Thomas P. DiNapoli
State Comptroller

110 State Street
Albany, New York 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

May 27, 2021

Félix V. Matos Rodríguez, Ph.D.
Chancellor
City University of New York
205 East 42nd Street
New York, NY 10017

Re: Compliance With Payment Card
Industry Standards
Report 2021-F-2

Dear Dr. Matos Rodríguez:

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 City University of New York to implement the recommendations contained in our audit report *Compliance With Payment Card Industry Standards* (Report 2018-S-61).

Background, Scope, and Objective

The City University of New York (CUNY) – the nation's largest urban public university – comprises 25 colleges located throughout New York City's five boroughs. As of April 2021, CUNY offers 1,400 academic programs, 200 majors leading to associate and baccalaureate degrees, and 800 graduate degree programs to over a half million students in a single integrated system. CUNY's Central Office is responsible for issuing various CUNY-wide policies in areas such as academic affairs, legal and compliance issues, facility management, and IT security, including credit card payment processing.

All industries 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 designed to protect cardholder data. Entities that do not comply with PCI DSS may be subject to fines and penalties, as well as lose the ability to accept credit card payments. The requirements apply to all system components included in, or connected to, the Cardholder Data Environment, which is composed of the people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.

CUNY colleges as well as auxiliary services corporations (i.e., affiliates) that use school resources to process credit card transactions and third-party vendors hired to process payments must comply with the PCI DSS. According to Central Office, each CUNY school is responsible for all PCI compliance activity occurring on its campus. Under the PCI DSS, CUNY is also required to establish and disseminate a security policy that addresses all PCI DSS requirements so that all personnel are aware of their compliance responsibilities.

Our initial audit report, issued on December 13, 2019, examined whether CUNY complied with PCI DSS. The audit covered the period November 7, 2018 through May 2, 2019. We found that CUNY had fallen short in providing CUNY colleges with sufficient guidance and direction needed to ensure campus-wide compliance. We identified areas where system and data controls need to be improved to meet compliance standards at all four of the colleges we sampled. Furthermore, Central Office did not oversee colleges' PCI compliance, and instead relied on each college to self-monitor. As a result, Central Office had no knowledge of the compliance status of any of its colleges – and thus no assurance that the relevant data is properly protected campus-wide.

The objective of our follow-up was to assess the extent of implementation, as of April 20, 2021, of the three recommendations included in our initial audit report.

Summary Conclusions and Status of Audit Recommendations

CUNY officials have made progress in addressing the audit findings identified in the initial audit report. Of the initial report's three audit recommendations, two have been implemented and one has been partially implemented.

Follow-Up Observations

Recommendation 1

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

Status – Implemented

Agency Action – CUNY officials have developed strategies to enhance compliance with the PCI DSS. CUNY has appointed PCI liaisons who are responsible for maintaining PCI compliance at each of their respective colleges, in addition to a Director of PCI Compliance to oversee the liaisons. CUNY has also provided guidance to the colleges through annual and supplemental trainings, meetings, FAQs, and instructions on aspects of PCI compliance, such as maintaining device inventory lists and conducting vulnerability scans.

Recommendation 2

Update CUNY-developed Guidelines to reflect issues pointed out in the report.

Status – Implemented

Agency Action – CUNY updated its policy for protecting credit card information in March 2021 and issued it to all PCI liaisons across the CUNY colleges. The policy covers security responsibilities for all personnel who use cardholder data, including, but not limited to, CUNY employees, related entities, and third-party vendors. These updated Guidelines now require all the colleges and related entities to verify the PCI compliance status of third parties by requesting and reviewing an attestation of compliance annually. Additionally, the colleges have instituted local policies to help strengthen PCI compliance.

Recommendation 3

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

Status – Partially Implemented

Agency Action – During our initial audit, we issued two preliminary reports to CUNY. The second report contained confidential recommendations specific to the schools we reviewed. Of the report's seven total recommendations, five were implemented and two were partially implemented.

Major contributors to this report were Daniel Raczynski, Andrew Philpott, Joseph Bachinsky, and Jeffrey Herrmann.

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 CUNY for the courtesies and cooperation extended to our auditors during this review.

Very truly yours,

Heather Pratt, CFE
Audit Manager

cc: Richard White, CUNY Vice Chancellor of Risk, Audit, and Compliance
Vernitta N. Chambers, CUNY Interim Executive Director and Chief of Staff