THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

December 27, 2017

Dr. Kristina M. Johnson
Chancellor
State University of New York
353 Broadway
Albany, NY 12246

Re: Compliance With Payment Card
Industry Standards
Report 2017-F-24

Dear Dr. Johnson:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law, we have followed up on the actions taken by officials of the State University of New York to implement the recommendations contained in our audit report, *Compliance With Payment Card Industry Standards* (Report 2015-S-65).

Background, Scope, and Objective

The State University of New York (SUNY) is the largest comprehensive university system in the United States, consisting of 64 institutions and about 436,000 enrolled students. SUNY System Administration (System Administration) acts as the governance arm of the SUNY system, providing the various SUNY schools with centralized services and support, including evaluating the security of SUNY schools' systems as well as defining policies and procedures applicable to all SUNY schools. These policies include procedures that address the actions required of all institutions to protect the confidentiality of sensitive data and compliance with applicable industry standards. All entities that accept credit cards as a method of payment should comply with technical and operational Data Security Standards (DSS) established by the Payment Card Industry (PCI) Security Standards Council, which were designed to protect cardholder data.

Our initial audit report, which was issued on June 8, 2016, covering the period August 25, 2015 through March 22, 2016, determined whether selected SUNY schools were in compliance with PCI standards and whether SUNY had provided sufficient guidance to the schools regarding PCI compliance. SUNY schools were generally knowledgeable about PCI compliance and the need to protect credit card data from unauthorized access; however, we identified a range of weaknesses concerning the completeness of systems' component inventories; network segmentation; the

resolution of compliance deficiencies; and the oversight of affiliated campus organizations. The objective of our follow-up was to assess the extent of implementation, as of December 8, 2017, of the three recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

SUNY has made significant progress in implementing the recommendations identified in our initial audit report. Of the three prior audit recommendations, two have been implemented and one has been partially implemented.

Follow-Up Observations

To SUNY Schools visited:

Recommendation 1

Implement the recommendations contained in the detailed preliminary reports.

Status - Partially Implemented

Agency Action - The audit team issued a preliminary report at each of the six SUNY schools reviewed during our initial audit. The preliminaries contained a total of 18 recommendations covering six different SUNY schools. Our review found that of the 18 recommendations, 14 recommendations have been implemented, three have been partially implemented, and one is no longer applicable. Three of the six SUNY schools implemented all of their recommendations, where applicable.

To System Administration:

Recommendation 2

Develop strategies to enhance compliance with PCI DSS and improve monitoring of PCI compliance at all SUNY colleges.

Status - Implemented

Agency Action - Since our initial audit, System Administration has developed and enacted strategies to enhance compliance with PCI DSS. Particularly, System Administration's Office of the University Controller issued a guidance document in October 2017, titled "Payment Card Industry Data Security Standards Overview and Best Practices," for use by SUNY campuses. In addition, PCI training has been given to campuses during an Accounting, Bursar, and Budget meeting, and to community college campuses during Community College Business Officers Association conferences.

System Administration has made efforts toward improving monitoring of PCI compliance

and the SUNY schools through the creation and addition of PCI-specific questions to the annual self-assessment questionnaire, which is completed by the SUNY schools and returned for review and monitoring by System Administration.

Recommendation 3

Revise contract templates for affiliates to address PCI DSS regulations and require affiliates' compliance.

Status - Implemented

Agency Action - System Administration has revised the model contract templates that are used by SUNY schools and their affiliate entities. The revisions included amendments to contractual language to require compliance with PCI DSS. Specifically, System Administration added a paragraph that states:

> *"The Corporation agrees to maintain data security that conforms to generally recognized 'industry standards' and best practices that the Corporation applies to its own processes and systems. Generally recognized industry standards include but are not limited to the current standards and benchmarks set forth and maintained by PCI DSS."*

Major contributors to this report were Bob Mainello, Jared Hoffman, Holly Thornton, and Christopher Bott.

We would appreciate your response to this report within 30 days, indicating any actions planned to address the unresolved issues discussed in this report. We thank the management and staff of the State University of New York for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Nadine Morrell, CIA, CISM, CGAP
Audit Manager

cc: Michael Abbott, University Auditor