BUREAU OF TECHNOLOGY SERVICES:
City fails to comply with payment card industry standard

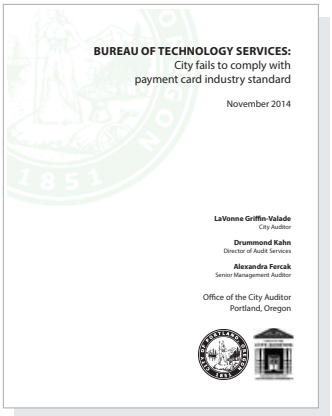
November 2014

LaVonne Griffin-Valade
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

CITY OF PORTLAND

Office of City Auditor LaVonne Griffin-Valade

Audit Services Division
Drummond Kahn, Director
1221 S.W. 4th Avenue, Room 310, Portland, Oregon 97204
phone: (503) 823-4005
web: www.portlandoregon.gov/auditor/auditservices

November 18, 2014

TO: Mayor Charlie Hales
Commissioner Nick Fish
Commissioner Amanda Fritz
Commissioner Steve Novick
Commissioner Dan Saltzman
Fred Miller, Chief Administrative Officer
Ben Berry, Chief Technology Officer
Jennifer Cooperman, City Treasurer

SUBJECT: Audit Report – *Bureau of Technology Services: City fails to comply with payment card industry standard* (Report #460A)

The attached report provides the results of our audit of the Bureau of Technology Services (BTS) and the City's compliance with the international payment card industry data security standard.

We found that since 2009, the City has remained out of compliance with the payment card industry data security standard. The City has never complied with all of the standard's requirements, and the City has not fully implemented recommendations or remediation steps to secure payment card processing.

The payment card data security standard is in place for merchants, like the City, that accept payment cards, in order to help protect both merchants and customers from data breaches and fraud. City policies and the City's contract with a major bank require that the City comply with this standard.

The audit recommends that the BTS should work with City bureaus to achieve full compliance with the payment card industry standard. We also recommend that the City Treasurer emphasize compliance with the standard by City bureaus accepting payment cards.

We ask that the Office of Management & Finance (OMF) provide us with a status report within one year detailing actions steps taken to implement the audit recommendations. We appreciate the cooperation and assistance we received from management and staff at OMF.

LaVonne Griffin-Valade
City Auditor

Audit Team: Drummond Kahn
Alexandra Fercak

Attachment

BUREAU OF TECHNOLOGY SERVICES:

City fails to comply with payment card industry standard

Summary The City of Portland collects a variety of payments from residents and visitors. In 2013, more than 9 million payments were made to the City using credit cards or debit cards. Payment cards, including those from major issuers like Visa and MasterCard, 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 utility service to payments for participating in Parks and Recreation classes.

An international standard, the Payment Card Industry (PCI) data security standard, is in place for merchants, like the City, that accept payment cards. The City and an outside contractor review the City's compliance with this international standard annually. The standard is important to help protect both merchants and customers from data breaches and from fraud. City policies and the City's contract with a major bank for card processing require that the City comply with this standard.

Annual outside reviews of the City's payment card processes since 2009 found that the City is out of compliance with the international standard. The City has never complied with all of the standard's requirements. The last review, in September 2013, concluded that the City's major card accepting units are "not fully compliant" with the standard. The City has not fully implemented recommendations or remediation steps to secure payment card processing.

Payment card data breaches and fraud are on the rise, costing organizations millions of dollars. Failing to comply with the international payment card standard places an organization at increased risk for fraud and data breaches, potentially exposing individuals' payment card data and violating the public's trust.

The City has not prioritized payment card security, and according to Bureau of Technology Services management, the City has not designated sufficient resources to address compliance with the payment card standard. In addition, authority over City payment processes is not clearly defined.

We recommend that the Bureau of Technology Services should work with City bureaus to implement PCI data security remediation steps and identify compliance related funding needs. We also recommend that the City Treasurer emphasize compliance with the payment card industry standard.

Background

City of Portland processes millions of payment card transactions

The City has various locations and operations that accept debit cards and credit cards (known as "payment cards"). For example, City-owned parking garages, parking meters, streetcar ticket machines, Parks and Recreation facilities, online payment of taxes and fees, and the Water and Environmental Services Bureaus (water and sewer service) all accept payment cards. Payment card transactions are processed using the city-developed Payment Gateway system and third party payment processing vendors used at City recreation facilities and parking garages. Payment card transactions for City services are routed from these City payment systems to a major bank for authorization. The City reports its compliance or non-compliance annually to this processing bank.

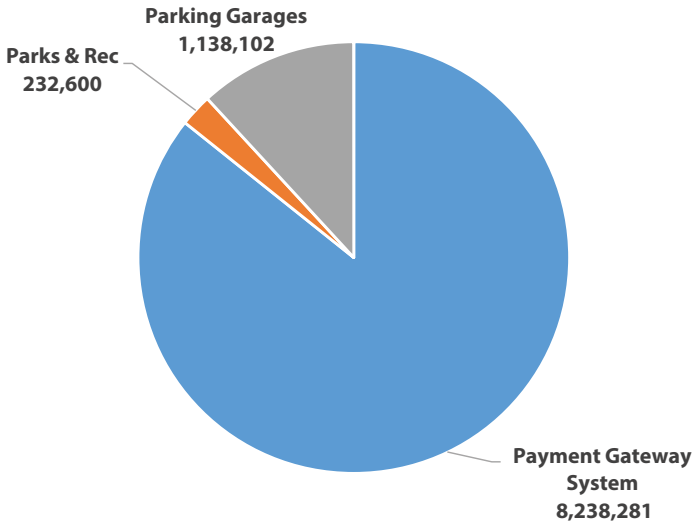
The City's card payment processing that is subject to the PCI data security standard falls into three areas:

City's Payment Gateway System
Current users are the Bureau of Transportation, Bureau of Development Services, Bureau of Environmental Services, Water Bureau, Revenue Bureau, and Bureau of Planning and Sustainability. Payments include permit and inspection fees, payment for water and sewer services, Multnomah County business taxes, and payment of City taxes.

City-Owned Parking Garages
The City owns six parking garages. Payments include fees to park in these garages.

Parks and Recreation Facilities
The City of Portland owns and operates 13 pools, 11 community centers, eight community schools, four art centers, one tennis center, and parks. Payments include registration fees for users to swim, attend classes, or reserve time on tennis courts.

Figure 1 **Number of Payment Card Transactions Processed by the City of Portland** (Sept 2012 - Aug 2013)



Source: Bureau of Technology Services

During the period from September 2012 through August 2013, the City processed over 9.6 million payment card transactions. This number continues to increase each year, as more City business is conducted online with payment cards, and the public increasingly uses payment cards.

Payment Card Industry Data Security Standard is required

Since 2008, there have been nationwide increases in attacks on payment processes and increases in merchant data breaches. The cost of data breaches in the United States has been increasing, with an average of $201 per record compromised or a total of $5.9 million for 2013, according to the Ponemon Institute. In addition, public trust is affected when cardholder data is breached and exposed to fraud.

The Payment Card Industry (PCI) Data Security Standard is a comprehensive set of 12 international requirements created and maintained by the PCI Security Standards Council, which represents the major card brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc.). The standards are used to verify that merchants and service providers are appropriately protecting cardholder data.

All merchants and organizations that store, process or transmit cardholder data are covered by this PCI data security standard. The standard covers all forms of payment card – debit, credit, and merchant and company purchasing cards – representing the majority of payment cards issued globally. With the exception of the State of Nevada, which incorporated the standard into state law, compliance with the standard is enforced by the major card brands through contractual agreements with banks and merchants.

The PCI Security Standards Council developed the standard to protect the public's cardholder information and to reduce the likelihood of fraud. It requires organizations to maintain a secure network, implement internal controls and perform regular testing. These controls cover everything from encrypting stored data to conducting vulnerability assessments and configuring access controls. Although compliance with the standard does not guarantee that payment systems will not be breached, the standard offers a baseline of technical and operational requirements to protect cardholder data.

The PCI data security standard is the most widespread and established standard of its kind, and there is evidence that the standard is effective in lowering security risks. The standard applies to all merchants, regardless of how many transactions they process. However, merchants that process over 6 million transactions per year (Level 1 merchants), are required to assess compliance onsite using an outside assessor instead of conducting self-assessments. The City processes more than 6 million transactions a year, and is considered a Level 1 merchant.

Figure 2 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

Note: Each requirement is divided into a number of sub-controls. Failing any of the sub-controls leads to non-compliance with the requirement and with the PCI standard. Although the 12 requirements have not changed since the inception of the standard, the sub-controls have been revised. The latest version 3.0 of the PCI Data Security Standard is effective starting on January 2015.

Each transaction processed, regardless of the dollar value, transmits card holder data, and organizations with a high number of transactions are processing a large volume of data. Organizations are reported as either 'fully compliant' or 'not compliant' with all 12 requirements.

Since the establishment of the standard in 2006, each year organizations are complying at a higher rate. By December 2013, 97 percent of organizations that process over 6 million payment card transactions annually were fully compliant with the standard, based on reports from Visa, Inc.

Audit Results

City of Portland is not compliant with payment card standard

The City's information technology and financial policies require compliance with the PCI data security standard. In addition, the City has a Merchant Services Contract with a major bank, which requires the City to comply with the standard. The City contracts with an outside assessor who conducts annual PCI data security reviews, and the results of these reviews are submitted by the City Treasurer to the bank. If the annual review report concludes that the City is not fully compliant, each report is accompanied by remediation steps with target dates for compliance. According to the City's bank, organizations are normally given one year to implement the remediation steps and comply with the standard.

In each year since 2009, the City's first year of external review, the City has not complied with the PCI data security standard. The City has not implemented all recommendations and remediation steps in order to secure payment card processing for the public. Instead, as demonstrated by the annual reviews, the City continues to be out of compliance with many of the requirements, and various payment card data security weaknesses persist.

Figure 3 **City of Portland PCI data security standard compliance rate**
(number of requirements complied with, by payment area)

Payment area	2009	2010	2011	2012	2013
Payment Gateway System	5/12	5/12	7/12	6/12	7/12
Parks & Recreation	1/12	7/12	7/12	7/12	7/12
Parking Garages	5/12	7/12	9/12	6/12	10/12

Source: Audit Services analysis of Bureau of Technology Services data

Note: The PCI Data Security Standard specifies 12 requirements for compliance, and each requirement is divided into a number of sub-controls. Failing any of the sub-controls leads to non-compliance with the related requirement and leads to non-compliance with the PCI data security standard.

City has not prioritized payment card security

The City's compliance with PCI data security standard has not been enforced. City policy directs BTS to provide authority and governance for information security policies and standards. BTS is responsible for enforcing these policies, including compliance with the PCI data security standard, on a City-wide basis. City policy also directs the City Treasurer to consult with BTS prior to approving bureaus' requests to accept and process payment cards. In addition, the City Treasurer signs and submits the annual PCI data security compliance reports to the bank, confirming that the City recognizes it must at all times maintain full compliance with the PCI data security standard. However, according to BTS and the City Treasurer, neither has the authority to enforce compliance by City bureaus.

The City has not prioritized compliance with the payment card security standard and according to BTS management, it has not designated sufficient resources to City-wide payment card data security. Currently, BTS' information security division, has the equivalent of four full-time positions, down from five positions in 2011. In addition, instead of reporting non-compliance to City Council, each year since 2009 the performance measure in BTS' adopted budget reports a 100 percent compliance with payment card standard.

Non-compliance carries risks

Continued non-compliance with the PCI data security standard may lead to fines imposed by the card brand network. According to the City's bank, these fines may be up to $500,000 per year. Moreover, Visa Inc. announced in October 2014 that it is enhancing their PCI standard enforcement plan beginning in January 2015. The City's bank told us they will work with the City on achieving full compliance.

Non-compliance with the PCI standard also exposes the City to legal challenges and significant costs in the case of cardholder data breach or fraud. In addition, the public expects that the City will protect their sensitive information and data, and a data breach could have significant impact on the public's trust.

Recommendations

Given that PCI data security compliance requires coordinated efforts by the City Treasurer, Bureau of Technology Services, City bureaus and Council, we make the following recommendations:

1. **BTS should work with bureaus to implement Citywide remediation steps. BTS should assist bureaus to identify PCI compliance-related funding needs and communicate these to Council.**

2. **The City Treasurer should work with Council and the City's bank to enforce Citywide recommended remediation steps in order to achieve full compliance with the payment card industry standard.**

Objective, scope and methodology

This audit report is the first part of an audit of the Bureau of Technology Services. The objective of the audit was to review the City's application of Information Technology Project Management Controls and compliance with Payment Card Industry (PCI) data security standard and best practices. The audit also includes an identification of City's obstacles to developing an information technology disaster preparedness and recovery plan. The Information technology project management controls and disaster preparedness components of our audit work will be issued in a separate report in 2015.

To accomplish our audit objective, we reviewed City policies and procedures related to payment card processing. We reviewed the City's payment card environment and the annual Reports of Compliance with PCI data security standard. To gain an understanding of the City payment card data security oversight and governance, we interviewed Bureau of Technology Services management, the City Treasurer, staff from the City Attorney's Office, and management from Parks and Recreation and City parking garages. We also interviewed the PCI data security standard auditors who conduct the City's annual assessment, and the City's bank compliance officer.

To identify PCI data security compliance requirements and best practices, we reviewed the Payment Card Industry Security Standards Council reports and guidance. We also reviewed the major bank card brand's requirements for payment card data. To gain an understanding of PCI data security compliance trends and data breaches across various industries, we reviewed research from national organizations and data security companies, and audits from other jurisdictions.

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: LaVonne Griffin-Valade, City Auditor

From: Fred Miller, Chief Administrative Officer Fred Miller

Date: November 13, 2014

Subject: Response to Audit – Bureau of Technology Services

The letter is in response to your November 2014 audit of the Bureau of Technology Services focusing on the City's compliance with Payment Card Industry (PCI) Standards.

I concur with the audit's overall assessment that the City of Portland is currently not in compliance with PCI standards. I also agree that City Council and City staff should make PCI compliance – and information security in general – a high priority for its staffing and resources.

OMF concurs with the two recommendations of the audit and will continue to work with City bureaus, as well as within BTS, to remediate, achieve, and maintain 100% compliance with PCI standards.

BTS will play an essential role working with bureaus to identify the steps those bureaus need to take to achieve PCI compliance. As appropriate, BTS can assist bureaus in developing cost estimates for those remedial actions. From there, it will be a shared responsibility of the City bureaus – and City Council – to identify and prioritize the resources to meet the respective funding needs.

The City Treasurer will work closely with the Council and bureau directors to comply with the recommended remediation steps, including working with the Council to enforce specific actions.

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

Bureau of Technology Services: City fails to comply with payment card industry standard

Report #460A, November 2014

Audit Team: Alexandra Fercak

LaVonne Griffin-Valade, City Auditor
Drummond Kahn, Director of Audit Services

Other recent audit reports:

City of Portland 24th Annual Community Survey results (#463, October 2014)

B.E.S. Columbia Building: Scope additions and ineffective design oversight led to substantially higher project costs (#446B, October 2014)

Portland Development Commission: Human resources and payroll practices functioning effectively (#458, August 2014)