New York State Office of the State Comptroller
Thomas P. DiNapoli

Division of State Government Accountability

Compliance With Payment Card Industry Standards

Central New York Regional Transportation Authority

Report 2016-S-31 February 2017

Executive Summary

Purpose

To determine whether the Central New York Regional Transportation Authority (Authority) complies with Payment Card Industry (PCI) security standards. Our audit scope covers the period January 1, 2015 through June 24, 2016.

Background

The Authority provides transportation services in Onondaga, Oswego, Cayuga, and Oneida counties. The Authority accepts credit cards as a method of payment for bus fares and parking. All organizations that accept credit cards as a method of payment, such as the Authority, must comply with the Data Security Standards (DSS) established by the PCI Security Standards Council (Council). The PCI DSS is a set of technical and operational requirements designed to protect cardholder data. Entities that do not comply with PCI DSS may be subject to fines and penalties, and lose the public's confidence and the ability to accept credit card payments. In calendar year 2015, the Authority reported 40,822 credit card transactions totaling more than $900,000 in revenue.

Key Findings

- We reviewed select operational and technical security controls over the protection of cardholder data at the Authority. Based on our review, we identified several matters that management should address to improve the Authority's information security program for cardholder data and to help ensure it meets PCI requirements.
- The Authority has not yet developed and disseminated an Information Security Policy that clearly defines information security responsibilities for all personnel. Also, it has not inventoried all devices that process cardholder data, implemented a formal risk assessment process to identify threats to cardholder data, ensured all devices that process cardholder data are physically secured, or implemented appropriately strong network user account and password controls.
- The Authority could also improve certain other technical safeguards over the cardholder data it processes.

Key Recommendations

- Develop strategies to enhance compliance with PCI DSS.
- Implement the recommendations detailed during the audit for strengthening technical controls over cardholder data.

Other Related Audits/Reports of Interest

Office of Information Technology Services: Security and Effectiveness of Department of Motor Vehicles' Licensing and Registration Systems (2013-S-58)

State University of New York: Compliance With Payment Card Industry Standards (2015-S-65)

State of New York
Office of the State Comptroller

Division of State Government Accountability

February 6, 2017

Mr. Brian Schultz
Chairman
Central New York Regional Transportation Authority
200 Cortland Avenue
P.O. Box 820
Syracuse, NY 13205-0820

Dear Mr. Schultz:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage government resources efficiently and effectively. By doing so, it provides accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit of the Central New York Regional Transportation Authority entitled *Compliance With Payment Card Industry Standards*. The audit was performed pursuant to the State Comptroller's authority as set forth in Article X, Section 5 of the State Constitution and Article II, Section 2803 of the Public Authorities Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this report, please feel free to contact us.

Respectfully submitted,

Office of the State Comptroller
Division of State Government Accountability

Table of Contents

State Government Accountability Contact Information:
Audit Director: John Buyce
Phone: (518) 474-3271
Email: StateGovernmentAccountability@osc.state.ny.us
Address:
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

This report is also available on our website at: www.osc.state.ny.us

Background

The Central New York Regional Transportation Authority (Authority) is a public benefit corporation that was created in 1970 to provide transportation services in Onondaga, Oswego, Cayuga, and Oneida counties. The Authority has a separate transportation system for each county served. Its main service area is the City of Syracuse and Onondaga County. The Authority operates a fleet of 237 buses 365 days a year, and its vehicles travel approximately 6 million miles and carry roughly 12 million passengers each year.

Customers can purchase bus passes at 37 different locations throughout central New York, including Authority transit hubs and offices, a bank, colleges, check-cashing businesses, a drug store, and supermarkets. These retailer locations purchase the passes in bulk and process payment card transactions on their own systems. In addition, the Authority processes credit card payments on its own systems, including: two ticket vending machines in Syracuse and another in Utica, the reception desk at the main office in Syracuse, the service window at the transportation hub in Utica, and four self-service parking kiosks and one payment card reader at the Syracuse Regional Transportation Center service window. Also, the Authority operates an online store where customers can purchase bus passes with a credit card.

All organizations that accept credit cards as a method of payment, such as the Authority, must comply with the Data Security Standards (DSS) established by the Payment Card Industry (PCI) Security Standards Council (Council). The PCI DSS is a comprehensive set of technical and operation requirements addressing security management, information security policies and procedures, network architecture, software design, and other critical protective measures associated with credit card data. It is intended to help organizations proactively protect customer credit card data that is either stored, processed, or transmitted. The requirements apply to all system components included in, or connected to, the Cardholder Data Environment (CDE). The CDE comprises people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data. “System components” include network devices, servers, computing devices, and applications.

About 25 percent of the Authority’s revenues come from passenger fares, which totaled about $16 million in FY 2014-15 according to the Authority’s audited financial statements. In calendar year 2015, the Authority reported 40,822 credit card transactions totaling more than $900,000 in revenue.

Audit Findings and Recommendations

We reviewed select operational and technical security controls over the protection of cardholder data at the Authority. Based on our review, we identified several matters that management should address to improve the Authority's information security program for cardholder data and to ensure it meets PCI requirements. For example, the Authority has neither established nor disseminated an Information Security Policy that addresses all PCI DSS requirements, nor has it implemented a formal risk assessment process to identify threats to cardholder data as required. Furthermore, to date the Authority has only issued limited guidance regarding security over confidential data, including credit card information. In addition, the Authority has not yet inventoried all devices that process cardholder data, ensured that all devices that process cardholder data are physically secured, or implemented appropriately strong network user account and password controls. Finally, we identified certain other technical controls in the Authority's systems that did not appropriately or fully address PCI requirements.

As a result of our audit, the Authority has already taken various actions to bolster its security over cardholder data, including conducting technical testing of systems handling cardholder data and addressing certain technical issues that we identified during our audit. However, the Authority still needs to take additional steps to improve its overall information security program to ensure it meets PCI DSS.

Payment Card Industry Compliance

To achieve PCI DSS compliance, an organization must meet all PCI DSS requirements. The PCI DSS comprises 12 high-level requirements and over 200 sub-requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. These requirements cover information security domains such as firewall configuration, system hardening, physical security, vulnerability management and patching, application security, and wireless controls.

We reviewed select Authority operational and technical data security controls over cardholder data and found several matters that require management's attention. Several weaknesses existed because the Authority had not yet effectively implemented certain core elements of an information security program over cardholder data. Recently, the Authority initiated an assessment (i.e., PCI self-assessment) to evaluate its compliance with PCI DSS. As the Authority moves forward with this process, management should take prompt actions to address our audit recommendations to better ensure that the Authority meets PCI DSS requirements.

Cardholder Data Security Program

Failing to integrate PCI DSS security processes into daily business and operational procedures, monitor security controls on a continuous basis, and maintain compliance at all times could leave organizations more susceptible to security control failures, malicious attack, and accidental information leakage. Ongoing compliance also requires centralized coordination of numerous

resources, actions, projects, and people. As a result, the Council recommends that specific individuals be assigned overall responsibility for these activities, be qualified to perform such functions, and be given adequate funding and the proper authority to effectively organize and allocate such resources appropriately.

An Information Security Policy (Policy) is an essential component of an organization's information security program, and is also a requirement of PCI DSS. The Policy helps an organization to define the security controls, requirements, and processes that facilitate the protection and confidentiality of its systems, network, and data. It also includes information on the rules of behavior that users are expected to follow, baselines for security controls, and security roles and responsibilities among staff. Documenting and assigning staff responsibilities within an organization's information security program will help to ensure that appropriate resources have been allocated to fully address security requirements, controls, and processes. Further, the Policy should be disseminated to all staff so they are aware of the sensitivity of the organization's data as well as their responsibilities for protecting it.

We found the Authority does not have a Policy that clearly defines information security responsibilities for all personnel. Further, management has not yet fully implemented other key components of a comprehensive information security program that are required by PCI DSS, including:

- Establishing a formal security awareness program to make all personnel aware of the importance of cardholder security;
- Implementing a formal process for identifying security vulnerabilities to the CDE;
- Tracking and monitoring all access to network resources and cardholder data;
- Implementing a formal risk assessment process to identify threats to cardholder data; and
- Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.

The security controls, requirements, and processes that are defined within the Policy should be further supported by supplementary procedures that provide more detailed information on the implementation of the control. Within the PCI DSS, comprehensive procedures are required for controls such as firewall and router maintenance, encryption of data transmissions, network and web application vulnerability scanning, user access controls, and physical security. However, we found that the Authority does not yet have documented procedures detailing the implementation of these PCI DSS-related security controls. Based on discussions with Authority officials, there are only informal word-of-mouth procedures in place.

Officials indicated resource limitations have inhibited their ability to implement a comprehensive information security program over cardholder data. Further, they acknowledged that the Authority needs to make improvements in its overall cardholder data security program. In response to our findings, officials indicated the Authority was finalizing an agreement with a cybersecurity consultant to facilitate comprehensive corrective action related to its cardholder data security program.

Physical Access Controls

PCI DSS requires that video cameras or other access control mechanisms (e.g., badge systems, door controls, and locks) be used to monitor physical access to sensitive areas and the CDE. Without the use of such controls, unauthorized persons could potentially gain access to the facility to steal, disable, disrupt, or destroy critical systems and cardholder data.

During our on-site review, we observed that there are no security cameras at the front desk in the Syracuse main office, nor is the office locked. This office also serves as the only access point to the area where the customer service representatives work, some of whom have no role in the processing of payment cards. Furthermore, we observed the video feeds from all of the remote payment card processing locations, and found that one ticket vending machine, four parking machines, and a payment card processing terminal were not monitored by on-site cameras. In addition, we noted that the Authority's camera system only retained video data for one month, as opposed to the three months recommended by PCI standards.

User Access Controls

To ensure that critical data can only be accessed by authorized personnel, PCI DSS requires that systems limit access based on "need to know" and according to job responsibilities. Need to know is when access rights are granted to only the least amount of data and privileges needed to perform a job. Accounts with access to an organization's CDE that are inactive (i.e., not used a regular basis) are often targets of attack due to the lower likelihood that administrative staff will notice modifications to them. To help organizations mitigate this risk, PCI DSS dictates that inactive user accounts be deleted or disabled from accessing the CDE after 90 days of inactivity. PCI DSS also requires that organizations implement a strong password policy within their information security program. This helps to ensure all account passwords in use are secure and have a level of complexity that will hinder an intruder's ability to identify them.

During our testing, we determined that the Authority could improve its user access controls. For example, of the 302 total active system users, 62 had some type of generic ID. PCI DSS requirements specifically state that group, shared, or generic IDs should not be used.

We also found that the Authority has not removed or disabled accounts within 90 days of inactivity as required by PCI DSS. Specifically, we identified 30 Authority accounts that would be considered inactive by PCI DSS standards. Of these 30 inactive accounts, nine belonged to an administrative domain group that had elevated privileges, and thereby increased the risk associated with these accounts. If an intruder compromised a privileged inactive account, the intruder would have escalated rights over all systems within the CDE, including those systems processing credit card data.

We also found that the Authority's domain policy, which governs its network password policy and passwords for some components of the CDE, did not meet PCI DSS's complexity requirements. To lessen the threat of dictionary or brute-force password attacks (i.e., automated attacks with special software that attempt to determine passwords by trying hundreds or sometimes millions

of likely possibilities, such as words in a dictionary), an organization should ensure all passwords in use on CDE components require an increased level of complexity by using multiple-character sets.

During our testing, we also found that of the 302 active Authority domain accounts, 146 had passwords that were considered stale by PCI DSS requirements and had not been changed in over 90 days. Further, 33 of the stale accounts were also part of the aforementioned administrative domain group, which had advanced privileges over systems within the CDE. If an intruder identified the stale password for a privileged account, the intruder would be able to more easily leverage the administrative access to gain unauthorized access to the CDE and credit card data. The Authority can help to mitigate this risk by: ensuring passwords are changed or updated on a 90-day cycle; and auditing those passwords belonging to privileged accounts to confirm they have been updated within the defined password policy time frame.

Completeness of Payment Card Industry Inventories

We found that the Authority maintained an overall inventory for all of their technology assets, but did not specifically distinguish those devices that process cardholder data. As stated in the PCI DSS, "maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing PCI DSS controls. Without a complete inventory, some system components could be forgotten, and be inadvertently excluded from the organization's configuration standards." System components operating without the proper PCI specific security controls significantly increase the risk of unauthorized access to cardholder data.

Recommendation

1. Develop strategies to enhance compliance with PCI DSS. This should include, but not be limited to:

    - Developing and disseminating a Policy and procedures that clearly define information security responsibilities for all personnel;
    - Inventorying all assets related to payment card processing activities;
    - Strengthening physical security over all systems that receive, process, transmit, and maintain cardholder data; and
    - Meeting PCI DSS user account and password requirements.

Technical Controls

During our testing, we identified technical controls in the CDE that did not appropriately or fully address PCI requirements. Due to their confidential nature, we reported these matters to officials in a separate report and, consequently, do not address them in detail in this report. If these matters are not adequately addressed, the Authority could be exposed to unnecessary risks if a breach occurs. These risks include not only potential unauthorized access to cardholder

data, but also potential fines or penalties if it is determined the Authority is responsible for the security incident. Furthermore, a compromise or breach could negatively impact public opinion or perception of the Authority as a whole. Subsequent follow-up audits will address the detailed findings and recommendations related to CDE technical controls.

Recommendation

2. Implement the recommendations detailed during the audit for strengthening technical controls over cardholder data.

Audit Scope and Methodology

The objective of our audit was to determine whether the Authority complies with Payment Card Industry (PCI) security standards. Our audit scope covered the period January 1, 2015 through June 24, 2016.

To accomplish our objective, we reviewed relevant laws, regulations, and the Authority's policies related to PCI compliance. We also became familiar with and assessed the Authority's internal controls as they relate to payment card handling and processing. We made physical observations at the Authority's payment card processing locations as well as other locations that are connected to the Authority's computer network. We held multiple meetings with Authority officials to gain an understanding of how payment cards are handled and processed as well as an overall understanding of how the Authority addressed PCI DSS. To determine if there were users who should no longer have access to the systems, we compared a list of system users from the active directory with a current list of employees on the payroll. We also reviewed domain user account and password settings along with user login and password change activity. Finally, we reviewed documentation maintained by the Authority related to payment card processing during our scope period.

We conducted our 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 objective. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions, and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating threats to organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Authority

The audit was performed pursuant to the State Comptroller's authority under Article X, Section 5 of the State Constitution and Section 2803 of the Public Authorities Law.

Reporting Requirements

We provided a draft copy of this report to Authority officials for their review and formal comment. Their comments were considered in preparing this report and are attached in their entirety at the end of it. Officials agreed with our findings and recommendations and have indicated they have already taken steps to facilitate comprehensive corrective action.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Chairman of the Central New York Regional Transportation Authority shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

Contributors to This Report

John F. Buyce, CPA, CIA, CFE, CGFM, Audit Director
Nadine Morrell, CIA, CISM, CGAP, Audit Manager
Mark Ren, CISA, Audit Supervisor
Raymond Barnes, Examiner-in-Charge
Jared Hoffman, OSCP, GPEN, GWAPT, Information Technology Specialist
Rachael Hurd, Senior Examiner
Joseph Robilotto, Senior Examiner

Division of State Government Accountability

Andrew A. SanFilippo, Executive Deputy Comptroller
518-474-4593, asanfilippo@osc.state.ny.us

Tina Kim, Deputy Comptroller
518-473-3596, tkim@osc.state.ny.us

Brian Mason, Assistant Comptroller
518-473-0334, bmason@osc.state.ny.us

Vision

A team of accountability experts respected for providing information that decision makers value.

Mission

To improve government operations by conducting independent audits, reviews and evaluations of New York State and New York City taxpayer financed programs.

Agency Comments

Central New York
Regional Transportation Authority

October 28, 2016

Mr. John Buyce
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, New York 12236

Dear Mr. Buyce

The CNYRTA is in receipt of your draft findings regarding the Office of the State Comptrollers PCI Compliance Audit. We agree with the findings and recommendations as stated in the report.

Although some corrective action has been taken to date, we would like to inform you that the CNYRTA has contracted with a cyber-security consultant to help facilitate comprehensive corrective action. The consultant commenced on October 3, 2016 and is expected to conclude their services by January 2017. We are confident, with the help of our consultant, we will be able to address the issues sited in your letters.

Sincerely,

Brian Schultz
CNYRTA, Chairman

Cc: Mark Wren, Office of State Comptroller
Richard Lee, CNYRTA, CEO
Robert LoCurto, CNYRTA, COO