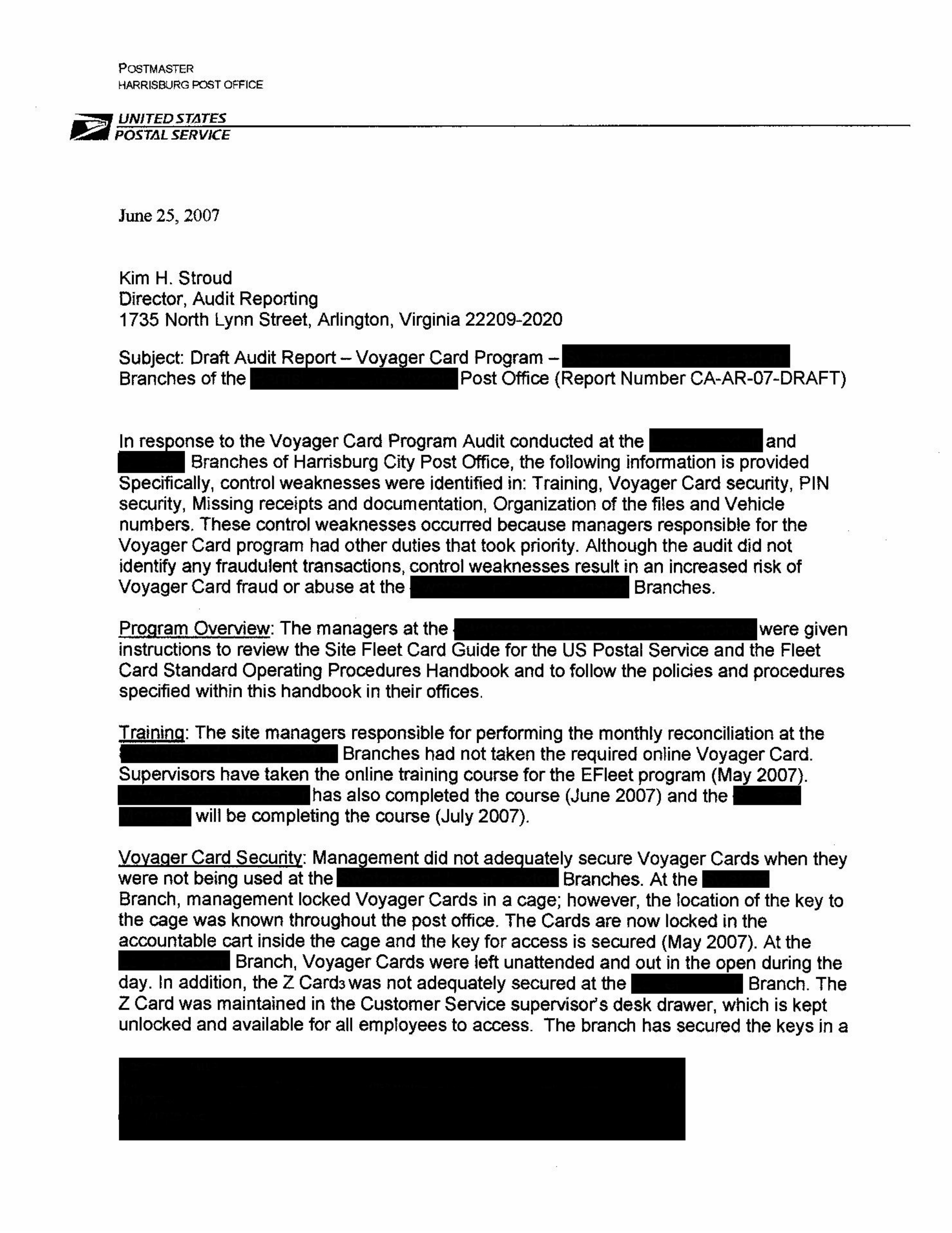
E-Signed by Darrell E. Benjamin, ?
VERIFY authenticity with ApproveIt

Darrell E. Benjamin, Jr.
Deputy Assistant Inspector General
for Support Operations

Attachment

cc: H. Glen Walker
Susan M. Brownell
Katherine S. Banks

APPENDIX. MANAGEMENT'S COMMENTS



POSTMASTER
HARRISBURG POST OFFICE

UNITED STATES
POSTAL SERVICE

June 25, 2007

Kim H. Stroud
Director, Audit Reporting
1735 North Lynn Street, Arlington, Virginia 22209-2020

Subject: Draft Audit Report – Voyager Card Program – [redacted]
Branches of the [redacted] Post Office (Report Number CA-AR-07-DRAFT)

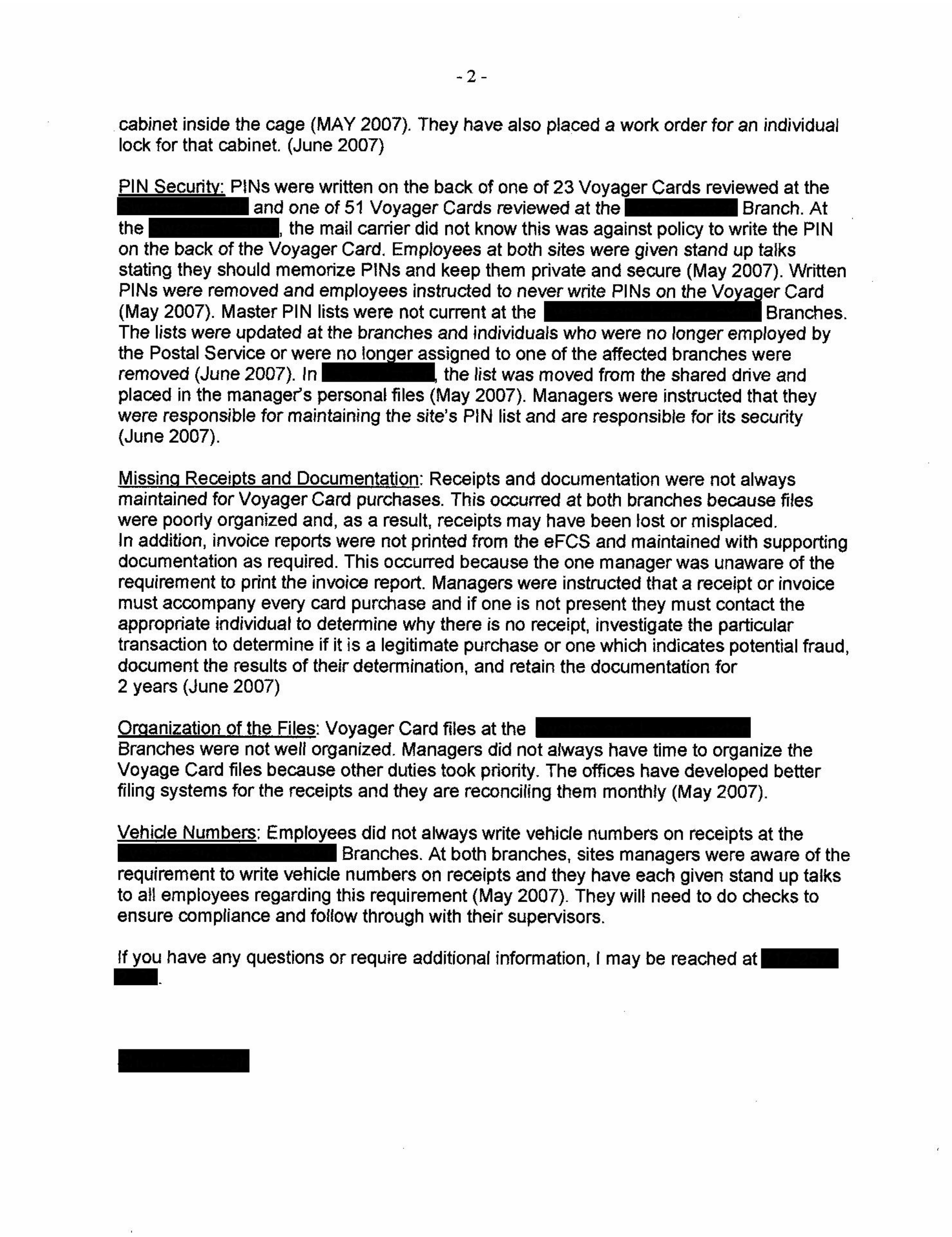
In response to the Voyager Card Program Audit conducted at the [redacted] and [redacted] Branches of Harrisburg City Post Office, the following information is provided Specifically, control weaknesses were identified in: Training, Voyager Card security, PIN security, Missing receipts and documentation, Organization of the files and Vehicle numbers. These control weaknesses occurred because managers responsible for the Voyager Card program had other duties that took priority. Although the audit did not identify any fraudulent transactions, control weaknesses result in an increased risk of Voyager Card fraud or abuse at the [redacted] Branches.

Program Overview: The managers at the [redacted] were given instructions to review the Site Fleet Card Guide for the US Postal Service and the Fleet Card Standard Operating Procedures Handbook and to follow the policies and procedures specified within this handbook in their offices.

Training: The site managers responsible for performing the monthly reconciliation at the [redacted] Branches had not taken the required online Voyager Card. Supervisors have taken the online training course for the EFleet program (May 2007). [redacted] has also completed the course (June 2007) and the [redacted] will be completing the course (July 2007).

Voyager Card Security: Management did not adequately secure Voyager Cards when they were not being used at the [redacted] Branches. At the [redacted] Branch, management locked Voyager Cards in a cage; however, the location of the key to the cage was known throughout the post office. The Cards are now locked in the accountable cart inside the cage and the key for access is secured (May 2007). At the [redacted] Branch, Voyager Cards were left unattended and out in the open during the day. In addition, the Z Card[3] was not adequately secured at the [redacted] Branch. The Z Card was maintained in the Customer Service supervisor's desk drawer, which is kept unlocked and available for all employees to access. The branch has secured the keys in a

[redacted]



cabinet inside the cage (MAY 2007). They have also placed a work order for an individual lock for that cabinet. (June 2007)

PIN Security: PINs were written on the back of one of 23 Voyager Cards reviewed at the [redacted] and one of 51 Voyager Cards reviewed at the [redacted] Branch. At the [redacted], the mail carrier did not know this was against policy to write the PIN on the back of the Voyager Card. Employees at both sites were given stand up talks stating they should memorize PINs and keep them private and secure (May 2007). Written PINs were removed and employees instructed to never write PINs on the Voyager Card (May 2007). Master PIN lists were not current at the [redacted] Branches. The lists were updated at the branches and individuals who were no longer employed by the Postal Service or were no longer assigned to one of the affected branches were removed (June 2007). In [redacted], the list was moved from the shared drive and placed in the manager's personal files (May 2007). Managers were instructed that they were responsible for maintaining the site's PIN list and are responsible for its security (June 2007).

Missing Receipts and Documentation: Receipts and documentation were not always maintained for Voyager Card purchases. This occurred at both branches because files were poorly organized and, as a result, receipts may have been lost or misplaced.
In addition, invoice reports were not printed from the eFCS and maintained with supporting documentation as required. This occurred because the one manager was unaware of the requirement to print the invoice report. Managers were instructed that a receipt or invoice must accompany every card purchase and if one is not present they must contact the appropriate individual to determine why there is no receipt, investigate the particular transaction to determine if it is a legitimate purchase or one which indicates potential fraud, document the results of their determination, and retain the documentation for 2 years (June 2007)

Organization of the Files: Voyager Card files at the [redacted] Branches were not well organized. Managers did not always have time to organize the Voyage Card files because other duties took priority. The offices have developed better filing systems for the receipts and they are reconciling them monthly (May 2007).

Vehicle Numbers: Employees did not always write vehicle numbers on receipts at the [redacted] Branches. At both branches, sites managers were aware of the requirement to write vehicle numbers on receipts and they have each given stand up talks to all employees regarding this requirement (May 2007). They will need to do checks to ensure compliance and follow through with their supervisors.

If you have any questions or require additional information, I may be reached at [redacted].

[redacted]

- 3 -

[redacted]