

New York State Office of the State Comptroller
Thomas P. DiNapoli
Division of State Government Accountability

Compliance With Payment Card Industry Standards

Thruway Authority



Executive Summary

Purpose

To determine whether the Thruway Authority (Authority) complies with Payment Card Industry Data Security Standards. Our audit scope covers the period March 1, 2017 through June 5, 2017.

Background

The Authority operates and maintains a toll superhighway (Thruway) throughout New York. Most of the toll points along the Thruway only accept cash and E-ZPass charges as toll payment. All Thruway E-ZPass customers have prepaid accounts, from which tolls are electronically deducted when the vehicle passes through toll points. Most E-ZPass accounts are automatically replenished with the customer's credit card on file. The Authority also accepts in-person credit card payments for E-ZPass tags at its administrative headquarters in Albany and at its Nyack and Tarrytown offices. In addition, the Authority accepts credit card payments over the phone, online, and in person for other costs (e.g., unpaid tolls, accident reports, oversized truck permits, commercial accounts). All organizations that accept credit cards as a method of payment must comply with the Data Security Standards (DSS) established by the Payment Card Industry (PCI) Security Standards Council. The PCI DSS is a comprehensive set of technical and operational requirements addressing security management, information security policies and procedures, and other critical protective measures associated with credit card data – intended to help an organization proactively protect customer credit card data that is either stored, processed, or transmitted through its network. The requirements necessitate that all system components included in, or connected to, the Cardholder Data Environment (CDE) – that is, the people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data – are accounted for and comply with respective requirements. From May 1, 2015 through April 30, 2016, Authority reports indicated it directly processed approximately 66,000 credit card transactions totaling more than \$1.4 million.

Key Findings

- Based on our review of select operational and technical security controls over the protection of cardholder data, 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 taken fundamental steps to secure its network. For example, it had neither classified its data, nor accounted for all of its systems that process or store credit card information. In addition, it had not performed a risk assessment covering its CDE. Unless the Authority performs these key information security program tasks, it will be significantly inhibited in its efforts to meet PCI DSS and State information security standards.
- 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, but not addressed in this report due to confidentiality reasons, for strengthening technical controls over cardholder data.

Other Related Audits/Reports of Interest

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

[Central New York Regional Transportation Authority: Compliance With Payment Card Industry Standards \(2016-S-31\)](#)

**State of New York
Office of the State Comptroller**

Division of State Government Accountability

September 19, 2017

Ms. Joanne M. Mahoney
Chair
Thruway Authority
200 Southern Boulevard
Albany, NY 12209

Dear Ms. Mahoney:

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 Thruway 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

Background	5
Audit Findings and Recommendations	7
Payment Card Industry Compliance	7
Technical Controls	10
Recommendations	10
Audit Scope, Objective, and Methodology	11
Authority	11
Reporting Requirements	12
Contributors to This Report	13
Agency Comments	14
State Comptroller's Comment	16

State Government Accountability Contact Information:

Audit Director: Brian Reilly

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 Thruway Authority (Authority) operates and maintains a toll superhighway (Thruway) throughout New York. The tolled mainline of the Thruway extends for 496 miles from the New York City line at Yonkers to the Pennsylvania state line by way of Albany, Syracuse, and Buffalo. Thruway tolls are collected at controlled entry and exit points. Most of the toll points along the Thruway only accept cash and E-ZPass charges as toll payment. Generally, all Thruway E-ZPass customers have prepaid accounts from which tolls are electronically deducted when the vehicle passes through toll points. Most E-ZPass accounts are funded through a credit card on file and automatically replenished when the balance drops below a set amount. In spring 2016, the Thruway began accepting cashless tolling for the Tappan Zee Bridge, where motorists can pay tolls either through E-ZPass or by mail.

While the Authority has contracted with Conduent to manage Thruway E-ZPass accounts (e.g., setting up accounts, issuing E-ZPass tags, and processing account payments), the Authority itself also directly handles credit card payments in certain circumstances. Specifically, it accepts in-person credit card payments for E-ZPass tags at its administrative headquarters in Albany and at two office locations, in Nyack and Tarrytown. In addition, it accepts credit card payments over the phone, online, and in person for unpaid tolls, accident reports, oversized truck permits, and commercial accounts.

During 2016, the Authority reported that total traffic on the Thruway was 264 million vehicles and toll revenues exceeded \$708 million, with the E-ZPass system accounting for about 79 percent of the net toll revenue collected. From May 1, 2015 through April 30, 2016, Authority reports indicated it directly processed approximately 66,000 credit card transactions totaling almost \$1.4 million.

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 operational requirements addressing security management, information security policies and procedures, and other critical protective measures associated with credit card data. It is intended to help an organization proactively protect customer credit card data that is either stored, processed, or transmitted in its network. The PCI DSS necessitates that all system components included in, or connected to, the Cardholder Data Environment (CDE) are accounted for and comply with their respective requirements. 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.

Besides PCI DSS, State information security standards and policies also contain requirements related to securing credit card information. Specifically, according to the NYS Information Security Policy (NYS-P03-002), all information must be classified on an ongoing basis based on its confidentiality, integrity, and availability characteristics. Based on the State's Information Classification Standard (NYS-S14-002), credit card data should be assessed the highest confidentiality classification.

To ensure State information security policies are followed, the Information Security Policy recommends specific individuals be assigned overall responsibility for risk management and monitoring information security controls, and that their responsibilities be clearly defined.

Audit Findings and Recommendations

Based on our review of select operational and technical security controls over the protection of cardholder data, we identified several matters that management should address to improve the Authority's information security program for cardholder data and ensure it meets PCI requirements. For example, the Authority neither classified its data, nor accounted for all of its systems that process or store credit card information. In addition, the Authority had not performed a risk assessment covering its CDE. Unless the Authority performs these key information security program tasks, it will have difficulty meeting PCI DSS and State information security standards.

As a result of our audit, the Authority has already taken various actions to bolster its security over cardholder data, including strengthening its security procedures and addressing certain technical issues that we identified. 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 information security policies and procedures, network monitoring and testing, physical security, vulnerability management and patching, application security, user access, and protection of cardholder data.

During our audit, we found several weaknesses in the Authority's operational and technical data security controls over cardholder data that require management's attention. Some stem from the Authority not yet having effectively implemented certain core elements of an information security program for cardholder data. In particular, the Authority had not made formal attempts to account for all aspects of its CDE, including the specific systems that handle credit card information. As a result, management was unaware that weaknesses and gaps existed in the security controls over the data and, consequently, could not take timely remedial actions. Going forward, management should address our audit recommendations to better ensure that the Authority meets PCI DSS requirements.

PCI Self-Assessment

According to PCI DSS, the first step of a PCI self-assessment is to accurately identify the CDE and document how it was determined. When defining the CDE, it is essential to evaluate how cardholder data flows through the organization. Ideally, the evaluation of each location and flow where cardholder data appears (i.e., what, when, and how data is obtained) is considered the starting point for such evaluation. The intermediate state (all processing and locations where cardholder data flows) and the end point (how cardholder data leaves the organization) should also be considered. Once determined, this process should be completed and updated on an annual basis.

In essence, the PCI DSS assessment process is an exercise in risk management. Besides identifying the CDE, it also involves assessing technical and operational controls, identifying weaknesses and gaps, and taking the necessary corrective actions. Conducting a PCI DSS self-assessment helps an organization to identify and understand the potential risks to its CDE. By understanding these risks, an organization can prioritize its risk mitigation efforts to address the most critical risks first. The PCI DSS Self-Assessment Questionnaire (Questionnaire) is a validation tool intended to assist entities in annually self-evaluating their compliance with PCI DSS and assessing risk. The Questionnaire includes questions relating to PCI DSS requirements and an “Attestation of Compliance.” Presently, there are eight different Questionnaire types that correlate to the method used to accept credit cards. For example, payment methods involving the storage of cardholder data are subject to more stringent security requirements; therefore, the associated Questionnaire includes more validation steps for an organization to complete. Thus, choosing the right Questionnaire is important because using an incorrect one could invalidate a self-assessment.

Contrary to PCI DSS requirements, the Authority has not attempted to define its CDE even though it processes and stores credit card information on its network. Specifically, it has not formally evaluated how cardholder data flows through the organization nor documented its CDE. In addition, it does not maintain an inventory of system components within the CDE as required by PCI DSS, and has not completed a formal data classification of assets, including those pertaining to credit card processing. Without a complete inventory, some system components could be excluded from the organization’s configuration standards or not securely protected, leaving them vulnerable to security threats.

While the Authority had obtained a recent, completed Questionnaire from its E-ZPass vendor, it has not completed a Questionnaire for itself. At the onset of our audit, management was not aware credit card data was processed or stored by systems on the Authority’s internal network. However, the audit team was able to identify a total of six Authority systems that are used for managing or transmitting credit card data. Authority officials indicated that a risk assessment involving the CDE and PCI DSS requirements has not been completed overall or in any department that handles, processes, or stores credit card information. When we questioned officials about the six systems, they gave specific explanations why they hadn’t initially thought PCI DSS requirements applied to Authority systems. Furthermore, they stated that “the Authority had not been asked” to complete a Questionnaire covering these credit card systems.

A PCI self-assessment illuminates any potential vulnerabilities in related systems to better ensure that all vital CDE elements stay protected. Until the Authority comprehensively defines its CDE, it will be unable to accurately complete a PCI self-assessment.

Cardholder Data Security Program

An information security policy is an essential component of an organization’s information security program, and is also a requirement of PCI DSS. It 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. The information security 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.

The Authority maintains high-level Information Technology Security Manuals (Manuals) that reference handling sensitive data, which Authority officials stated would cover the systems that process and store credit card data. During our testing, management provided an application inventory listing of Authority systems, which denoted whether each system handled sensitive data and the nature of the data. However, none of the systems that handle credit card information were noted as handling sensitive data (contrary to the State's Information Classification Standard), which fails to reflect the highly sensitive nature of credit card information and the resulting security measures that should be followed. Furthermore, the Manuals do not refer to the CDE – nor do they address PCI-specific policies or procedures and requirements.

Further, management has not yet developed key policies and procedures that are required by PCI DSS, including:

- Data retention, disposal, and encryption;
- Protecting systems against malware;
- Restricting access to cardholder data;
- User identification and authentication;
- Physical access over cardholder systems;
- Monitoring access to network resources and cardholder data;
- Controlling storage and maintenance of all media; and
- Security monitoring and testing.

Without clearly defined responsibilities, there could be inconsistencies in how credit card data is handled. Since an information security policy creates the roadmap for implementing security measures to protect an organization's most valuable assets, without an overarching security policy that clearly addresses PCI DSS, the Authority is failing to comply with requirements to make their employees aware of the sensitive nature of credit card processing and the employees' responsibility to protect it.

PCI DSS also requires that a formal security awareness program be implemented and given for new hires and be held at least annually in order to make all employees aware of the importance of cardholder data security. However, the Authority does not have a security awareness program tailored to its specific business processes and the risks associated with credit card processing and storing. Rather, it relies on the general security training offered by the Governor's Office of Employee Relations, which does not cover the processing, handling, and storing of sensitive credit card information.

According to its Manuals, the Authority's Information Security Officer (ISO) is responsible for coordinating the development and implementation of information security policies and

procedures; monitoring security risks and identifying and assessing needed controls; providing information security expertise to program areas about data classification, operational standards, processes, and procedures; and implementing a process to proactively assess and remediate information security vulnerabilities. Officials did not specifically address why certain information security policies or procedures had not been developed or a formal data classification done. Officials indicated that the Authority had an ISO in the past who retired, and that two employees have been jointly performing the duties of the ISO for over a year. They further explained that, over the past few years, greater emphasis has been given to protecting the Authority's computing environment from cyber threats.

While we understand the significant risks posed by cyber threats, it is important that PCI DSS be implemented and followed as part of the Authority's "business-as-usual" activities and overall security strategy. Otherwise, the Authority will have difficulty meeting PCI DSS requirements.

Physical Access Controls

PCI DSS requires strict controls over the storage and accessibility of media processing credit cards. However, we found that strict controls are not maintained over the accessibility of the credit card terminals, nor are the terminals that are actively used physically secured as required by PCI DSS standards. For instance, all four credit card terminals currently in use are kept out, unprotected and unattended, overnight. Furthermore, while the two terminals in the main office are protected from public access via required use of badge readers upon entry to the building, this does not prevent unauthorized access by internal employees. Without physically securing these machines, they are subject to potentially improper access, and cardholder data are susceptible to potential unauthorized scanning, viewing, or copying by devices such as a credit card skimming device.

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 Authority 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.

Recommendations

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

- Inventorying all assets related to payment card processing activities;

- Conducting a PCI risk self-assessment;
 - Developing and disseminating policies and procedures that clearly define information security responsibilities for all personnel; and
 - Strengthening physical security over all systems that receive, process, transmit, and maintain cardholder data.
2. Implement the recommendations detailed during the audit, but not addressed in this report due to confidentiality reasons, for strengthening technical controls over cardholder data.

Audit Scope, Objective, and Methodology

The objective of our audit was to determine whether the Authority complies with PCI DSS. Our audit scope covers the period March 1, 2017 through June 5, 2017.

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. Finally, we reviewed documentation maintained by the Authority related to payment card processing during our scope period.

We conducted our 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 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 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. We considered their comments in preparing this final report and attached them in their entirety to it. Of the two recommendations in the report, officials agreed with one and disagreed with the other. Despite disagreeing with Recommendation 1, officials indicated they will be implementing certain additional measures to further enhance its PCI DSS compliance – measures, we are pleased to note, that are virtually identical to those included in our recommendation. Additionally, a comment by Authority officials in the response was misleading, and our rejoinder to this comment is included in the State Comptroller's Comment.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Chair of the Thruway 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

Brian Reilly, CFE, CGFM, Audit Director

Nadine Morrell, CIA, CISM, CGAP, Audit Manager

Mark Ren, CISA, Audit Supervisor

Holly Thornton, CISA, CFE, Examiner-in-Charge

Jared Hoffman, OSCP, GPEN, GWAPT, Information Technology Specialist

Christopher Bott, Senior Examiner

Nicole Tommasone, Senior Examiner

Mary McCoy, Senior Editor

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

Ken Shulman, Assistant Comptroller

518-473-0334, kshulman@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



ANDREW M. CUOMO
Governor

**Thruway
Authority**

JOANNE M. MAHONEY
Chair

BILL FINCH
Acting Executive Director

September 5, 2017

Mr. Brian Reilly
Audit Director
Office of the New York State Comptroller
Division of State Government Accountability
110 State Street
Albany, New York 12236

Dear Mr. Reilly:

On behalf of Chair Mahoney, this letter is in response to the NYS Office of the State Comptroller's (OSC) Draft Audit Report 2017-S-11, which assesses the New York State Thruway Authority's (Authority) Compliance with Payment Card Industry (PCI) Standards for the period March 1, 2017 through June 5, 2017.

The Authority is a public benefit corporation that is required to comply with all NYS Office of Information Technology Services (ITS) policies and standards. These ITS policies define security controls, requirements, protocols, and processes that protect systems, network, and data. In addition to these ITS policies, the Authority has developed, documented, and distributed procedures and guidelines that support these policies.

Over 99.9% of the Authority's credit card activity is processed directly by our contracted E-ZPass vendor and was in full compliance with PCI Data Security Standards (DSS). This audit focused on less than 0.1% of our credit card activity and did not find that any of the Authority's credit card data had been lost, stolen, or compromised in any way.

*
Comment 1

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

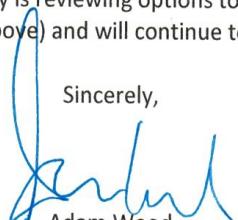
- Inventorying all assets related to payment card processing activities;
- Conducting a PCI risk self-assessment;
- Developing and disseminating policies and procedures that clearly define information security responsibilities for all personnel; and
- Strengthening physical security over all systems that receive, process, transmit, and maintain cardholder data.

Response: The Authority generally disagrees with this recommendation. The Authority's current standards comply with PCI DSS standards. The Authority is also implementing additional measures to further enhance its DSS compliance, including:

- Completing an inventorying of all assets related to its payment card processing activities;
- Initiating a PCI Self-Assessment Questionnaire (SAQ), which will include a risk assessment and identify whether any security vulnerabilities exist associated with its Cardholder Data Environment (CDE);
- Developing and disseminating additional policies and procedures that clearly define information security responsibilities for all personnel regarding PCI DSS; and
- Identifying additional methods to strengthen its physical security over all systems that receive, process, transmit, and maintain cardholder data if weaknesses are determined to exist.

Recommendation 2: Implement the recommendations detailed during the audit, but not addressed in this report due to confidentiality reasons, for strengthening technical controls over cardholder data.

Response: The Authority generally agrees with this recommendation. Based on the findings and detailed recommendations of the audit, the Authority is reviewing options to strengthen technical controls over cardholder data (including those outlined above) and will continue to make PCI DSS compliance a top priority.

Sincerely,

Adam Wood
Chief of Staff

State Comptroller's Comment

1. This statement is misleading. As stated in the report, from May 1, 2015 through April 30, 2016, Authority data indicated it directly processed approximately 66,000 credit card transactions totaling almost \$1.4 million. Further, at the onset of our audit, Authority management was not aware credit card data was processed or stored by systems on its internal network. The audit's stated objective was to determine whether the Authority complied with PCI standards, not to determine whether credit card data had been lost, stolen, or compromised. Finally, we strongly believe a breach of even one credit card number would be too many, and encourage Authority officials to make the improvements noted in this report and our confidential report.