PAYMENT CARD DATA SECURITY:
Consumer information is safer

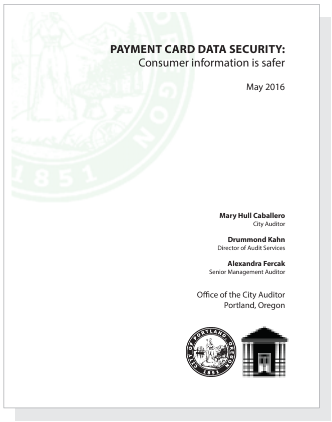
May 2016

Mary Hull Caballero
City Auditor

Drummond Kahn
Director of Audit Services

Alexandra Fercak
Senior Management Auditor

Office of the City Auditor
Portland, Oregon



PAYMENT CARD DATA SECURITY:
Consumer information is safer

May 2016

Mary Hull Caballero
City Auditor

Drummond Kahn
Director of Audit Services

Alexandra Fercak
Senior Management Auditor

Office of the City Auditor
Portland, Oregon

Production / Design
Robert Cowan
Public Information Coordinator

Portland City Auditor
Audit Services Division

Auditor Mary Hull Caballero
Director Drummond Kahn

May 11, 2016

TO:
Mayor Charlie Hales
Commissioner Nick Fish
Commissioner Amanda Fritz
Commissioner Steve Novick
Commissioner Dan Saltzman
Fred Miller, Chief Administrative Officer, Office of Management and Finance

SUBJECT: Audit report: Payment Card Data Security: Consumer information is safer (Report #486)

The attached report provides results of our follow-up audit of the Bureau of Technology Services and the City's compliance with the Payment Card Industry Data Security Standard.

In 2014, we reported that the City was not in compliance with the standard with its handling of payment card transactions. Certified external assessors now report that the City complies with the standard. The City met compliance by outsourcing payment card processing services and improving data security.

We appreciate the cooperation and assistance we received from management and staff in the Office of Management and Finance.

Mary Hull Caballero

Mary Hull Caballero
City Auditor

Audit Team: Drummond Kahn
Alexandra Fercak

Attachment

cc:
Ken Rust, Chief Financial Officer
Jeff Baer, Chief Technology Officer
Jennifer Cooperman, Treasurer
Dan Bauer, Bureau of Technology Services
Celia Heron, Office of Management and Finance
Christopher Paidhrin, Bureau of Technology Services
Josh Alpert, Office of the Mayor

PAYMENT CARD DATA SECURITY:

Consumer information is safer

In 2014, we reported that the City was not in compliance with the Payment Card Industry Data Security Standard for its handling of payment card transactions. Certified external assessors now report that the City complies with the standard. The City met the standard by improving data security and outsourcing payment card processing services.

History of non-compliance

In a 2014 audit, we reported that the City had not complied with the Payment Card Industry Data Security standard since 2009, and the City had not fully implemented recommendations or remediation steps to secure the processing of payment cards.

The Payment Card Industry Data Security Standard specifies 12 requirements for compliance, and each requirement is divided into a number of sub-categories. Failing tests of any of the sub-categories means failing to meet the overall standard.

The standard applies to merchants, like the City, that accept payment cards, and compliance with the standard is reviewed annually by an outside assessor. The data security requirements help protect both merchants and customers from data breaches and fraud. City policies and the City's contract with a major bank for card processing require that the City comply with this standard.

Figure 1 **Payment Card Industry Data Security Standard**

Goals	Requirements
Build and maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Source: Payment Card Industry Security Standards Council

In 2015, more than 10 million payments were made to the City using credit cards or debit cards. Payment cards are used for an increasing number of payments to the City. These range from payments for parking in City-owned garages to payments for monthly water and sewer service to payments for participating in Parks and Recreation classes. The City has been out of compliance with the standard since 2009, according to annual outside reviews.

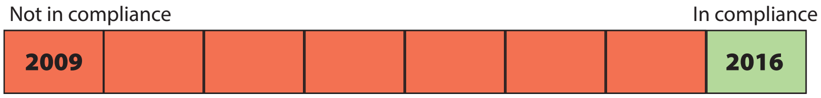
The City did not meet the standard because it had not prioritized payment card security or designated sufficient resources to address compliance. In addition, authority over payment card data security was not clearly defined.

In 2014, we recommended that the Bureau of Technology Services work with City bureaus to implement data security remediation steps and identify compliance-related funding needs. We also recommended that the City Treasurer emphasize compliance with the standard.

The City achieved compliance

Reports from the City's outside assessor show that Parks and Recreation Bureau facilities and city-owned parking garages are now compliant with the standard, as is the City's payment gateway system.

Figure 1 **City of Portland PCI Data Security Standard compliance**



Source: Audit Services analysis of Bureau of Technology Services data

The City achieved compliance by outsourcing selected payment card processing practices. Vendors under contract to the City provide data encryption, and the City removed payment card data from the City's technology network.

The City also clarified roles and responsibilities regarding compliance and implemented procedures and training, including:

- All payment card transactions, assets, processes and procedures are documented by the bureau or department processing payments
- Governance for all payment card standard-related policy, processes and procedures resides with the City Treasurer
- Administrative governance, auditing, monitoring and reporting of payment card standard-related services reside within the Information Security Office
- Operational management and supervision resides with the respective bureaus, who are accountable to the City Treasurer and Information Security Office for compliance with the standard
- The Bureau of Technology Services is to provide extensive assets, services and controls to securely maintain cardholder data
- The Information Security Office has been tasked with:
    - developing and maintaining regularly updated standard training courses through a citywide training system
    - in collaboration with Technology Services, changing control processes, and continuously assessing the scope of standard-related services, systems and assets within the City

- in collaboration with the City Treasurer, regularly assessing the City's payment card standard program for effectiveness and opportunities for improvement
- in collaboration with Technology Services' technical teams, regularly assessing the City's standard related infrastructure, services and data channels

The City discontinued some payment options to achieve compliance

The City discontinued some of its payment card processing options, such as electronic recurring payments for water bills and collection of building permit fees over the phone, because they did not comply with the standard. City bureaus together with Technology Services are working on upgrading these payment processing options to comply with the standard.

Management Response

We shared a copy of this report with the City Treasurer, Bureau of Technology Services, and the Mayor's Office. Response is attached.

Objective, Scope and Methodology

The objective of our audit was to determine the actions taken by the City to implement the recommendations in our 2014 audit report on payment card processing. We obtained and reviewed Reports of Compliance with the Payment Card Industry Data Security Standard issued by the City's outside assessor and letters and Attestation of Compliance submitted to the City's bank. We interviewed the City's information security manager and obtained documentation from the Office of Management and Finance. We also reviewed work papers from our November 2014 audit report on payment card processing.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

RESPONSE TO THE AUDIT

Charlie Hales, Mayor
Fred Miller, Chief Administrative Officer
1120 SW Fifth Ave., Suite 1250
Portland, Oregon 97204-1912
(503) 823-5288
FAX (503) 823-5384
TTY (503) 823-6868

CITY OF PORTLAND

OFFICE OF MANAGEMENT AND FINANCE

To: Drummond Kahn, Director of Audit Services
Alexandra Fercak, Management Auditor

From: Fred Miller, Chief Administrative Officer Fred

Date: May 6, 2016

Subject: Follow-up Audit to the PCI Compliance Audit

Thank you for the opportunity to review your brief audit that followed up on the audit you issued in November 2014 on the City's compliance with Payment Card Industry standards.

We appreciate that you highlighted the work that was completed which required several bureaus to make significant changes to their business process. We will continue our efforts to ensure the City remains compliant with PCI standards.

Audit Services Division
Office of the City Auditor
1221 SW 4th Avenue, Room 310
Portland, Oregon 97204
503-823-4005
www.portlandoregon.gov/auditservices

Payment Card Data Security: Consumer information is safer

Report #486, May 2016

Audit Team: Alexandra Fercak

Mary Hull Caballero, City Auditor
Drummond Kahn, Director of Audit Services

Other recent audit reports:

Technology Projects: Lack of governance hurts City projects and disaster planning (#460B, February 2016)

City Council Grants: No competition and limited oversight (#479, January 2016)

Portland Development Commission: Management of on-call contracts inconsistent with Commission expectations (#474, January 2016)

This report is intended to promote the best possible management of public resources. This and other audit reports produced by the Audit Services Division are available for viewing on the web at: www.portlandoregon.gov/auditor/auditservices. Printed copies can be obtained by contacting the Audit Services Division.