# City University of New York

## Compliance With Payment Card Industry Standards

Report 2018-S-61 | December 2019

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Division of State Government Accountability

# Audit Highlights

## Objectives

To determine whether the City University of New York (CUNY) has provided sufficient guidance to the CUNY colleges regarding Payment Card Industry (PCI) compliance and whether selected CUNY colleges are in compliance with PCI standards. Our audit scope covered the period November 7, 2018 through May 2, 2019.

## About the Program

CUNY – the nation's largest urban public university – comprises 25 colleges located throughout New York City's five boroughs. As of January 2019, CUNY offered 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 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 PCI Security Standards 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, as well as lose the ability to accept credit card payments. CUNY colleges accept credit cards as a method of payment (e.g., donations, events) and, as such, must comply with the PCI DSS to protect against electronic security breaches and theft of payment card data.

## Key Findings

While Central Office recognizes the importance of PCI DSS compliance and is committed to maintaining strong internal controls, it has not provided its colleges with sufficient guidance and direction for addressing and maintaining compliance with PCI DSS requirements.

- The four CUNY colleges we visited were significantly unfamiliar with the PCI DSS requirements, compliance thereof, and the need to protect credit card data from unauthorized access.
- We identified areas where system and data controls need to be improved to meet compliance standards.

## Key Recommendations

**To Central Office:**

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

**To the CUNY Colleges Visited:**

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

**Office of the New York State Comptroller**
**Division of State Government Accountability**

December 13, 2019

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

Dear Dr. Matos Rodríguez:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage government resources efficiently and effectively and, by so doing, providing 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 City University of New York entitled *Compliance With Payment Card Industry Standards*. The audit was performed 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.

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,

*Division of State Government Accountability*

# Contents

# Glossary of Terms

| Term | Description | Identifier |
|---|---|---|
| ASV | Approved Scanning Vendor | *Key Term* |
| CDE | Cardholder data environment | *Key Term* |
| CUNY | City University of New York | *Auditee* |
| DSS | Data Security Standards | *Standards* |
| Guidelines | CUNY PCI DSS Guidelines | *Guidelines* |
| PCI | Payment Card Industry | *Key Term* |
| ROC | Report on Compliance | *Key Term* |
| SAQ | Self-Assessment Questionnaire | *Key Term* |

# Background

The City University of New York (CUNY) – the nation's largest urban public university – comprises 11 senior colleges, 7 community colleges, and 7 graduate, honors, and professional colleges (collectively referred to as colleges in this report) located throughout New York City's five boroughs. As of January 2019, 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.

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. Created in 2004 by the five global payment brands (American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.), the PCI DSS is a set of 12 high-level technical and operational requirements, and over 200 sub-requirements, designed to protect cardholder data. The requirements apply to all entities involved in payment card processing, including merchants, processors, and service providers, and cover information security domains such as policies and procedures, network monitoring and testing, physical security, vulnerability management, user access, and protection of cardholder data.

The PCI DSS applies to all system components (e.g., network devices, servers, computing devices, applications) that are included in, or connected to, an entity's cardholder data environment (CDE). (The CDE comprises people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.) All such system components must be accounted for through inventory and comply with their respective requirements.

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.

To assist entities in establishing compliance, the PCI DSS provides detailed assessment procedures encompassing six categories of system and data controls:

- Build and maintain a secure network.
- Protect cardholder data.
- Maintain a vulnerability management program.
- Implement strong access control measures.
- Regularly monitor and test networks.
- Maintain an information security policy.

All colleges, as well as affiliates and vendors, must perform these assessments and submit an annual report – either a Self-Assessment Questionnaire (SAQ) or a Report on Compliance (ROC), respectively – to each payment brand as attestation of their PCI DSS compliance. Failure to comply with the PCI DSS may result in fines and penalties as well as forfeiture of the ability to accept credit card payments.

# Audit Findings and Recommendations

While Central Office recognizes the importance of PCI DSS compliance, it has fallen short in providing CUNY colleges with sufficient guidance and direction needed to ensure campus-wide compliance. In fact, despite the existence of the PCI DSS since 2004, it was not until May 2019 that CUNY Administration issued guidance that specifically addresses PCI DSS.

All four of the colleges we sampled similarly acknowledged the importance of PCI DSS (these colleges are identified as College A, B, C, and D, respectively, throughout the report). While the colleges have moved most of their credit card processing to third-party vendors to reduce their PCI scope, officials at each were unaware of the detailed requirements. We identified areas where system and data controls need to be improved to meet compliance standards.

Furthermore, Central Office does not oversee colleges' PCI compliance to ensure they perform the periodic vulnerability assessments as required, instead relying on each college to self-monitor. As a result, Central Office has no knowledge of the compliance status of any of its colleges – and thus no assurance that the relevant data is properly protected system-wide.

## Guidance and Monitoring From CUNY Central Office

According to Central Office officials, all colleges are required to comply with PCI DSS. However, while they have issued some guidance to the colleges on the protection of confidential data, including credit card information, guidance specific to PCI DSS requirements – the cornerstone of compliance control – has been lacking. As discussed later in this report, this has resulted in colleges' inadvertent non-compliance in certain areas. The fact that Central Office does not monitor colleges' PCI compliance creates the risk that any vulnerabilities may continue to exist unabated.

### CUNY's PCI DSS Guidance

Central Office just released its CUNY PCI DSS Guidelines (Guidelines) in May 2019 – about 15 years after the PCI DSS were introduced. According to officials, the Guidelines were in the works before then. The Guidelines were developed based, in part, on results from two surveys in 2015 and 2016, involving 10 of the 25 colleges, undertaken to determine the scope of CUNY's PCI exposure and the magnitude of credit card transactions.

Prior to the Guidelines, the various IT and data security policies in place served as guidance for CUNY colleges. Although the policies may have been useful to some extent, we note that they did not specifically address PCI DSS

requirements and compliance, and therefore were inadequate to preempt risk. Central Office disagreed, stating that, while the policies did not explicitly reference PCI DSS, they were designed to address cybersecurity risk factors from a broader perspective, including those required for PCI DSS compliance, and therefore sufficed at the time.

These Guidelines note CUNY's commitment to safeguarding personal information transmitted or stored during the processing of credit card information. We reviewed the current Guidelines and found they cover a wide range of topics. In addition to a summary of the six categories of system and data controls and the 12 high-level requirements, they provide guidance related to adequate oversight, cardholder data storage, and outside vendor compliance, among other topics, and include resource links as well as a PCI DSS Program checklist.

However, while the list of contents is exhaustive, we found the actual guidance might not always accurately reflect the PCI DSS. For example, under Scope, the Guidance states:

*These guidelines do not apply to college foundations or separately-incorporated alumni associations, unless these entities are using a College network to process payment cards. (p. 1)*

We question the validity of this statement, as PCI DSS applies to all entities involved in CUNY payment card processing, which in this case includes college foundations. Consequently, CUNY's reputation is at risk for any breach of any payment card processor on their campus. CUNY officials responded, stating that its policy applies to college foundations to the extent they use CUNY's network, and that colleges have separate memorandums of understanding with the college foundations. CUNY officials further responded that, as a condition of a foundation's use of a college's name, facilities, and/or other resources, the foundation must accept and follow the CUNY Foundation Guidelines, which include data and confidentiality requirements as well as the obligation to maintain network security standards, including but not limited to PCI DSS. CUNY officials further state that CUNY's PCI DSS compliance efforts extend only to those entities and third-party vendors that process CUNY-related transactions on CUNY's behalf. We believe this would include all credit card-processed donations made on behalf of the college. In addition, while credit card donations to the foundations were processed online via third-party processors, CUNY staff is significantly involved in these transactions and in the retention of credit card data. As such, the Guidelines should include PCI DSS controls and compliance for these foundation transactions.

In another instance, the Guidelines state:

*The merchant environment and complexity of compliance depends on the merchant level … and corresponding merchant level requirements … by the major payment card companies. In most cases, a Self-Assessment Questionnaire … is required. (p. 2)*

According to the PCI DSS, all entities involved in credit card transaction processing must prepare a SAQ or a ROC as part of the PCI DSS assessment process. In response, CUNY officials argued that there are various circumstances where a SAQ is not required, such as when CUNY is not the merchant of record. However, our reviews at the four sampled colleges indicated that, even when CUNY was not the merchant of record, credit card documentation was retained, which then requires PCI DSS controls and compliance.

## CUNY Monitoring

Central Office does not monitor colleges' compliance with PCI, nor does it perform an overall PCI risk assessment to identify instances of non-compliance, and thus could not speak to the status of PCI compliance at each campus. In response, Central Office officials pointed to several recent proactive steps taken. While each is a positive step, we note that, even collectively, they are insufficient for monitoring purposes. For example:

- Central Office hired a University Manager of PCI Compliance in January 2019. We acknowledge the importance of this position to manage PCI compliance, but note that it occurred years after the PCI DSS was introduced. While this newly hired PCI manager did not have direct PCI experience, CUNY officials noted the individual had extensive experience with CUNY banking security as well as familiarity and extensive interaction with CUNY's business personnel. The University Manager of PCI Compliance has since earned PCI Professional certification.
- CUNY-wide affiliate contracts (e.g., vending machines, virtual bookstores) include language regarding PCI compliance. Again, while this is a notable action, we also found other important documents where this is omitted, including CUNY's web brochures related to internal control, its internal control certifications, and its assessment questionnaires. Finally, the colleges' spring 2018 attestations of compliance were related to general IT controls only; there was no specific mention of the detailed PCI DSS requirements.
- To assist colleges in their PCI compliance responsibilities, Central Office established the PCI DSS compliance task force, which provided

support, promoted awareness, and conducted training for the colleges over the past few years. We recognize these efforts, but our visits to the four sampled colleges indicate that CUNY's guidance and direction for addressing and maintaining compliance with the PCI DSS requirements were insufficient.

- As discussed later, officials at the sampled colleges were generally not sufficiently familiar with the PCI DSS requirements, and the colleges were deficient in their PCI compliance.
- Officials at all four colleges advised us they had no CUNY written policies and procedures related to PCI DSS compliance. Nor had the colleges developed their own PCI DSS-related procedures, with College D asserting that it was waiting for Central Office to develop policies and procedures.

CUNY officials reiterated that the responsibility for implementing the Guidelines rests with the individual colleges.

- CUNY officials also noted that CUNY encourages its colleges to use third-party credit card processors, thereby reducing their PCI scope. As such, according to CUNY officials, most credit card transactions "never touch" CUNY's network as they are processed by a third party. We disagree, in that it cannot be inferred that a reduced PCI scope will eliminate transactions within CUNY's network, only that the scope of in-network transactions is reduced. Our review at the sampled colleges bears this out: we confirmed that much credit card processing is, in fact, done via third-party processors, but found colleges were still processing credit cards for items such as athletic venue rentals, conference room rentals, and continuing education fees.

In responding to our preliminary findings overall, Central Office officials attributed any deficiencies to the challenge of addressing the entire range of PCI DSS requirements and sub-requirements, many of which are complex. We counter that this reasoning does not justify the 15 years it took CUNY to develop its Guidelines after PCI DSS was first initiated. Furthermore, credit card security is crucial and, by its very nature, complex, requiring equally complex controls and requirements – not only to protect cardholder data but also the integrity of CUNY's reputation.

## Colleges' Payment Card Industry Compliance

To achieve PCI DSS compliance, an organization must meet all PCI DSS requirements. During our review of credit card processes, including selected operational and technical data security controls, at the four sampled CUNY

colleges, we identified multiple areas with compliance deficiencies. Significant improvements are required to meet PCI DSS.

## Compliance Assessment and Attestation

Entities that accept credit card payments are required to conduct PCI assessments and complete an assessment report – either the SAQ or the ROC as appropriate – attesting to full PCI DSS compliance. These assessments help identify those areas where elements of a PCI requirement have not been met fully, either by the entity itself or a vendor. None of the four colleges completed the annual SAQ and, in fact, some colleges' officials were not even aware of this requirement. Specifically:

- Colleges B, C, and D had no assessments for their vendors and thus were not aware of the vendors' PCI compliance status. Colleges C and D obtained vendor SAQs only following our audit request.
- College A had a PCI compliance certification from a third-party processor; however, it was from 2017.

In their response, CUNY officials explained that the examples we cited involved CUNY-wide vendors, and as such, Central Office is responsible for monitoring their PCI DSS compliance. Colleges, on the other hand, are only responsible for the compliance of vendors or related entities that use their college network. CUNY officials also stated that CUNY's ongoing PCI compliance training is expected to continue to increase awareness among colleges.

Despite CUNY officials' clarification of duties, we contend that colleges still have the responsibility for confirming vendors' PCI compliance, which can only be done with the actual compliance assessment in hand. Furthermore, while vendors or related entities may not use the college network, PCI controls and compliance are necessary for cardholder data storage.

For its part, College C responded that, since the issuance of the Guidelines in May 2019, it has established a PCI Committee. Its members include personnel from IT, the Business Office, and a representative from every unit and related entity that oversees the acceptance of payment cards, as well as those that maintain the network and/or systems involved in payment card information transmission, processing, and storage. The college further stated it will complete SAQs for the college and related entities for each merchant account and request ROCs for all vendors and third-party processors.

## Risk Assessment

Entities must perform a risk assessment at least annually and upon significant changes to the environment (e.g., acquisition, merger, relocation) to identify critical assets, threats, and vulnerabilities, and produce a formal, documented analysis of risk. Performed on this schedule, these risk assessments allow the entity to keep up to date with organizational changes and evolving threats, trends, and technologies.

Colleges C and D did not have a formal annual risk assessment or review process. College B provided a 2018 in-house report, the recommendations of which have not been fully implemented. College A provided a PCI gap assessment dated 2016, the findings of which were never addressed, and conditions continue to exist approximately three years later.

Central Office stated it completes many internal control and risk documents annually to ensure full internal control compliance, asserting that CUNY's Information Security Program is based on various security policies and procedures. However, as we noted previously, CUNY's web brochures related to internal control, its internal control certifications and assessment questionnaires, and its information security policies and procedures do not include PCI DSS compliance.

In their response, CUNY officials advised us that Central Office will request College A to provide a corrective action plan to rectify the gap assessment findings. They also noted that College B had provided an internal PCI assessment report.

## PCI Inventory

As stated in the PCI DSS, entities must maintain an inventory of system components that are in scope for PCI. This will enable organizations to accurately and efficiently define the scope of their environment for implementing PCI DSS controls and preclude the risk that some system components could be inadvertently excluded from their configuration standards. Systems without the proper PCI-specific security controls significantly increase the risk of unauthorized access to the cardholder data. Entities are required to maintain an up-to-date list of devices, including the device make, model, location, and serial number or other method of unique identification.

None of the four colleges maintained a complete or accurate inventory of their PCI components. The inventories provided by officials at Colleges A, C, and D did not include all the specific devices nor devices' make, model, location, and serial number, as required. College B did not maintain a PCI inventory listing.

## Network Segmentation

Network segmentation refers to isolating systems that process credit card data from the remainder of the entity's network. Although network segmentation is not a PCI DSS requirement, it is strongly recommended as a method that may reduce the scope and cost of the PCI DSS assessment, the cost and difficulty of implementing and maintaining PCI DSS controls, and the risk to an organization (by consolidating cardholder data into fewer, more controlled locations). Without adequate network segmentation, the entire network is in scope of the PCI DSS assessment.

While most of the credit card processing at the four sampled colleges was done online, some transactions were processed via credit card terminals. We found that three of the four visited colleges have not followed best practices regarding isolating system components from other portions of their networks.

In responding, Central Office officials stated that our preliminary findings did not seem to consider whether transactions associated with the terminals are encrypted, thereby limiting compliance scope to the terminals themselves. However, CUNY's own response to our preliminary findings cited a blog, which further noted that encryption alone may not be sufficient to render the cardholder data out of scope for PCI DSS. CUNY officials nevertheless agreed with our finding, indicating that segmentation may be appropriate if the terminals do not limit scope through encryption and to focus compliance efforts, avoiding any ambiguity as to where the scope border may exist.

## Improper Storage and Disposal

Entities are required to keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures, and processes. Entities are not permitted to store the card verification code or value (the three- or four-digit number printed on the payment card) after authorization. Unprotected credit card information must never be sent via end-user messaging technologies (e.g., e-mail, instant messaging). Hard-copy material must be cross-cut shredded, incinerated, or pulped when no longer needed for business or legal reasons so that there is reasonable assurance that hard-copy materials cannot be reconstructed.

We identified poor storage controls of credit card data at the four sampled colleges, increasing the risk of unauthorized access.

At College A, hard-copy student registration forms that included credit card information were insecurely maintained, including:

- Forms left in an open mailroom cubby;

- Processed current-semester registration forms retained in a folder on an office desk;
- Past-semester forms dating as far back as 2010 scanned into a desktop computer; and
- Donor documents containing credit card information stored for two fiscal years atop a file cabinet.

College A officials advised us that the previously scanned/saved registration forms will be deleted, and students will now use laptops for direct access to the college and third-party processor websites. In addition, other documents had been subsequently redacted and shredded.

We found similar issues at College B:

- Processed documents – some dating as far back as 2010 – containing complete credit card information were retained in an open storage room. According to officials, records that were beyond their seven-year retention policy have since been shredded. While the retention policy is an important part of data security, more important – and detrimental – is the fact that complete credit card information is retained on the transaction documents.
- Documents containing complete credit card information were retained by two offices within the college. Officials explained that the information was retained as transaction backup for the accounting firm that audits student housing. Subsequent to our visit, officials informed us that documentation for these credit card payments would be retained by one office only. We still, however, question the need to retain credit card information at all.
- Credit card information had been stored in email files for up to eight months, and some credit card information had been kept by staff members on their desks for a period of time. While the office was locked when staff was not present, security and cleaning staff had access to the office after hours. Additional credit card information had been transferred to an unsecured file cabinet in a locked storage room, to which security and cleaning staff also had after-hours access.

At College C, we found six-year-old donation forms with poorly redacted credit card information (i.e., still readable through the black marker redaction) that had been stored in binders in an unlocked cabinet. At College D, mailed-in forms had been shredded in a strip-cut shredder rather than the required cross-cut shredder.

Central Office officials responded that CUNY's record retention and disposition schedule is derived from New York State's Record Retention and Disposition Schedule. The schedule is meant to ensure that records are retained as long as required for administrative, legal, and fiscal purposes and to encourage the systematic disposal of records that are no longer needed. However, as mentioned, while records may be within the required retention period, the cardholder data generally has no business use after authorization; records can be retained but certain credit card information should be deleted as soon as possible after authorization in accordance with the New York State Record Retention and Disposition Schedule.

CUNY officials also responded that they presented the new Guidelines at various business council meetings, during which they also reminded attendees that cardholder data should not be stored unless there is a business need to do so. The attendees were also re-instructed about the importance of proper disposal of physical cardholder data, specifically using a cross-cut shredder.

## Terminal Inspection for Tampering

Entities are required to periodically inspect credit card devices to look for tampering or substitution and train personnel to be aware of attempted tampering or replacement of devices. We found there was insufficient training and devices were not checked for tampering at all four visited colleges. CUNY officials responded that the PCI DSS Awareness Trainings, offered during the past three years, addressed device skimming and checking devices for tampering, and reported that all staff from the four sampled colleges were in attendance. CUNY will continue to support all campuses in meeting PCI compliance requirements.

## Vulnerability Scans

Internal and external network vulnerability scans are designed to expose potential vulnerabilities that could otherwise be exploited by malicious individuals, and must be conducted at least quarterly and after any significant change in the network. Quarterly external vulnerability scans are to be performed via an Approved Scanning Vendor (ASV) approved by the PCI DSS.

External vulnerability scans were not performed in a scheduled manner by an ASV, as required, at all four sampled colleges, apparently stemming from confusion regarding the respective roles of the colleges and CUNY. According to CUNY officials, the colleges are responsible for internal vulnerability scans, and had been provided with a PCI DSS-approved scanning tool for this

purpose; external vulnerability scans of colleges, on the other hand, are done by CUNY. Also, CUNY has begun a pilot program with an external entity to perform ongoing external vulnerability scans. In its response, CUNY noted that, "while these scans are not specifically tied to PCI DSS compliance, coverage addresses the Internet-facing attack surface of the pilot colleges."

In their response, College B officials stated they use an external service provider for credit card processing, and they are not hosting any PCI data on any of the college's servers. However, we did find a credit card terminal connected to the college's network. They further acknowledged the importance of security and stated they are in the process of hiring an IT Security Officer. This position's responsibility includes ensuring that the college meets all relevant requirements as well as leading the hardening, monitoring, auditing, and reporting efforts for the college's IT infrastructure.

In their response, Central Office officials reiterated that CUNY campuses are responsible for all PCI compliance activity occurring on their campuses, asserting that CUNY's IT Security Procedures require campuses to perform periodic vulnerability assessments, to which they attest twice a year. Going forward, CUNY will substantiate that campuses conduct the required PCI vulnerability scans.

### Technical Controls

During our testing, we identified technical controls that did not appropriately or fully address PCI requirements. Due to their confidential nature, we reported these matters to CUNY officials in our preliminary reports and, consequently, do not address them in detail in this report. If these matters are not adequately addressed, the colleges 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 CUNY is responsible for the security incident. Furthermore, a compromise or breach could negatively impact public opinion or perception of CUNY as a whole. Subsequent follow-up audits will address the detailed findings and recommendations related to technical controls.

## Other Matter

During the course of our site visits, we noted that, across our sample of CUNY colleges, departments used different third-party processors for similar services. While CUNY prefers that each college select vendors for credit card processing, the use of CUNY-wide contracts – as is done for vending machines and virtual bookstore operations – might be more cost-effective, while at the same time streamlining the number of vendors within CUNY's

CDE and lessening individual colleges' burden of vendor compliance monitoring.

## Recommendations

**To Central Office:**

1. Develop strategies to enhance compliance with PCI DSS and improve monitoring of PCI compliance at all CUNY colleges.
2. Update CUNY-developed Guidelines to reflect issues pointed out in the report.

**To the CUNY Colleges Visited:**

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

# Audit Scope, Objectives, and Methodology

The objectives of this audit were to determine whether CUNY has provided sufficient guidance to the CUNY colleges regarding PCI compliance and whether selected CUNY colleges are in compliance with PCI DSS. Our audit scope covered the period November 7, 2018 through May 2, 2019.

To accomplish our objectives and assess the adequacy of internal controls related to PCI compliance, we interviewed CUNY System Administration officials as well as officials at the four sampled colleges to gain an understanding of the guidance given to the CUNY colleges and the PCI controls in place at each school visited. During our survey, at our request, officials of CUNY's Office of Internal Audit and Management Services contacted all 25 CUNY colleges, requesting credit card data such as transaction dollar amount, campus merchant identification information, and inventory/campus location where credit cards are accepted. Based on the information received, we judgmentally selected four CUNY colleges to visit, based on credit card transaction amount where available and student enrollment data (which could coincide with the number of transactions). Our intent was to visit different types of colleges (i.e., community, senior, and graduate colleges) as well as colleges with high enrollment and those with low enrollment. These colleges are identified as College A, B, C, and D throughout the report. Our sample was not designed to be projected to the population as a whole. We conducted extensive walk-throughs of each of the four colleges, interviewing pertinent school officials, including IT and financial department staff, obtaining and reviewing relevant documents, and observing their credit card processes. We visited the colleges from December 2018 through May 2019.

# Statutory Requirements

## Authority

The audit was performed 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 conducted our performance audit in accordance with generally accepted government auditing standards. These 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.

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 management functions do not affect our ability to conduct independent audits of program performance.

## Reporting Requirements

We provided a draft copy of this report to CUNY officials for their review and formal comment. We considered their comments in preparing this final report and have included them in their entirety at the end of it. While CUNY officials commented on report issues they felt needed further clarity, they generally agreed with the report's recommendations. For one recommendation, officials disagreed with comments about the Guidelines but stated updates will be made if and when required. Our responses to CUNY comments are included in the report's State Comptroller's Comments.

Within 180 days after the final release of this report, as required by Section 170 of the Executive Law, the Chancellor of the City University of New York 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.

# Agency Comments

**Senior Vice Chancellor and Chief Financial Officer**

230 W. 41st Street, 5th Floor
New York, NY 10036
tel: 646-664-3014

**December 6, 2019**

Brian Reilly
Audit Director
Office of the State Comptroller
Division of State Government Accountability
110 State Street - 11th Floor
Albany, NY 12236-0001

Re: Compliance with Payment Card Industries Standards – Draft Report 2018-S-61

Dear Mr. Reilly,

This letter is in response to the NYS Office of the State Comptroller's (OSC) draft report referenced above, which assesses whether the City University of New York (CUNY) has provided sufficient guidance to the CUNY colleges regarding Payment Card Industry (PCI) compliance and whether the selected CUNY colleges are in compliance with PCI standards. CUNY is committed to safeguarding personal and account information transmitted or stored when processing payment card transactions, and ensuring that appropriate controls and processes are in place. PCI compliance revolves around security, and CUNY has strong IT security and compensating controls in place to protect sensitive data.

CUNY has always used the OSC's reports to improve controls and processes, as well as to minimize risks, and we appreciate this review and the recommendations. We disagree, however, with the finding that CUNY has not provided its colleges with sufficient guidance and direction for addressing and maintaining compliance with Payment Card Industry Data Security Standards (PCI-DSS) requirements. As the report indicates, we have done a number of things to provide guidance and enhance CUNY's overall PCI compliance program, such as PCI presentations and awareness training, since 2015, and most recently, we disseminated the CUNY PCI-DSS Guidelines across the University and hired a Director for PCI Compliance, who holds a Payment Card Industry Professional certification.

In addition, we would like to correct two items as follows:

1. The report indicated that the CUNY Guidelines are not accurate with respect to when Self-Assessment Questionnaires (SAQs) by CUNY are required. An SAQ is always required to be completed by the merchant of record. There are cases whereby the merchant of record is a third-party vendor. In these cases, the third-party is required to complete the SAQ and not CUNY. Furthermore, the CUNY Guidelines include guidance on handling PCI compliance for third-party vendors.

Comment 1

2. The report also stated that external vulnerability scans are performed by CUNY. This is incorrect, as PCI-DSS compliant external vulnerability scans must be performed by an Approved Scanning Vendor and not CUNY.

Comment 2

**Response to the Recommendations in the Draft Report**

The following three recommendations were issued by OSC. CUNY has provided responses to each of the recommendations below.

**To Central Office:**

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

   Compliance with PCI requirements is important to CUNY. The following are some of the steps that CUNY has taken towards achieving University-wide PCI compliance since 2014:

   - CUNY Central Office surveyed a sample of 10 colleges on their Card Data Environment (CDE).
   - CUNY Central Office has presented at various CUNY council meetings to raise awareness and enhance compliance with PCI. The college participants included Vice Presidents for Finance and Administration, Vice Presidents of Advancement, Business Managers, Chief Information Officers, Risk Management, Enrollment Management, Bursars, etc.
   - CUNY Central Office also hired an external Qualified Security Assessor (QSA) firm that provided annual PCI Awareness training (Merchant, Executive and IT level) for all pertinent staff University-wide.
   - PCI-compliant language has been included in all new centralized RFPs and contracts, and CUNY Central Office reviewed Attestations of Compliance and/or SAQs for these contracts.
   - CUNY Central Office developed and distributed the 'CUNY PCI-DSS Guidelines' and administered follow-up training specific to the Guidelines. This document has also been made publicly available via the University's website.
   - PCI liaisons at the colleges have been designated, and a CUNY PCI listserv has been created to facilitate communication and guidance University-wide.
   - CUNY has appointed a University Director of PCI Compliance-- a certified Payment Card Industry Professional whose dedicated role is to enhance compliance and maintain administrative oversight.
   - CUNY Central Office established a PCI Committee, which meets quarterly to develop strategies to enhance compliance efforts across the University.
   - CUNY Central Office distributed a PCI-DSS Compliance Checklist to monitor PCI compliance at all CUNY colleges.

   CUNY will continue to enhance its PCI compliance program, and listed below are future plans.

   - In order to ensure that the appropriate SAQs are being completed, CUNY Central Office will be holding SAQ training for all pertinent staff University-wide.

- CUNY Central Office will deploy a portal page to manage and provide oversight of SAQs University-wide.
- CUNY Central Office is looking into an Approved Scanning Vendor for vulnerability scanning.
- CUNY is also working toward uniformed payment processing solution(s), which will reduce our PCI scope and the overall risks associated with payment card processing.
- An eLearning solution for PCI Awareness Training, which aims to ensure all new and existing hires are aware of PCI requirements to safeguarding sensitive data, is expected to be implemented by the end of fiscal year 2020. This will provide targeted training for staff.

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

   The University disagrees with the auditors' comments related to the issues with respect to the CUNY PCI-DSS Guidelines. The current guidelines are an accurate representation of the latest version of the PCI-DSS (version 3.2.1) and any updates to the Guidelines will be made if and when required.

**To the CUNY Colleges Visited:**

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

   Due to the sensitive nature of this topic, we are not providing a detailed response to the information cited in this report but would be available to meet to discuss actions taken by the selected colleges that were in the scope of the audit. The colleges visited by OSC during the course of the audit have reviewed the recommendations for strengthening technical controls over cardholder data and have either addressed them, or are working to address them, as applicable.

Thank you again for the opportunity to respond to this audit report. We agree that there are improvements that CUNY can make in regards to PCI compliance and are prepared to do so. Please contact me if you need any additional information.

Respectfully,

Matthew Sapienza
Senior Vice Chancellor and Chief Financial Officer
The City University of New York

# State Comptroller's Comments

1. As noted on page 10, CUNY Guidelines state, "The merchant environment and complexity of compliance depends on the merchant level … and corresponding merchant level requirements … by the major payment card companies. In most cases, a Self-Assessment Questionnaire … is required." We agree that there are cases where the merchant of record is a third-party provider; however, as also noted on page 10, our reviews at the four sampled colleges indicated that, even when CUNY was not the merchant of record, credit card documentation was retained, which then requires PCI DSS controls and compliance.

2. We are confused by this correction. We agree that quarterly external vulnerability scans should be performed by an ASV. However, during the course of our audit, as noted on page 17, CUNY officials stated that external vulnerability scans of colleges are done by CUNY. Nevertheless, we are pleased to see that CUNY is working with an external entity to conduct these scans.

# Contributors to Report

## Executive Team

**Tina Kim** - *Deputy Comptroller*

**Ken Shulman** - *Assistant Comptroller*

## Audit Team

**Brian Reilly**, CFE, CGFM - *Audit Director*

**Nadine Morrell**, CIA, CISM - *Audit Manager*

**Daniel Raczynski** - *Audit Supervisor*

**Holly Thornton** - *Audit Supervisor*

**Marsha Paretzky** - *Examiner-in-Charge*

**Renee Boel** - *IT Specialist*

**Christopher Bott** - *Senior Examiner*

**Wayne Scully** - *Senior Examiner*

**Mary McCoy** - *Supervising Editor*

**Contact Information**
(518) 474-3271
StateGovernmentAccountability@osc.ny.gov
Office of the New York State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller
For more audits or information, please visit: www.osc.state.ny.us/audits/index.htm