Table of Contents

Highlights

Objective

Our objective was to assess the effectiveness of the U.S. Postal Service's management controls for Voyager Fleet Card (Voyager card) Personal Identification Numbers (PIN) nationwide. Voyager Fleet Systems Inc., owned by U.S. Bank, issues the Voyager cards and PINs.

The Postal Service operates one of the largest vehicle fleets in the U.S. and used 229,682 vehicles in fiscal year (FY) 2018 primarily to deliver and collect mail. The Postal Service does not issue Voyager cards to employees, but assigns the cards to vehicles, delivery units, and vehicle maintenance facilities (VMF). Postal Service employees use these cards to purchase fuel, oil, and maintenance services from external commercial businesses (vendors) either ███████████ ███████████. Postal Service policy requires employees to enter a PIN to complete a Voyager card purchase. The PIN identifies the Postal Service employee authorizing the purchase.

Site managers assign PINs to new employees or employees who have transferred into a unit and who are responsible for purchasing fuel (such as drivers) or paying for maintenance (such as VMF clerks and site managers). ██ ███ ███ ███████████████████████████████████████ Postal Service policy provides guidance over the assignment, use, and monitoring of PINs. For example:

- Only Postal Service employees are assigned a PIN – a vendor cannot be assigned a PIN.

- Voyager cards and PINs each have limits of $300 per day, three transactions per day, and $1,000 per month.

- Site managers are required to contact the VMF if they require PIN increases above established limits. These requests must be authorized and processed by the responsible VMF manager or their designee by ███████████ ███ ████████████████████

- Site managers are required to conduct a semiannual review to verify that PIN information is accurate and complete.

- Site managers must terminate an ███████████████████████████ ███████████████████████████████████ when an employee leaves the Postal Service, transfers to a new location, or retires.

Our audit focused on the 423,681 active PINs for mail delivery and collection operations as of July 2018. Employees made purchases totaling $627 million in FY 2018 using these PINs.

What the OIG Found

Controls over Voyager PINs are ineffective nationwide. Our analysis of 423,681 active PINs in mail delivery and collection operations showed that site managers:

- Inappropriately assigned 651 PINs to vendors who made 321,586 purchases totaling $30,672,985.

- Failed to deactivate 18,697 PINs for employees assigned more than one PIN, transferred to another unit, or no longer employed at the Postal Service. These PINs were used to make 314,962 purchases totaling $15,454,663.

- Did not assign an employee name to 776 PINs which were used for purchases totaling $188,391.

- PINs with no assigned name do not identify the individual authorizing the purchase, only the finance number of the facility where the PIN was issued.

We also identified 7,326 PIN limits which exceeded the authorized purchase limit of $1,000 per month. Because documentation to support approvals to exceed authorized limits is maintained at local VMFs across the country and not electronically, we selected a judgmental sample of 49 PINs to verify if management approved these increased limits. We found that 10 PINs were

approved for increased purchase limits, but management did not respond to or provide supporting documentation for the remaining 39 PINs sampled. We made referrals to our Office of Investigations, as appropriate.

These conditions occurred and were not detected because of a lack of automated controls and ineffective management oversight. We noted:

- The Voyager FCO application the Postal Service uses to manage PINs did not include automated controls to prevent vendors from receiving PINs, assigning PINs to employees who already had PINs, and PINs without valid employee names. Further, controls did not exist for Voyager to authenticate Postal Service officials who were authorized to increase PIN limits.

- Site managers did not always comply with the requirements in the *Voyager Fleet Card Standard Operating Procedures* (SOP), including completion of required semiannual reviews – the primary method of oversight that identifies the issues identified in this report. We could not quantify the number of reviews that were conducted because the Postal Service did not have a mechanism to track and monitor completion of these reviews.

The absence of these controls and ineffective oversight increased the risk of improper and unauthorized purchases and resulted in about $46 million in questioned costs for FY 2018.

> " *These conditions occurred and were not detected because of a lack of automated controls and ineffective management oversight.* "

What the OIG Recommended

We recommended the Vice President, Controller:

- Coordinate with U.S. Bank Voyager to implement automated controls in the Voyager Fleet Commander Online application to: (1) prevent assignment of PINs to vendors, (2) prevent assignment of multiple PINs to employees, (3) prevent assignment of PINs without valid employee names, and (4) ensure only authorized employees are allowed to request PIN limit changes.

We recommended the Vice President, Delivery & Retail Operations:

- Implement corrective action to: (1) deactivate PINs issued to vendors, (2) deactivate multiple PINs issued to employees or define policy exceptions for multiple PINs, (3) deactivate PINs without a valid employee name, (4) ensure authorized approval of requests for increasing PIN purchasing limits, and (5) track and monitor completion of semiannual reviews.

- Develop and implement interim controls to prevent and detect the issues noted in this report until the Postal Service updates the Voyager Fleet Commander Online application.

- Reinforce to site managers, VMF managers and their designees to follow the requirements in the *Voyager Fleet Card SOP* for issuing PINs, requesting PIN limit increases, and conducting semiannual reviews.

Transmittal Letter

June 24, 2019

MEMORANDUM FOR: CARA M. GREENE
VICE PRESIDENT, CONTROLLER

KEVIN L. MCADAMS
VICE PRESIDENT, DELIVERY & RETAIL OPERATIONS

Janet Sorensen

FROM: Janet M. Sorensen
Deputy Assistant Inspector General
 for Retail, Delivery, & Marketing

SUBJECT: Audit Report – Nationwide Review of Voyager Fleet Card
Personal Identification Numbers
(Report Number DR-AR-19-006)

This report presents the results of our audit of Voyager Fleet Card Personal Identification Numbers (Project Number 18RG015DR000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Rita F. Oliver, Director, Delivery and Retail Operations, or me at 703-248-2100.

Attachment

cc: Corporate Audit Response Management
    Postmaster General

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the Voyager Fleet Card Personal Identification Numbers (PIN) (Project Number 18RG015DR000). Our objective was to assess the effectiveness of the U.S. Postal Service's management controls for Voyager Fleet Card (Voyager card) PINs nationwide.

Background

The Postal Service operates one of the largest vehicle fleets in the U.S. and used 229,682 vehicles[1] in fiscal year (FY) 2018, primarily to deliver and collect mail. The Postal Service has been part of the government commercial card program under the General Services Administration's SmartPay® Program since 2000. The Postal Service's fleet card program is co-sponsored by Headquarters Supply Management, Finance, and Fleet Management. Voyager Fleet Systems Inc., owned by U.S. Bank, issues Voyager cards and PINs.[2]

Postal Service Voyager cards are not issued to employees, instead the cards are assigned to vehicles, delivery units, and vehicle maintenance facilities (VMF). Postal Service employees use these cards for fuel, oil, and maintenance purchases from external commercial businesses (vendors) ███████████ ███████████████. Postal Service policy requires employees to enter a PIN to complete a Voyager card purchase. This PIN identifies the Postal Service employee authorizing the purchase.

Site managers assign PINs to new employees or employees who have transferred into a unit and who are responsible for purchasing fuel (such as drivers) or paying for maintenance services (such as VMF clerks and site managers). ████████████████████████████████ ████████████████████████████████ ████████████████████████████████

████████████████████████████████ ██████

Controls over PINs are crucial in maintaining the integrity of the program to control costs. Postal Service policy provides guidance over the assignment, use, and monitoring of PINs.

For example:

- Only Postal Service employees are assigned a PIN – a vendor cannot be assigned a PIN.

- Voyager cards and PINs each have limits of $300 per day, three transactions per day, and $1,000 per month.

- Site managers are required to contact the VMF if they require PIN increases above established limits. These requests must be authorized and processed by the responsible VMF manager or their designee ████████████ ████████████████████████████████ ███████████████.

- Site managers are required to conduct a semiannual review to verify that PIN information is accurate and complete.

- Site managers must terminate an ███████████████████████ ████████████████████████████████ when an employee leaves the Postal Service, transfers to a new location, or retires.

As of July 2018, Voyager had issued the Postal Service 480,861 Voyager cards, with 602,476 active PINs, with our audit focusing on the 423,681 PINs used for mail delivery and collection operations. Employees made $627 million in Voyager card purchases in FY 2018 (see Table 1).

---

1   This also includes vehicles used for mail transport, administrative, and other service vehicles but does not include Inspection Service and other law enforcement.

2   ██

█

Table 1: FY 2018 Voyager Card Statistics

Area	FY 2018 Purchases	Total Number of Cards Issued	Total Number of Active PINs	Total Number of Active Delivery and Collection PINs
Capital Metro	$81,830,951	46,625	71,218	49,913
Eastern	101,766,122	36,819	94,479	67,764
Great Lakes	79,573,254	32,731	68,700	49,832
Northeast	93,572,152	33,461	83,833	56,970
Pacific	68,272,005	30,437	73,162	51,527
Southern	111,536,353	262,787	111,755	80,513
Western	90,619,805	38,001	99,329	67,162
Total	**$627,170,642**	**480,861**	**602,476**	**423,681**

Source: U.S. Postal Service Office of Inspector General (OIG) analysis of FCO.

Finding #1: Ineffective Internal Controls Over Personal Identification Numbers

Controls over Voyager PINs were ineffective nationwide. Our analysis of 423,681 active PINs in mail delivery and collection operations showed that site managers:

- Inappropriately assigned 651 PINs to vendors who made 321,586 purchases totaling $30,672,985.

- Failed to deactivate 18,697 PINs for employees assigned more than one PIN, transferred to another unit, or no longer employed at the Postal Service. These PINs were used to make 314,962 purchases totaling $15,454,663.

- Did not assign a name to 776 PINs which were used for purchases totaling $188,391. PINs with no assigned name do not identify the individual authorizing the purchase, only the finance number of the facility where the PIN was issued.

We also identified 7,326 PIN limits which exceeded the authorized purchase limits of $1,000 per month. Because documentation to support approvals to exceed authorized limits is maintained at local VMFs across the country and not electronically, we selected a judgmental sample of 49 PINs to verify if management approved these increased limits. We found that 10 PINs were approved for increased purchase limits, but management did not respond to or provide supporting documentation for the remaining 39 PINs sampled. Of the 39 that were not approved, ███. We made referrals to our Office of Investigations, as appropriate.

"Controls over Voyager PINs were ineffective nationwide."

Vendors Assigned Dedicated Personal Identification Numbers

Site managers inappropriately assigned 651 PINs to vendors[4] who made 321,586 purchases totaling $30,672,985 during FY 2018. According to *Voyager Fleet Card Standard Operating Procedures* (SOP),[5] management is not to assign PINs to vendors. We noted that one vendor made 201 purchases totaling $444,897 with one PIN. We provided the results of our analysis to each Postal Service area, which took corrective action and deactivated 252 vendor PINs during our audit (see Table 2).

Table 2. Vendor PINs Assigned

Area	Active Vendor PINs	Number of Transactions	Total Purchases	Total Deactivated PINs
Capital Metro	77	8,369	$1,634,001	32
Eastern	179	17,266	1,550,588	55
Great Lakes	16	670	86,928	5
Northeast	78	9,136	1,336,767	13
Pacific	47	1,074	190,960	9
Southern	252	266,698	23,900,905	138
Western	2	18,373	1,972,836	0
Total	**651**	**321,586**	**$30,672,985**	**252**

Source: OIG analysis of FCO.

Multiple Personal Identification Numbers

Site managers failed to deactivate 18,697 PINs for employees assigned more than one PIN, transferred to another unit, or no longer employed at the Postal Service. These PINs were used to make 314,962 purchases totaled $15,454,663 in FY 2018. The OIG further analyzed individual PINs and identified five employees in three Postal Service areas that had more than 10 assigned PINs (see Table 3). One employee in the Northeast Area had 18 assigned PINs.

Table 3. Number of Employees with More than Ten PINs

Area	Number of Employees with More than Ten PINs	Number of PINs Assigned
Capital Metro	0	0
Eastern	1	14
Great Lakes	0	0
Northeast	3	41
Pacific	0	0
Southern	0	0
Western	1	14
Total	**5**	**69**

Source: OIG analysis of FCO.

Postal Service policy[6] requires site managers to terminate an employee's ███ ███ when an employee leaves the Postal Service, transfers to a new location, or retires.

We provided the results of our analysis to management in each Postal Service area, who took corrective action and deactivated 5,882 PINs during our audit for employees that were either removed, retired, or transferred to another location (see Table 4).

4 ██
5   *Voyager Fleet Card SOP*, Section 2.2.2, PIN Management, November 3, 2016.
6   *Voyager Fleet Card SOP*, Section 2.2.2, PIN Management, November 3, 2016.

Table 4. Multiple Assigned PINs

Area	Number of Multiple PINs	Number of Transactions	Total Purchases	Total Multiple PINs Deactivated
Capital Metro	4,862	94,239	$4,895,141	790
Eastern	636	11,371	576,898	161
Great Lakes	125	1,935	68,031	41
Northeast	5,688	69,415	4,078,347	1,561
Pacific	991	19,838	1,039,783	271
Southern	837	10,659	1,212,127	449
Western	5,558	107,505	3,584,336	2,609
Total	**18,697**	**314,962**	**$15,454,663**	**5,882**

Source: OIG analysis of FCO.

Table 5. PINs With No Driver Name Assigned

Area	Number of PINs with No Driver Name	Number of Transactions	Total Purchases	Deactivated PINs
Capital Metro	79	493	13,365	74
Eastern	81	739	21,872	66
Great Lakes	25	265	7,015	17
Northeast	231	1,796	84,201	179
Pacific	30	221	6,610	22
Southern	279	1,717	39,643	229
Western	51	516	15,685	48
Total	**776**	**5,747**	**$188,391**	**635**

Source: OIG analysis of FCO.

No Driver Names Assigned

Site managers did not assign employee names to 776 PINs, used for purchases totaling $188,391 in FY 2018. PINs with no assigned name do not identify the individual authorizing the purchase, only the finance number of the facility where the PIN was issued. Postal Service policy[7] requires site managers to supply Voyager with the employee name associated with each PIN.

We provided the results of our analysis to managers of each Postal Service area, who took corrective action and deactivated or deleted 635 PINs with no driver name assigned (see Table 5).

Personal Identification Numbers Over the Authorized Limits

We identified 7,326 PIN limits which exceeded the authorized purchase limits of $1,000 per month. Because documentation to support approvals to exceed authorized limits is maintained at local VMFs across the country and not electronically, we selected a judgmental sample of 49 PINs to verify if management approved these increased limits. We found that 10 PINs were approved for increased purchase limits. For the remaining 39, management did not respond or provide supporting documentation for the increased limits (see Appendix B).

> *"PINs with no assigned name do not identify the individual authorizing the purchase, only the facility finance number where the PIN was issued."*

---

7   *Voyager Fleet Card SOP,* Section 2.2.2, PIN Management, November 3, 2016.

Of these 39, ███ ███ ████████ Seven of the 39 PINs had spending limits of at least $300,000.[8] We estimated $660,439,515 at risk, representing PIN limits exceeding the Postal Service's monthly authorized PIN limit of $1,000[9] (see Table 6).

Table 6. PINs Over the Authorized Limit

Area	Employees with PINs Exceeding Authorized Limits	Unauthorized PIN Limit per Year	Total Amount at Risk
Capital Metro	190	$1,622,100	$14,806,549
Eastern	1,148	9,767,696	89,159,651
Great Lakes	1,456	16,409,500	149,786,120
Northeast	1,482	17,867,651	163,096,141
Pacific	1,289	9,380,600	85,626,234
Southern	405	7,175,400	65,497,141
Western	1,356	10,130,100	92,467,679
Total	**7,326**	**$72,353,047**	**$660,439,515**

Source: OIG analysis of FCO.

Postal Service policy[10] states that site managers are required to contact the VMF if they require PIN increases above the established limits. These requests must be authorized and processed by the responsible VMF manager or their designee ██ ██ ████████████████████████████████████

These conditions occurred and were not detected because of a lack of automated controls and ineffective management oversight. Specifically:

- The FCO application the Postal Service uses to manage PINs did not include automated controls to prevent vendors from receiving PINs, assignment of PINs to employees who already had a PIN, and assigning PINs without valid employee names. Further, controls did not exist for Voyager to authenticate Postal Service officials who were authorized to increase PIN limits. The U.S. Bank Postal Service account representative stated that FCO application controls were designed for the Voyager cards and *not* for the PINs. Because the Postal Service does not own this system, any application control changes to add PIN controls would require a software change in the FCO application.

---

8   We did not identify purchases exceeding the spending limits.
9   This is the calculated difference over the $1,000 monthly limit per Postal Service policy. We calculated assets at risk using the OIG risk assessment tool.
10 *Voyager Fleet Card SOP*, Section 2.2.1, Limit Changes, November 3, 2016.

- Site managers did not always comply with requirements in the *Voyager Fleet Card SOP* to include completing required semiannual reviews – the primary method of oversight to identify the issues identified in this report. We could not quantify the number of reviews that were not conducted because the Postal Service does not have a mechanism to track and monitor completion of these reviews. Previous audit work has identified that reviews were not always performed[11] and we noted in discussions with area management during this audit that these reviews were not conducted.

The absence of automated application controls and ineffective oversight increases the risk of improper and unauthorized purchases. As a result, we estimated the Postal Service incurred $46,316,039 in questioned costs for FY 2018. We also estimated $660,439,515 at risk, representing the PIN limits we found that were in excess of the Postal Service's monthly authorized PIN limits of $1,000.

Recommendation #1

We recommend the Vice President, Controller, coordinate with U.S. Bank Voyager to implement automated controls in the Voyager Fleet Commander Online application to (1) prevent assignment of multiple Personal Identification Numbers (PIN) to vendors, (2) prevent assignment of multiple PINs to employees, (3) prevent assignment of PINs without valid employee names, and (4) ensure only authorized employees are allowed to request PIN limit changes.

Recommendation #2

We recommend the Vice President, Delivery & Retail Operations, implement corrective action to (1) deactivate Personal Identification Numbers (PIN) issued to vendors, (2) deactivate multiple PINs issued to employees or define policy exceptions for multiple PINs, (3) deactivate PINs without a valid employee name, (4) ensure authorized approval of requests for increasing PIN purchasing limits, and (5) track and monitor completion of semiannual reviews.

Recommendation #3

We recommend the Vice President, Delivery & Retail Operations, develop and implement interim controls to prevent and detect the issues noted in this report until the Voyager Fleet Commander Online application is updated.

Recommendation #4

We recommend the Vice President, Delivery & Retail Operations, reinforce to site managers, VMF managers and their designees, follow the requirements in the *Voyager Fleet Card Standard Operating Procedures* for issuing multiple Personal Identification Numbers (PIN), requesting PIN limit increases, and conducting semiannual reviews.

---

11 *Fleet Specialty Card Management – Pacific Area* (Report Number DR-AR-18-009, dated July 17, 2018) and *Voyager Card Transactions – Roseburg, OR, Post Office* (Report Number FCS-FM-19-007, dated April 11, 2019).

Management's Comments

Management agreed with our finding and recommendations, but in subsequent correspondence disagreed with the monetary impact.

In response to recommendation 1, management agreed to coordinate with US Bank to implement automated controls in the Voyager Fleet Commander Online application to prevent the assignment of PINs to vendors, prevent the assignment of multiple PINs to employees, and prevent assignment of PINs without valid employee names. In addition, the Travel and Relocation office will work with US Bank and Postal Service Fleet Management to communicate the PIN limit policy and processes and ensure only authorized personnel are requesting PIN limit changes. The Travel and Relocation office will also work with US Bank to reinforce acceptance of PIN limit change requests submitted by authorized personnel only. Management's target implementation date is February 29, 2020.

In response to recommendation 2, management will clarify policy guidelines for the PIN naming convention to allow for the operational needs of multiple PINs for an employee and the criteria for requesting and approving multiple PINs for an employee. To address the current PIN concerns, management will review and ensure all PIN names comply with the naming convention and deactivate all PINs not in compliance with the naming convention or assigned to vendors contrary to purchasing guidelines. To ensure ongoing controls, management will establish a process for semi-annual review of PIN lists, establish guidelines for requesting and authorizing increases of PIN limits, and perform training for all site managers. These actions are targeted for implementation by September 30, 2020.

In response to recommendation 3, management will implement the activities identified in response to recommendation 2 to comply with this recommendation until the Fleet Commander Online system changes can be made. These actions will be completed by September 30, 2020.

While management did not respond in writing to Recommendation 4, in subsequent correspondence and at the exit conference on May 23, 2019, they agreed and stated that web-based training for all site managers will be performed by September 30, 2020.

Management disagreed with the questioned costs of $46,316,039, stating that based on their review, the number of suppliers receiving PINs and employees with multiple PINs identified by the OIG were significantly overstated, with many of these PINs issued within policy guidelines. Further, they stated the report misrepresents the extent of financial risk associated with PIN management controls because it fails to acknowledge the primary financial controls that are in place to authorize and approve funding for purchases.

See Appendix C for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations in the report.

Regarding management's disagreement with the monetary impact, we identified the number of suppliers receiving PINs and employees with multiple PINs and higher PIN limits using the policy guidelines outlined in the *Voyager Fleet Card SOP*. This policy states merchants are not to be provided with a dedicated PIN and that employees will be assigned a randomly generated PIN, which must be terminated when an employee leaves the Postal Service or is transferred to a different unit. Regarding the Postal Service's statement that the report misrepresents financial risk, we continue to believe that the absence of automated application controls over PINs and ineffective oversight increases the risk of improper and unauthorized purchases. We believe these calculations are accurately reflected in our report.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All 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.

Appendices

Click on the appendix title below to navigate to the section content.

Appendix A: Additional Information

Scope and Methodology

Our objective was to assess the effectiveness of the U.S. Postal Service's management controls for Voyager Fleet Card PINs nationwide.

To meet our objective, we:

- Obtained and analyzed Postal Service computerized data on Voyager PINs used at area, district, and VMF levels. Our analysis included a review of over 600,000 PINs from the FCO application and over 15 million purchases from the Postal Service Fuel Asset Management System (FAMS) for FY 2018.

- Reviewed laws, regulations, and guidance related to the government commercial fleet card program under the General Services Administration's SmartPay® Program and Voyager Fleet Systems Inc., owned by U.S. Bank.

- Obtained and reviewed the Postal Service's written policies and procedures for FAMS and FCO.

- Obtained and analyzed the maximum monthly limit for each PIN at risk and calculated the risk for a 12-month period (FY 2018).

- Tested user controls to determine effectiveness, gaps and/or redundancy between both systems for data reliability purposes.

- Interviewed Postal Service Headquarters officials in Fleet Management, Supply Management Policies and Procedures, and Travel & Relocation.

- Interviewed area and fleet management personnel to discuss OIG audit results and obtain feedback on deviations from established policies and procedures.

- Provided PIN data to each Postal Service area office in November 2018 for review and analysis.

- Obtained the PIN nationwide data in February 2019 to review the corrective actions taken by each area office.

- Judgmentally selected a sample of 49 PINs — seven PINs from each Postal Service area that were over the authorized monthly ($1,000) PIN limits. Specifically, the OIG judgmentally selected three with high, two with medium, and two with low transactions and ███████████████████████ ██████████████████████████ to test the internal controls for approving PIN limits above these amounts.

We conducted this review from August 2018 through June 2019, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on May 23, 2019 and included their comments where appropriate.

We assessed the reliability of computer-generated data from the Postal Service's FAMS and Voyager FCO application data by reviewing related documentation and correspondence, internal controls, and interviewing knowledgeable Postal Service personnel. We determined the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Objective	Report Number	Final Report Date	Monetary Impact
Voyager Card Transactions – Roseburg, OR, Post Office	Determine whether high-risk Voyager card transactions were properly reconciled and Voyager card PINs were properly managed.	FCS-FM-19-007	4/11/2019	$23,297
Fleet Specialty Card Management – Pacific Area	Assess the effectiveness of controls over fleet specialty cards for delivery operations in the Pacific Area.	DR-AR-18-009	7/17/2018	$4,378,278

Appendix B: Additional Information

Sample Analysis of *USPS Voyager Limit Change Forms*

Area Office	VMF	Site Name	Dollar Amount Per Month Limit	USPS PIN Limit Change Request Form Filed	Form Approved by VMF Manager or Designee
Capital Metro	Washington DC	Capital VMF	100,000	No	N/A
	Charlotte	Asheville VMF	50,000	No	N/A
	Baltimore	Baltimore-HealthOP	50,000	Yes	Yes
	Charlotte	Matthews Post Office	10,000	No	N/A
	Dulles	VMF Sterling	10,000	No	N/A
	Charleston SC	Annex MVS Only	5,000	No	No
	Charlotte	Admin VEH Charlotte	5,000	No	No
Eastern	Norwood	Norwood OH VMF	300,000	No	N/A
	Norwood	Norwood OH VMF	300,000	No	N/A
	Cincinnati	Sharonville OH	300,000	No	N/A
	Philadelphia	Newtown Square PO	10,000	No	N/A
	Buffalo	West Seneca PO	10,000	No	N/A
	Philadelphia	Ridley Park PO	5,000	No	N/A
	Philadelphia BMC Aux	Huntingdon Valley PO	5,000	No	N/A

Area Office	VMF	Site Name	Dollar Amount Per Month Limit	USPS PIN Limit Change Request Form Filed	Form Approved by VMF Manager or Designee
Great Lakes	Grand Rapids	VMF Grand Rapids	100,000	Yes	Yes
	Detroit	Detroit VMF	99,000	Yes	Yes
	Detroit	Detroit VMF	99,000	No	N/A
	Milwaukee	Mid-City Milwaukee	10,000	Yes	Yes
	Milwaukee	Germantown	10,000	Yes	Yes
	Carol Stream	Carol Stream PO	5,000	No	N/A
	Carol Stream	Carol Stream VMF	5,000	No	No
Northeast	Brockton	Brockton VMF	300,000	No	N/A
	Bronx	Bronx VMF	200,000	No	N/A
	Bronx	Bronx VMF	150,000	Yes	Yes
	Western Nassau	Valley Stream	10,000	No	N/A
	Western Nassau	Bellmore PO	10,000	No	N/A
	Kilmer	Piscataway PO	5,000	No	N/A
	Kilmer	Somerset PO	5,000	No	No
Pacific	Sacramento	VMF Sacramento	100,000	No	N/A
	Sacramento	West Sacramento VMF	100,000	No	N/A
	Sacramento	VMF Sacramento	100,000	Yes	Yes
	North Bay	San Rafael Main	10,000	Yes	Yes
	Santa Ana	Huntington Bch VMF	10,000	Yes	Yes
	Sacramento	Weed PO	5,000	No	N/A
	Honolulu	Kula PO	4,000	Yes	Yes

Area Office	VMF	Site Name	Dollar Amount Per Month Limit	USPS PIN Limit Change Request Form Filed	Form Approved by VMF Manager or Designee
Southern	Oklahoma	Oklahoma City VMF	315,000	No	N/A
	Oklahoma	Oklahoma City VMF	315,000	No	N/A
	Oklahoma	Oklahoma City VMF	315,000	No	N/A
	Jacksonville	VMF Gainesville	10,000	No	N/A
	Shreveport	Monroe Northside	10,000	No	N/A
	Lafayette La Aux	VMF Lafayette Rese	5,000	No	N/A
	Fort Worth	Ft Worth VMF	5,000	No	N/A
Western	Seattle	Seattle VMF	100,000	No	N/A
	Sioux Falls	Bismarck PO	100,000	No	N/A
	Seattle	VMF Stockroom	100,000	No	N/A
	Minneapolis	Willmar Post Office	10,000	No	N/A
	Kansas City	Waynesville PO	10,000	No	N/A
	Cedar Rapids	Cedar Rapids PO	5,000	No	N/A
	Albuquerque	Bloomfield PO	5,000	No	N/A

Source: OIG Analysis and Voyager Driver Inventory Report

Appendix C: Management's Comments

UNITED STATES POSTAL SERVICE

June 17, 2019

LAZERICK C. POLAND
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Nationwide Review of Voyager Fleet Card Personal Identification
Numbers (Report Number DR-AR-19-DRAFT)

Management agrees with the OIG's finding that USPS should improve automated
controls over Voyager PINs.

Recommendation [1]:
The OIG recommended for USPS management to coordinate with US Bank
Voyager to implement automated controls in the Voyager Fleet Commander Online
(FCO) application to: (1) prevent assignment of PINs to vendors; (2) prevent
assignment of multiple PINs to employees; (3) prevent assignment of PINs without
valid employee names; and (4) ensure only authorized employees are allowed to
request PIN limit changes.

Management Response/Action Plan:
Management agrees with the OIG's recommendation to coordinate with US Bank
to implement automated controls in the Voyager Fleet Commander Online
application as it relates to the Voyager PIN process.

The USPS Travel and Relocation office will work with US Bank to implement
automated controls in Fleet Commander Online (FCO) to prevent assignment of
PINs to vendors, prevent assignment of multiple PINs to employees, and prevent
assignment of PINs without valid employee names. In addition, the Travel and
Relocation office will work with US Bank and USPS Fleet Management to
communicate the PIN limit policy and process and ensure only authorized
personnel are requesting PIN limit changes. The Travel and Relocation office
will work with US Bank to reinforce acceptance of PIN limit change requests
submitted by authorized personnel only.

Target Implementation Date:
February 29, 2020

Responsible Official:
Anna Vazquez, Manager Corporate Accounting (A)

Recommendation [2]:
Implement corrective action to: (1) deactivate PINs issued to vendors; (2) deactivate multiple PINs issued to employees or define policy exceptions for multiple PINs; (3) deactivate PINs without a valid employee name; (4) ensure authorized approval of requests for increasing PIN purchasing limits, and (5) track and monitor completion of semi-annual reviews.

Management's Response:
Management agrees, and will clarify policy guidelines for the PIN naming convention to allow for operational needs of multiple PINs for an employee and the criteria for requesting and approving multiple PINs for an employee. To address the current PIN concerns, management will review and ensure all PIN names comply with the naming convention, deactivate all PINs not in compliance with naming convention or assigned to vendors contrary to purchasing guidelines. To ensure ongoing controls, management will establish a process for semi-annual review of PIN lists, establish guidelines for requesting and authorizing increases of PIN limits, and perform training for all site managers

Target Implementation Date:
Fiscal Year 2020

Responsible Official:
Jennifer Vo, Director City Delivery

Recommendation [3]:
Develop and implement interim controls to prevent and detect the issues noted in this report until the Voyager Fleet Commander Online application is updated.

Management's Response:
Management agrees. Activities in response to recommendation #2 appear to comply with this recommendation until Fleet Commander Online system changes can be made.

Target Implementation Date:
Fiscal Year 2020

Responsible Official:
Jennifer Vo, Director City Delivery

Cara M. Greene
Vice President
Controller

Kevin L. McAdams
Vice President
Delivery and Retail Operations

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, contact Agapi Doulaveris
Telephone: 703-248-2286
adoulaveris@uspsoig.gov