OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

eCommerce Customer Registration

Audit Report

Report Number
IT-AR-14-008

August 15, 2014

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

Effective management and technical controls are needed to strengthen oversight, further reduce fraud-related credit card chargebacks, and prevent a cyber criminal from obtaining postage using stolen credit card data.

Background

The U.S. Postal Service's Customer Registration application allows customers to create accounts through USPS.com to purchase products and services through over 40 eCommerce applications such as Every Door Direct Mail, Premium Forwarding Service, Click-N-Ship, and the Postal Store. Customers must provide personally identifiable information to create an account. There were over 24 million Customer Registration users as of June 2014 and revenue totaled about $1.2 billion in fiscal year (FY) 2013.

Our objective was to determine the effectiveness of controls used to safeguard the eCommerce Customer Registration process and reduce online credit card fraud.

What the OIG Found

Controls used to safeguard the eCommerce Customer Registration process and reduce online credit card fraud need improvement. Management has not established a threshold for fraud-related chargebacks (transactions rejected by credit card companies) for the four eCommerce applications in our review. As a result, management cannot objectively measure when to increase oversight and controls to reduce fraud.

Of the four applications, Click-N-Ship's credit card fraud-related loss of $4.6 million was above the industry's recommended threshold for acceptable levels of credit card fraud in FY 2013. In addition, management did not always ensure all credit card company chargebacks were validated.

Further, seven of the eight Customer Registration controls we tested worked as management intended. However, we identified one vulnerability that could permit a cyber criminal to impersonate a valid user and obtain postage using stolen credit card data. Finally, we did not identify any critical or high-risk vulnerabilities when conducting over 3,000 additional tests of the USPS.com login page.

What the OIG Recommended

We recommended management establish a threshold for credit card fraud and develop a policy defining chargeback roles and responsibilities.We also recommended management maintain chargeback research results from all eCommerce managers and configure eCommerce applications to prevent the noted security vulnerability.

Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 15, 2014

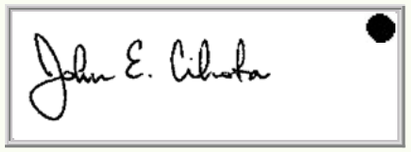
MEMORANDUM FOR: NAGISA M. MANABE
EXECUTIVE VICE PRESIDENT, CHIEF MARKETING
AND SALES OFFICER

SCOTT G. DAVIS
ACTING VICE PRESIDENT, CONTROLLER

JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY

KELLY M. SIGMON
VICE PRESIDENT, RETAIL CHANNEL OPERATIONS

ELIZABETH M. SCHAFER
TREASURER, CORPORATE TREASURY



FROM: John E. Cihota
Deputy Assistant Inspector General
for Financial and Systems Accountability

SUBJECT: Audit Report – eCommerce Customer Registration
(Report Number IT-AR-14-008)

This report presents the results of our audit of eCommerce Customer Registration processes and controls (Project Number 13BG018IT000).

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

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

Introduction

This report presents the results of our self-initiated audit of eCommerce Customer Registration (Project Number 13BG018IT000). Our objective was to determine the effectiveness of controls used to safeguard the eCommerce Customer Registration process and reduce online credit card fraud. See Appendix A for additional information about this audit.

Customers use the Customer Registration application to register accounts through USPS.com.[1] These accounts give them access to the U.S. Postal Service eCommerce applications such as Click-N-Ship,[2] Every Door Direct Mail (EDDM),[3] Premium Forwarding Service (PFS),[4] and the Postal Store,[5] and allow them to purchase products and services through the Internet using a major credit card.[6] There were over 24 million Customer Registration users as of June 2014. To create an account, customers must enter personally identifiable information such as name, address, and telephone number. To purchase products and services, customers also provide their credit card data.[7]

Credit card fraud carried out through an eCommerce application, such as Customer Registration, often starts with a cyber criminal[8] successfully applying for a new account, or taking over an existing account by circumventing identity-proofing techniques.[9] In January 2013, management detected a high volume of automated, unauthorized attempts to log into Customer Registration application accounts. After further analysis, management determined that cyber criminals obtained stolen credit card data from unknown sources outside the Postal Service. They also accessed existing Postal Service accounts and created fictitious Customer Registration accounts to purchase domestic and international shipping labels[10] from Click-N-Ship. Affected credit cardholders alerted their credit card issuers[11] to report their credit card data had been stolen and used to make unauthorized purchases. The issuer then generated chargebacks[12] that resulted in a financial loss to the Click-N-Ship program management office.[13] As a result, the January 2013 Click-N-Ship credit card chargebacks related to fraud increased 122 percent (from $266,762 to $594,408) over those recorded for September 2012.[14] Additionally, management identified minimal credit card fraud in the Postal Store, EDDM, and PFS applications. See Appendix C for additional information.

In January 2013, management began implementing additional controls to reduce fraudulent activity.[15] Click-N-Ship credit card chargebacks declined as the new controls were implemented; however, continuous assessment of Customer Registration controls and a detailed knowledge of current cyber threats are some of the measures needed to continuously combat cyber criminal activity.

---

1 Provides various tools for customers to ship at any time, as well as help control home, business, or Post Office Box™ mail delivery with easy-to-use links.
2 Enables customers to create pre-paid shipping labels for certain mail classes using the customer's personal computer and printer.
3 Enables businesses to send advertising mail to their desired audience without acquiring an address list or printing specific names and addresses on mailpieces.
4 Provides the ability for customers to forward their mail from their permanent address to a temporary address.
5 Enables customers to easily purchase products online such as stamps, supplies, gifts, and collectibles.
6 Visa, MasterCard, Discover, and American Express. Customers may also use PayPal to purchase Click-N-Ship products.
7 Customers are redirected to the [redacted] Payment application to enter their credit card data when making a purchase.
8 An individual who commits cyber crimes using the computer as a tool, a target, or both.
9 Identity-proofing techniques include a layer and risk-based approach that provides assurance of identity verification.
10 Many of these labels were placed on packages used as part of reshipping schemes, where stolen or illegally obtained goods were shipped to overseas destinations.
11 The issuer provides credit cards and contracts with its cardholders for billing and payment of transactions.
12 Chargebacks occur when the bank debits the Postal Service for a previously settled credit or debit card transaction. The most common reasons for chargebacks include customer disputes, fraud, processing errors, and authorization issues.
13 The issuer reversed the chargebacks the Postal Service successfully disputed.
14 September 2012 represents the lowest recorded fraud-related chargeback period in fiscal year (FY) 2012.
15 Examples of Customer Registration controls implemented since January 2013 include disabling accounts when users attempt to change their account profile more than five times a day and detection of cyber criminals who use scripts to create numerous accounts within a short timeframe.

The Postal Service incurred Click-N-Ship credit card fraud-related losses of $4.6 million in FY 2013 exceeding the industry best practice by a total of $2.8 million.

A threshold for eCommerce application fraud-related credit card chargebacks was not established.

Conclusion

Controls used to safeguard the eCommerce Customer Registration process and reduce online credit card fraud need improvement. Management did not establish a specific threshold for expected fraud-related chargebacks for Click-N-Ship, EDDM, PFS, and the Postal Store. Specific thresholds were not established because the Click-N-Ship manager believed the existing controls were sufficient and EDDM, PFS, and Postal Store managers thought the minimal chargebacks in their programs did not warrant establishing thresholds. Although we agree chargebacks for EDDM, PFS, and the Postal Store were minimal for the period we reviewed, management needs a threshold to objectively measure whether fraud chargebacks reach an unacceptable level or effectively gauge when to escalate oversight and preventative controls to reduce credit card fraud. A threshold would also help management determine whether the costs of controls implemented to prevent fraud outweigh the benefits.

The Postal Service incurred Click-N-Ship credit card fraud-related losses of $4.6 million in FY 2013.[16] This exceeded the industry best practice of 0.35 percent of revenue[17] by a total of $2.8 million.

Additionally, we determined the program managers for PFS and EDDM did not research chargebacks related to their programs. Furthermore, Eagan Accounting Services did not maintain records needed to monitor, account for, and ensure timely receipt of the program manager's research results because there are no standard operating procedures explaining the roles and responsibilities for these functions. Without performing this research and maintaining the results, the Postal Service is at risk for monetary loss from the sale.[18]

Furthermore, we determined seven of the eight Customer Registration controls we tested worked as management intended; however, we identified one security vulnerability that could permit a cyber criminal to impersonate a valid user and obtain postage using stolen credit card information.[19] We did not identify any critical or high-risk vulnerabilities when conducting over 3,000 additional tests of the USPS.com login page.

Threshold for Chargebacks

Program managers did not establish a specific threshold for expected fraud-related chargebacks for Click-N-Ship, EDDM, PFS, and the Postal Store. Industry best practice[20] recommends establishing thresholds that escalate incidents of fraud to higher levels of management visibility. Our research found the recommended threshold was 0.35 percent of revenue for fraudulent credit card chargebacks associated with "card not present" purchases.[21]

Click-N-Ship management believed the existing controls were sufficient and EDDM, PFS, and Postal Store managers thought a threshold was not warranted because chargebacks were minimal. Even though chargebacks for EDDM, PFS, and the Postal Store were minimal for the period we reviewed, management needs an established threshold for all four applications to objectively measure whether fraud-related chargebacks have reached an unacceptable level. Establishing a threshold would

16 Click-N-Ship chargeback amounts included 95 percent of the total MasterCard and Visa chargebacks identified as fraudulent. They also included 100 percent of American Express and Discover chargeback amount because the Postal Service was unable to [redacted].
17 Provided by Gartner, Inc., a leading information technology research and advisory company.
18 The time required to respond to the acquirer with dispute documentation varies by credit card brand and the acquirer's internal procedures. Historically, for Visa chargebacks, Eagan Accounting Services had to respond to the acquirer in 7 to 10 days.
19 We tested three additional controls; however, the results were inconclusive. This was a result of an existing compensating control that limits the number of times a user can edit his or her profile (five times per day). This control is in place because numerous changes to a user's account profile are an indicator of a user with malicious intentions.
20 *Managing the Business Risk of Fraud: A Practical Guide,* sponsored by the Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners.
21 Transactions in which the customer is not required to physically present the credit card (for example, online transactions).

Hover over active areas for more information.

allow managers to consistently gauge when to escalate oversight of the program and increase the preventative controls needed to mitigate fraud. A threshold would also help management determine whether the costs of controls implemented to prevent fraud outweigh the benefits.

We reviewed the credit card chargebacks associated with purchases made through the Click-N-Ship, EDDM, the Postal Store, and PFS applications for FYs 2012 and 2013. Only the Click-N-Ship application incurred chargebacks over the recommended threshold. Figure 1 shows FYs 2012 and 2013 revenue and chargeback comparisons for Click-N-Ship. Fraud-related chargebacks were 0.9 percent higher in FY 2012 and 0.52 percent higher in FY 2013 than the best practice recommended 0.35 percent threshold.

Figure 1. Click-N-Ship Revenue and Chargeback Data

Safeguard Controls for Online Fraud Need Improvement

Click-N-Ship Revenue and Chargeback Data

Click-N-Ship	FY 2012	FY 2013
Revenue	$490,375,618	$535,865,158
Chargebacks (percentage of revenue)	$6,137,780 (1.25%)	$4,686,252 (0.87%)
Best Practice Threshold (0.35 percent of revenue)	$1,716,315	$1,875,528
Chargeback Variance >0.35 percent of revenue	$4,421,465	$2,810,724
FY 2012/2013 Chargeback Variance Total		$7,232,189

Chargeback disputes were not properly managed.

Management of Chargeback Disputes

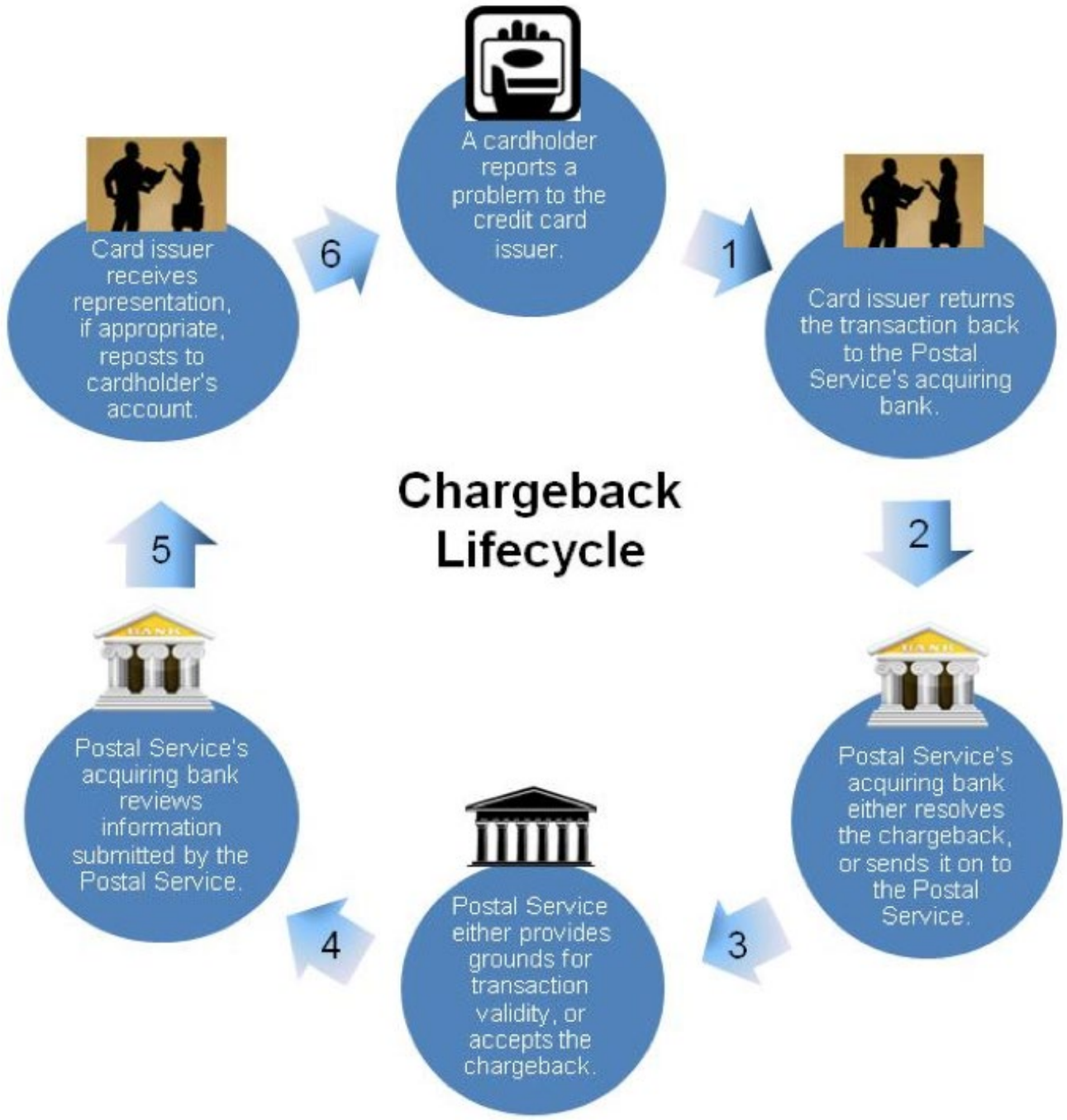
Managers from Eagan Accounting Services and the program management offices for Click-N-Ship, EDDM, and PFS did not effectively manage all credit card chargeback disputes. Postal Service policy[22] states that responses to chargebacks should occur immediately after a request from the financial institution or the Postal Service will incur the expense of the sale. Untimely responses occurred because there is no standard operational procedure explaining the roles and responsibilities for effective management of these chargeback disputes for all parties involved. Timely responses to chargeback inquiries are needed to assist Eagan Accounting Services in providing the acquirer[23] compelling evidence that certain chargebacks are not valid; otherwise, the program office's budget is at risk for monetary loss from the sale. Click-N-Ship credit card fraud resulted in sales losses of $6.1 million in FY 2012 and $4.6 million in FY 2013.

The Finance Branch, Eagan Accounting Services, provided a daily list of the credit card chargebacks to all of the program managers;[24] however, program managers for Click-N-Ship, PFS, and EDDM did not use this information to research the chargebacks and did not provide the documented proof to Eagan Accounting Services that it needed to dispute any chargebacks. Management indicated program managers were not trained to perform this function. In addition, the program manager for Click-N-Ship stated he was not aware of the requirement to communicate the results to Eagan Accounting Services. Further, Eagan Accounting Services did not maintain records needed to monitor and ensure timely receipt of program managers' chargeback research results.

22 Postal Service Handbook F-101, *Field Accounting Procedures,* Section 9-2.8, October 2013.
23 The merchant's (Postal Service's) bank.
24 The list of credit card chargebacks is provided daily unless there are no chargebacks.

See Figure 2 for a flowchart describing the chargeback lifecycle. See Appendix C for a summary of chargeback amounts for FYs 2012 and 2013.

Figure 2. Chargeback Lifecycle[24]



Source: *VISA – Chargeback Management Guidelines for Visa Merchants, 2011.*

25 This diagram is a generic representation of the Visa chargeback lifecycle.

Customer Registration security controls were working as intended with the exception of one vulnerability that could allow a cyber criminal to obtain postage using stolen credit card information.

Customer Registration Controls

Our test of eight selected Customer Registration security controls demonstrated that seven controls were working as intended. Furthermore, we used software[26] that performed over 3,000 tests of the USPS.com login page and did not identify any critical or high-risk vulnerabilities.[27] See Appendix C for complete results of our tests and information about the controls we tested.

Examples of controls that work as management intended include the following:

- Customer Registration users are limited to three login attempts. This control is in place to help prevent cyber criminals from successfully guessing an account holder's password. Customer Registration accounts are locked after the third login attempt. To unlock the account, the user may call the Customer Registration Help Desk, use the "I Forgot My Password" feature by answering secret questions, or wait 24 hours and try again.

- Changes to user profiles are limited to five per day. This control is in place because numerous changes to a user's account profile indicate a user with malicious intentions. If a user needs to change his or her profile after exceeding the daily limit, the user can call the Help Desk and answer his or her secret questions and may be granted an override (one time in 24 hours).

While most security controls we tested were working as intended, we identified one security vulnerability that may permit a cyber criminal to impersonate a valid user and obtain postage using stolen credit card information.[28] Specifically, two [redacted] related to the Click-N-Ship and the Postal Store applications were not configured to safeguard the [redacted] information from unauthorized disclosure and modification. Although management was aware of the vulnerability in 2012, they did not take corrective action because they prioritized their efforts by addressing high and medium risks first.

26 We used Hewlett-Packard (HP) WebInspect to perform these tests.
27 Using HP WebInspect, we were able to thoroughly test the USPS.com login page, but the limit of five edits to the Customer Registration profile per day prevented us from performing any useful tests on the Customer Registration web pages.
28 In 2012, an outside vendor reported this as a low-risk finding and recommended addressing this vulnerability. Although there is a small probability of an exploit, the impact could be great.

[redacted]

Recommendations

We recommend the executive vice president, chief Marketing and Sales officer, in coordination with the vice president, Retail Channel Operations, direct the program managers for Click-N-Ship, Every Door Direct Mail, Premium Forwarding Service, and the Postal Store to:

1. Establish thresholds for acceptable levels of credit card fraud for their program areas to help determine when escalation of oversight and additional controls are needed.

We recommend the treasurer, Corporate Treasury, in coordination with the acting vice president, Controller, direct the manager, Banking, to coordinate with the manager, Accounting Services, to:

2. Create standard operating procedures documenting the roles and responsibilities for all program offices responsible for managing chargebacks and Eagan Accounting Service's responsibility for monitoring and obtaining timely receipt of program managers' chargeback research results.

We recommend the vice president, Information Technology, direct the manager, Business Relationship Management, to:

3. Eliminate the identified security vulnerability concerning [redacted] on all Customer Registration integrated applications.

Management's Comments

Management partially agreed with the findings in our report, and agreed with recommendations 2 and 3. Management disagreed, in part, with recommendation 1 and disagreed with the monetary impact.

Regarding recommendation 1, management agreed with the mathematical calculations performed. However, they disagreed with the metric (.35 percent ratio) provided by an industry expert to determine monetary impact as stated in the report, and cited ratios from other sources that could be used. Management also disagreed with the recommendation because their eCommerce programs have a goal of zero percent for fraudulent chargebacks. Management is currently enhancing their fraud detection activities and will begin sending a monthly fraud/chargeback report to senior management by December 31, 2014.

Regarding recommendation 2, management will create standard operating procedures documenting the roles and responsibilities for all program offices responsible for managing chargebacks and Eagan Accounting Service's responsibility for monitoring and obtaining timely receipt of program manager's chargeback research results. Chargeback research will be contingent on the results of a future cost benefit analysis, targeted for completion by March 31, 2015.

Regarding recommendation 3, management advised that they eliminated the identified security vulnerability concerning [redacted] The last set of corrections was completed for all applicable applications on May 12, 2014. Management did take exception to how we portrayed the severity of the [redacted] vulnerability, noting that evaluation and assessments rated this as a low vulnerability.

Management disagreed with the amount of monetary impact because of subsequent consultation they obtained from an independent source indicating a higher level of acceptable credit card fraud. Also, management does not agree entirely with the amount of chargebacks classified as fraudulent.

Management cited specific statements that they consider inaccurate or could be misleading. Specifically, management disagreed with the ratio of .35 percent of credit card sales used as an acceptable level of credit card fraud. In addition, management stated a portion of the criteria used was not applicable to eCommerce transactions and noted the importance of fraud prevention. They also stated there was not an office named "Corporate Treasury, Fraud and Risk Mitigation." See Appendix D for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 2 and 3 and the corrective action proposed should resolve the issues identified in the report. Management cited that they have taken corrective action for recommendation 3. The OIG considers management's comments to recommendation 1 to be non-responsive.

Regarding recommendation 1, we believe sending a monthly fraud/chargeback report will enhance management's efforts to reduce fraudulent chargebacks. However, we believe management's goal of zero percent fraud is not practical from a cost/benefit perspective. Although we used a threshold ratio of .35 percent of revenue for our analysis, we believe management should perform their own analysis to determine a reasonable threshold that would be used to help determine when escalation of oversight and additional controls are needed.

Although management disagreed with the .35 percent ratio that we received from an industry expert and used throughout our report, we believe this ratio is valid. Management stated they identified a different ratio from a separate source and then confirmed this ratio with the same expert we used. However, we do not know the context of management's communications with the industry expert, and management did not provide any additional evidence of this communication. Based on the objective of our audit and consultation with our industry expert, we continue to believe the ratio is reasonable. However, as noted in recommendation 1, we believe it is important for the Postal Service to establish its own threshold. We commend the Postal Service for conducting additional research on potential thresholds and suggest it use that research to identify a threshold that is cost beneficial to the Postal Service.

Additionally, management stated they do not entirely agree with our monetary impact because the OIG classified 100 percent of the American Express and Discover chargebacks as fraudulent. In the report, the OIG explained that the Postal Service was unable to [redacted] at the time of our audit and did not provide a basis for the 95 percent ratio cited in management's response. As a result, the OIG considers the entire amount at risk.

Management also stated that our reference to Handbook F-101 is not relevant to eCommerce transactions. However, management did not provide us with any alternative policy. We believe the intent of the policy is relevant to disputing credit card chargebacks regardless of where the transaction took place. Responding immediately after a request would ensure research results are provided in time to meet the acquirer's timeframes for chargeback reversal consideration.

We agree with management's comments about the importance of preventing fraud and believe prevention is a valuable component of minimizing fraud risk. It is for this reason we stress that management needs a threshold to objectively measure whether fraud chargebacks reach an unacceptable level or effectively gauge when to escalate oversight and preventative controls to reduce credit card fraud.

Based on management's comments, we changed the title of the group that oversees fraud and risk mitigation from "Corporate Treasury, Fraud and Risk Mitigation" to "Corporate Treasury."

Regarding recommendation 3, we concur that the vulnerabilities related to the [redacted] is low. In fact, we reported that management had been aware of the vulnerability but did not take corrective action because they addressed high and medium risks first. Although the vulnerability is low, the risk that cyber criminal could impersonate a valid user and obtain postage using stolen credit card information remains. Since management has been aware of this vulnerability for nearly 2 years, we believed it was important for management to further reduce the risk, particularly in light of management's detection of a high volume of automated, unauthorized attempts to log into Customer Registration application accounts in January 2013.

The OIG considers recommendation 1 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action is completed. This recommendation should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed. Although we believe a zero percent fraud policy is not practical from a cost/benefit perspective, we view the disagreement on significant recommendation 1 as unresolved but do not plan to pursue it through the formal audit resolution process. We understand management's decision to defer other corrective actions for recommendation 2 until May 2015, pending completion of a positive cost-benefit analysis.

Appendices

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

Appendix A: Additional Information

Background

According to a Trustwave® 2013 Global Security Report, the primary data type targeted by cyber criminals in 2011 and 2012 was credit cardholder data. There is a well-established underground marketplace for stolen credit card data. Criminals purchase and sell this data quickly for use in fraudulent transactions. eCommerce applications were more susceptible to credit card fraud activities compared to in-store purchase transactions where the credit card is presented and physical verification of identity is possible. This makes the Internet extremely attractive to fraud perpetrators. Determined criminals have compromised almost every electronic identity-proofing technique and, unfortunately, there is no infallible solution to eliminating all fraudulent schemes and practices. As a result, the Postal Service is challenged, as are all eCommerce businesses, with safeguarding its eCommerce applications from cyber criminals, identifying those involved, and determining their full intentions.

Corporate Treasury, oversees fraud and risk mitigation and supports the development and implementation of strategies, policies, and programs for mitigating payment fraud. This office is also responsible for analyzing fraud risk, leading the implementation of all corporate business initiatives to identify and mitigate fraud, and coordinating with various stakeholders to reduce fraud.

The Marketing Relationship Management Portfolio within Information Technology (IT), is the responsible owner of the Customer Registration application. This office collaborates with managers and key officials from other offices, and helps mitigate credit card fraud. These offices include program management offices (Click-N-Ship, EDDM, PFS, and the Postal Store), IT, the U.S. Postal Inspection Service, and Corporate Information Security (CIS).

Eagan Accounting Services is responsible for disputing chargebacks in a timely manner. The program management offices are responsible for researching chargebacks and providing supporting documentation to Eagan Accounting Services to dispute chargebacks. If a chargeback is not resolved, Eagan Accounting Services will expense it to the appropriate program management office, which considers it a loss.

Objective, Scope, and Methodology

Our objective was to determine the effectiveness of controls used to safeguard the eCommerce Customer Registration process and reduce online credit card fraud. To accomplish our objective, we interviewed managers and key officials from Marketing Relationship Management, Corporate Treasury, Eagan Accounting Services, CIS, IT, and the Postal Inspection Service. We also interviewed program managers for Click-N-Ship, EDDM, PFS, and the Postal Store.

We reviewed select Customer Registration security controls (implemented and planned) and performed manual and automated tests of those controls. We performed a web vulnerability assessment during our audit using HP WebInspect,[30] McAfee's SSLDigger,[31] and Mozilla Firefox[32] to test select controls implemented in the Customer Registration application. We performed our tests in the Customer Acceptance Test environment at the Eagan Computer Operations Service Center.

We analyzed revenue and credit card chargeback data for FYs 2010 through 2013 for the Click-N-Ship, EDDM,[33] PFS, and the Postal Store applications. In addition, we consulted with a contractor who has expertise in the field to determine an industry-wide threshold for credit card fraud chargebacks. We used this data to conduct a comparative analysis of chargebacks to yearly revenue for each of the four applications.

We conducted this performance audit from June 2013 through August 2014, 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 during the week of June 16, 2014, and included their comments where appropriate.

We assessed the reliability of chargeback data by collaborating and verifying the accuracy of the data with multiple managers from Corporate Treasury, Fraud Risk and Mitigation, and Eagan Accounting Services. 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.

30 An automated and configurable web application security-testing tool that mimics real-world hacking techniques and attacks.
31 A software utility that evaluates and rates the security of Secure Socket Layer (SSL) ciphers accepted by a web server.
32 Mozilla Firefox is a free and open-source web browser that provides support for add-ons written by third parties that integrate with Firefox.
33 EDDM did not generate revenue in FY 2010 because it was not in production at that time.

Appendix B: Customer Registration Controls Test Results

Table 2 identifies eight of the 11 judgmentally selected Customer Registration security controls we tested and the results of those tests. Test results for three controls were inconclusive. We were able to test the Customer Registration login web page and determined that [redacted] did not exist on that web page; however, we were not able to determine whether these controls passed or failed on subsequent web pages. This was a result of an existing compensating control that limits the number of times a user can edit his or her profile to five times per day. While the compensating control that limited our tests would also limit a cyber criminal's attempt to perform the same tests, it is not an indicator of whether the control passed or not. For the remaining eight controls, our tests demonstrated that seven are working as management intended; however, we identified one that did not pass our test. We used automated tools and manual methods to perform these tests in the customer acceptance test environment and on the USPS.com web page.

[redacted]

Table 2. Customer Registration Controls Test Results

No.	Controls	Results: Passed	Results: Failed
	Using Firefox plug-ins[1] we tested the following:		
1.	Cookies are marked as secure A secure cookie helps secure a user's identity.	X	
2.	[redacted]		X
	Using the SSLDigger[3] tool we tested the following:		
3.	Disable support in the web server for weak cryptography Weak cryptography refers to weak algorithms and/or weak keys used to encrypt data.	X	
	Using manual methods we tested the following:		
4.	Set email address limitations For example, limits the user's choice of email name to a subset of the technically valid characters.	X	
5.	Limit attempts to edit profile to five per day Numerous changes to a user's account profile are an indicator of a user with bad intentions	X	
6.	Lock account after three unsuccessful login attempts When the user attempts to login three times with an incorrect password, the user's account is immediately locked. This control helps prevent cyber criminals from successfully guessing an account holder's password.	X	
7.	Multiple user roles established Customer Registration roles include Administrator, Help Desk, and Data Analyst. These roles help to segregate duties and improve access controls.	X	
8.	Enable account disabling in volume Multiple accounts can be disabled in large quantities based on indications of fraudulent behavior/patterns.	X	
	Total	**7**	**1**

Source: OIG audit team's judgmental selection of controls in coordination with Marketing Relationship Management.

1 Software that is added to existing software to increase program functionality.

[redacted]

3 Foundstone SSLDigger is a tool to assess the strength of SSL servers by testing the ciphers supported.

Appendix C: Summary of Chargebacks

Table 3 summarizes the revenue and chargebacks for each application under review for FYs 2012 and 2013. Click-N-Ship chargeback amounts include 95 percent[37] of the total MasterCard and Visa chargebacks identified as fraudulent plus 100 percent[38] of American Express and Discover chargeback amounts. EDDM, PFS, and the Postal Store amounts represent 100 percent of the chargebacks for each of the four previously stated credit card brands.

Table 3. Summary of Revenue and Chargebacks

Application	FY Revenue (in millions)	FY Chargeback Totals	Monthly Average	Monthly High	Monthly Low
Click-N-Ship					
FY 2012	$490	$6,137,781	$511,482	$798,049	$266,762
FY 2013	536	4,686,252	390,521	594,408	127,918
Total		**$10,824,033**			
EDDM[4]					
FY 2012	$299	$249	$249	$249	$249
FY 2013	430	28,817	2,401	5,987	212
Total		**$29,066**			
PFS[5]					
FY 2012	$19	$ 3,427	$492	$1,402	$15
FY 2013	22	15,519	1,293	2,042	823
Total		**$18,946**			
Postal Store					
FY 2012	$244	$312,017	$26,001	$37,453	$13,928
FY 2013	266	282,947	23,579	42,961	12,995
Total		**$594,964**			

Source: OIG calculations based on Eagan Accounting Services chargebacks and revenue provided by program managers.

4 EDDM was placed into production in 2011; therefore, chargebacks were minimal in FYs 2011 and 2012.

5 PFS revenue included online and retail sales.

37 MasterCard and Visa identify fraudulent chargebacks. According to the Postal Service, those charges have historically been about 95 percent of all chargebacks.

38 We are using 100 percent of American Express and Discover chargeback amounts because the Postal Service was unable to [redacted].

Appendix D: Management's Comments

JOHN T. EDGAR
VICE PRESIDENT
INFORMATION TECHNOLOGY

UNITED STATES
POSTAL SERVICE

July 11, 2014

JUDITH LEONHARDT
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Response to Draft Audit Report - eCommerce Customer Registration (IT-AR-14-DRAFT)

Recommendation 3:

Eliminate the identified security vulnerability concerning [redacted] on all Customer Registration integrated applications.

Management Response/Action Plan:

Management requests that this recommendation be closed at the issuance of the final audit report. Management has completed the task of eliminating the identified security vulnerability concerning [redacted] The last set of corrections was completed for all applications in question on May 12, 2014. USPS has provided evidence that corroborates a historical decline in chargeback fraud.

Management disagrees with the severity of the [redacted] security vulnerability as stated by the OIG. Specifically, within the "Customer Registration Controls" section, the report calls attention to two [redacted] related to the Click-N-Ship and Postal Store applications. The report suggests that the improperly configured [redacted] cause a security vulnerability that may allow a cybercriminal to impersonate a valid user and fraudulently obtain postage using stolen credit card information. Management notes that evaluations and assessments rated this vulnerability as low.

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-2100
202-268-3977
FAX: 202-268-4492
JOHN.T.EDGAR@USPS.GOV
WWW.USPS.COM

This report contains information which management believes may contain proprietary or other business information that may be exempt from disclosure under the Freedom of Information Act (FOIA). Attached is the report detailing the exact information that should be redacted.

John T. Edgar, Vice President, Information Technology

cc:
Barbara Wheeler
John Byrne
Robert Dixon Jr.

Detailed Redaction Report:

This report contains information that management believes may contain proprietary or other business information that may be exempt from disclosure under the Freedom of Information Act (FOIA).

Management requests that the content of the report be redacted so that controls used to protect the security of USPS data and systems are not published to the public.

Please redact the following sections:

- On page 6 of the report, footnote #9: "Customers are redirected to the [redacted] Payment application to enter their credit card data when making a purchase"
- On page 7 of the report, footnote #20: "We tested three additional controls; however, the results were inconclusive. This was a result of an existing compensating control that limits the number of times a user can edit his or her profile (five times per day). This control is in place because numerous changes to a user's account profile are an indicator of a user with malicious intentions."
- On page 11 of the report, the entire section titled "Customer Registration Controls" and the associated footnotes (#27, #28, #29, and #30)
- On page 16 of the report, the entire section titled "Appendix B: Customer Registration Controls Test Results" including the associated footnotes (#35, #36, #37)
- On page 17 of the report, the table titled "Table 2: Customer Registration Controls Test Results" including the associated table-specific footnotes (#1, #2, and #3)

UNITED STATES POSTAL SERVICE

July 22, 2014

To LORI LAU DILLARD
(A) DIRECTOR, AUDIT OPERATIONS

SUBJECT: eCommerce Customer Registration (Report Number IT-AR-14-DRAFT)

Finance management agrees with recommendation number 2 of the report but wishes to address specific findings and statements that are not accurate or could be considered misleading. The most significant of those are:

- The report refers to a ratio of 0.35 percent for credit card fraud chargebacks to revenue as being the acceptable level of credit card fraud. Management disagrees that this ratio correctly reflects the industry standard and does not believe it is appropriate that this ratio is used throughout the report as a baseline. The report fails to cite the source of this ratio and provided no documentation to Management as support. Management identified the CyberSource (a Visa subsidiary) 2013 Online Fraud Report as an appropriate source for this ratio. The Report contains an industry standard ratio of 0.9 percent for fraud chargebacks to revenue for digital goods such as labels sold on Click-N-Ship®. Management subsequently consulted with the OIG's uncited industry expert who confirmed that 0.9 percent is a relatively good proxy for the industry rate plus or minus 25 basis points based on various factors. The expert stated there was no data or study to support the referenced 0.35 percent threshold metric.

- Management does not agree with the monetary savings as calculated in the report. Management does not agree with the baseline ratio used of 0.35 percent as noted above and the amount of chargebacks classified as fraudulent. The report classified 100 percent of the American Express and Discover chargebacks as fraudulent because "the Postal Service was unable to [redacted] This approach clearly overstates the American Express and Discover fraud chargebacks by assuming 100 percent are fraud related. Management has recalculated the level of chargebacks assuming the 95 percent ratio for MasterCard/Visa (Attachment A).

- The report states "Industry best practice recommends establishing thresholds that escalate incidents of fraud to higher levels of management visibility" as noted in the Managing the Business Risk of Fraud. Managing the Business Risk of Fraud also stresses the importance of prevention which was not addressed in the report. Chargebacks exist because the fraudster was able to successfully complete a transaction. Prevention can occur at all stages of the transaction including preventing fraudulent registrations.

- The report contains the statement that "Postal Service policy states that responses to chargebacks should occur immediately after a request from the financial institution or the Postal Service will incur the expense of the sale." This statement was taken from the Postal Service Handbook F-101, Field Accounting Procedures and is "The PRU

must respond to a chargeback immediately after receiving a request. Failure to do so could result in monetary loss of the sale, which will result in an expense for the PRU." PRU stands for Postal Retail Unit. Handbook F-101 is for Postal Service employees who perform financial duties at field units. The statement is not applicable to chargebacks resulting from eCommerce transactions.

- The report states "Corporate Treasury, Fraud and Risk Mitigation, oversees fraud and risk mitigation and supports the development and implementation of strategies, policies and programs for mitigating payment fraud. This office is also responsible for analyzing fraud risk, leading the implementation of all corporate business initiatives to identify and mitigate fraud, and coordinating with various stakeholders to reduce fraud." There is no office in Corporate Treasury with this name. There is one individual with the title of Program Manager Fraud and Risk Mitigation who manages no staff.

- The report states that "If a chargeback is not resolved, Eagan Accounting Services will expense it to the appropriate program management office, which considers it a loss." Upon receipt of a chargeback, the Postal Service incurs the loss as the funds originally received from the sale are reversed. In order for the chargeback to be reversed and the funds returned, the Postal Service must successfully dispute the chargeback. Just responding to a chargeback does not guarantee that the documentation provided will result in a chargeback reversal.

Recommendation (2)
"We recommend the treasurer, Corporate Treasury, in coordination with the acting vice president, Controller, direct the manager Banking, to coordinate with the manager, Accounting Services to:

2. Create standard operating procedures documenting the roles and responsibilities for all program offices responsible for managing chargebacks and Eagan Accounting Service's responsibility for monitoring and obtaining timely receipt of program managers' chargeback research results."

Management Response/Action Plan:

Management will create standard operating procedures documenting the roles and responsibilities for all program offices responsible for managing chargebacks and Eagan Accounting Service's responsibility for monitoring and obtaining timely receipt of program managers' chargeback research results. As part of the creation of the procedures, management will make determinations regarding the cost verses benefit of researching the chargebacks which may impact the decision as to whether chargebacks will be researched.

Target Implementation Date:

March 2015.

Responsible Officials:

Maura McNerney, Controller, Vice President and Elizabeth M. Schafer, Treasurer

Management believes this report contains both proprietary and other business sensitive information that may be exempt from disclosure under the Freedom of Information Act (FOIA). This information would be of potential benefit to individuals seeking to defraud the Postal Service. This entire report should be exempted from disclosure due to its confidential nature as under good business practices it would not be publically disclosed.

Scott G. Davis
Manager SOX Management Controls and Integration

Elizabeth M. Schafer
Treasurer

cc: Joseph Corbett
Maura McNerney
Manager, Corporate Audit Response Management

Attachment A

Table 2 . Click-N-Ship Revenue and Chargeback Data - Revised

Click-N-Ship	FY 2012	FY 2013
Revenue	$ 490,375,618	$ 535,865,15
Chargebacks (percentage of revenue)	$ 6,081,804 1.24%	$ 4,632,82 0.86
Best Practice Threshold (0.90 percent of revenue)	$ 4,413,381	$ 4,822,78
Chargeback Variance > 0.90 percent of revenue	$ 1,668,423	$ -
FYs 2012/2013 Chargeback Variance Total		$ 1,668,42

July 22, 2014

LORI LAU DILLARD
ACTING DIRECTOR, AUDIT OPERATIONS

SUBJECT: eCommerce Customer Registration Report Number IT-AR-14-DRAFT

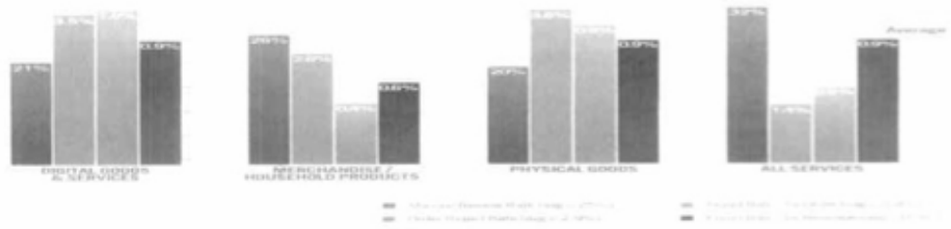
The United States Postal Service has reviewed and disagrees with the findings of Recommendation #1, concerning the level of credit card fraud. We agree with the monetary impacts with the simple mathematical calculation performed, however the United States Postal Service management does not agree with the metric recommendation of .35 percent that was used to perform the calculation.

RECOMMENDATION #1:
We recommend the executive vice president, Chief Marketing and Sales Officer, in coordination with the vice president, Retail Channel Operations, direct the program managers for Click-N-Ship, Every door Direct Mail, Premium Forwarding Service, and the Postal Store to:

1. Establish thresholds for acceptable levels of credit card fraud for their program areas to help determine when escalation of oversight and additional controls are needed.

Management Response/Action Plan:
The OIG audit report states that the industry best practice for fraud related card-not-present chargebacks is 0.35 percent of revenue but the source is not cited in the report. Based on the graph below from the 2013 Online Fraud Report sponsored by CyberSource, a wholly owned subsidiary of Visa, the Fraud Rate by Revenue varies based on the product being sold (industry). For digital goods and services which Click-N-Ship, Every Door Direct Mail, Premium Forwarding Service, and the Postal Store would fall under, the rate is 0.9 percent of revenue. For all industries, the rates in the report are substantially above the 0.35 percent used in the OIG audit report.

KPIs BY SELECT INDUSTRIES



Today eCommerce programs have a goal of 0 percent for fraudulent chargebacks set by the CMSO. To achieve this goal, we have worked closely with Treasury and the Inspection Service groups to better understand the activities of our fraudsters and have implemented fraud detection software. This allows us to be more proactive in our battle against fraudulent transactions and allows us to monitor all transactions activity 24 x 7 x 365.

We continue to identify ways to reduce fraud as the industry continues to adopt new methods to combat fraud. As a result of these efforts, our fraud has declined from a high of 1.31 percent of chargebacks versus revenue in FY12 to a projected 0.26 percent in FY14. We expect to continue to drive this percentage down over time. Without our current fraud prevention efforts, chargeback levels would be constantly escalating.

The OIG audit report implies that as a result of no formal threshold having been established that there is no oversight or escalation process being utilized and that no effort has been undertaken to reduce the fraud chargeback levels. In conjunction with our current fraud detection activities and the enhancements that are scheduled to be implemented in late 2014 and early 2015, a reporting process that provides revenue visibility to senior management within the CMSO and CFO functional areas also includes chargeback information. Going forward and to satisfy the OIG's concern regarding fraud escalation, we will send a monthly Fraud/Chargeback report to senior management so that they are fully aware of our fraud levels month over month.

We feel the OIG recommendation is a step backwards in our efforts. We need to continue to improve with technology our proactive efforts to reduce and prevent fraudulent activity.

Target Implementation Date:
December 2014

Responsible Official:
Patti Mason, Mgr. Digital Media
Brad Parish, PM. Click-N-Ship
Loretta Tolliver, A/Mgr, Retail Services, PFS

We believe that there are elements of the report that contains commercially sensitive information and concur with the suggested redactions contained in the response from Finance.

Shirani Gambhir (for Nagisa Manabe)
NAGISA M. MANABE
CHIEF MARKETING AND SALES OFFICER
AND EXECUTIVE VICE PRESIDENT

Kelly M. Sigmon
KELLY SIGMON
VICE PRESIDENT RETAIL CHANNEL 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, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100