CENTRAL TICKET OFFICE

CASHIERING

AUDIT REPORT #22-2203

Audit & Advisory Services

October 2022

CENTRAL TICKET OFFICE

CASHIERING

AUDIT REPORT #22-2203

Background

In accordance with the UCLA Administration fiscal year 2021-22 audit plan, Audit & Advisory Services (A&AS) performed an audit of internal controls and procedures related to UCLA’s Central Ticket Office (CTO) cashiering activities.

CTO is responsible for servicing, processing, selling, and distributing tickets for on-campus events sponsored by a variety of clients including student groups, the Department of Intercollegiate Athletics (DIA), the Center for Art of Performance, campus academic units, and other registered organizations. CTO also acts as a distributor for tickets for off-campus events and services that include, but are not limited to, movie tickets, theme park admissions, and Go Metro and other public transit passes. CTO distributes in excess of 1.4 million tickets to over 600 events, handles 68,000 walk-up customers to the Central Ticket Office, processes 41,000 internet transactions, and answers over 46,000 calls annually.

Tickets can be purchased online through CTO’s website, the Ticketmaster website, by phone, mail, or in-person at the CTO windows. CTO accepts cash, check, and credit and debit cards. Maitre’D is the cashiering system used to process transactions and record ticket sales. The Paciolan ticketing software is used to manage ticket inventory and sales for athletic and performing arts events. UCLA’s web-based payment and deposit processing system CashNet is used for deposits.

For fiscal year 21-22, CTO’s total revenue was approximately $3 million. CTO, which employs 11 career personnel and 35 student employees, is headed by a Director who reports to the Administrative Vice Chancellor.

Purpose and Scope

The primary purpose of the audit was to evaluate CTO’s processes and internal controls associated with the cashiering activities to ensure business practices comply with applicable University accounting principles and standards. Where applicable, the audit also sought to evaluate compliance with campus and University policies and procedures.

The audit focused on the following areas:

* Cash & Cash Equivalent Collections
* Deposits
* Reconciliations
* Physical Security
* Information Systems

The audit was conducted in conformance with the *International Standards for Professional Practice of Internal Auditing* and included interviews, tests of records, and other procedures considered necessary to achieve the audit purpose.

Summary Opinion

Based on the result of the work performed within the scope of the audit, CTO’s processes and internal controls associated with the cashiering activities help ensure that its business practices comply with applicable University accounting principles and standards; however, management could further strengthen controls by (1) ensuring that when a CTO employee separates from the University, all of that employee’s access to CTO systems is removed and (2) maintaining Payment Card Industry (PCI) certificates for each staff member that completes his or her Security Awareness Education (SAE).

Audit Results and Recommendations

Cash and Cash Equivalent Collections

A&AS reviewed cash collection controls and business practices to determine whether assets are protected and properly reported in compliance with (i) UCLA policies and procedures, including UC Business and Finance Bulletin (BUS-49), “Policy for Cash and Cash Equivalents Received,” and (ii) CTO internal operating procedures. Cash collections were reviewed to determine if cash and cash equivalents were received and recorded appropriately. In addition, A&AS tested individual accountability during the collection of cash and cash equivalent processes.

1. Cash and Cash Equivalent Collections

Cash and cash equivalent transactions were tested by reviewing various CTO cashiering documents on a sample of five dates during the February 2022 - April 2022 time period. For each transaction selected, A&AS obtained supporting documentation to verify that the person collecting cash, issuing cash receipts, and preparing deposits was someone other than the person performing the monthly review of the general ledger. In addition, A&AS verified that individual accountability and separation of duties were maintained and documented.

There were no significant control weaknesses noted in this area.

1. Voids and Refunds

A&AS sought to review void and refund transactions during a sample of five dates during the February 2022 – April 2022 time period. Department procedures require CTO supervisors to login to the Maitre’D system to approve the void. Voided receipts are maintained for support. There were no void transactions on the five sample dates, and, therefore, we were unable to verify if void transactions were processed in accordance with CTO policies.

Refunds are approved by a CTO supervisor via the Maitre’D system. A refund form is required to support the refund transaction, which should include all approval signatures and the reason for the refund. Five deposit dates within the February 2022 – April 2022 time period were selected for review. Two refunds were obtained and reviewed (1) for supervisor approval demonstrated by signature, (2) for accuracy, (3) to ensure that supporting documentation was maintained for the transaction, and (4) for timeliness. All of the refunds reviewed had supervisor approval, were accurate, had appropriate documentation, and were processed in a timely manner.

There were no significant control weaknesses noted in this area.

1. Change Funds

To operate CTO windows for daily operations, cashiers are provided a $150 change fund. Before a cashier begins using a register station, the cashier must first verify and sign for a daily change fund issuance using the CTO Change Fund Verification form. Once verified, the cashier logs on to the station to record sales into the Maitre’D and Paciolan systems. Each cashier is provided his or her own login to the Maitre’D and Paciolan systems to ensure proper registration and accountability throughout the shift. At the end of the shift, cashiers record their total amount of cash and cash equivalents on hand onto a Seller’s Sheet that breaks down totals. A count is performed by the cashier and an independent staff member for verification. Both the cashier and the independent staff member sign the Seller’s Sheet for accuracy. The Change Fund Verification forms and Seller’s Sheets for five sample dates within the time period of February 2022 – April 2022 were reviewed for completeness and accuracy.

There were no significant control weaknesses noted in this area.

1. Mailed-in Payments

CTO rarely receives mailed-in payments (i.e., checks, etc.); however, departmental procedures are in place to maintain accountability in the process. According to department procedures, mailed-in payments are verified and processed by two employees. Operations staff store mailed-in checks in a locked cabinet for security. Each check is entered into the Maitre’D and Paciolan systems. Each check is combined with all other deposited cash or cash equivalents. The total is then entered into CASHNet.

No significant control weaknesses were identified in this area; however, given that there were no mailed-in payments during the period of review (February 2022 – April 2022), A&AS was not able to verify that mailed-in payments are processed in accordance with departmental procedures.

Deposits

A sample of five deposits were obtained and reviewed to ensure that cash receipts documented for cash, check, debit and credit card transactions matched their respective CASHNet totals. Test work showed that all deposits matched the bank statement, and that cash overages/shortages maintained the proper support and explanation for each transaction.

There were no significant control weaknesses noted in this area.

Reconciliation

Reconciliation practices, procedures, and supporting documentation were reviewed for accuracy and timeliness. Five sample dates were selected from the time period of February 2022 – April 2022 to verify that each deposit was reconciled to the bank statement and general ledger appropriately. CTO bulk imports deposits into CASHNet via the payment batch import process. This process limits the number of manual entries needed, and removes potential manual errors that may be entered into the general ledger. The department matches deposits from CASHNet on a nightly basis.

Based on our review of the sample five deposit dates, A&AS verified that each of the deposits reconciled to the general ledger and bank statements, and the reconciliation reviews were properly documented.

There were no significant control weaknesses noted in this area.

Physical Security

Procedures for safeguarding cash were examined to verify that controls are adequate and comply with BUS-49. Controls surrounding the physical security of monies were assessed to ensure proper safeguarding of cash and cash equivalents. This review included controls around the safe and keys. Finally, A&AS reviewed employee training and background checks.

1. Physical Security

Cash and cash equivalents appear to be properly safeguarded. CTO utilizes 20 surveillance cameras to help monitor the safety and security of personnel and to record the handling and processing of cash and cash equivalents.

There were no significant control weaknesses noted in this area.

1. Safe Combination and Keys

Management maintains a listing of employees who have access to the safe and office keys. A&AS verified that the listing of employees as of the date of review were current employees and that the safe was properly restricted to authorized personnel. A combination change log is maintained that provides the date and reason for the change in safe combination, which is (i) whenever a person who knows the combination leaves his or her position or (ii) at least once a year in accordance with UCLA Policy. Lastly, we verified that the office keys are marked “Do not duplicate.”

There were no significant control weaknesses noted in this area.

1. Background Checks and Training

Background checks are performed for all CTO employees that handle cash or cash equivalents. Training is provided to new employees and at least annually for all cash handling employees. The training includes departmental and University cash handling policies, procedures, and techniques.

Sample testing of 10 recently hired CTO employees showed that background checks were performed on all 10 employees.

There were no significant control weaknesses noted in this area.

Information Systems

A&AS held discussion with CTO management to obtain an understanding of the authorization, administration and review of user access to systems used by CTO: Maitre’D, Paciolan and CASHNet. CTO’s compliance with the PCI Data Security Standards (DSS) was also reviewed.

1. System Access

System access is authorized and provided by the Assistant Director or the Director based on job responsibilities. All users require an individual login and password for each system. As of June 2022, there were 40 CTO employees that have system access. A&AS reviewed the listing of user access for Maitre’D, Paciolan, and CASHNet to verify all users were current CTO employees and their access was appropriate based on job classification and responsibilities.

CTO has established procedures for the authorization and administration of user access to the systems used by their employees and the Associate Director reviews that access on an annual basis. All 40 users who had access to Paciolan and all 23 users who had access to Maitre’D as of June 2022 were then-current employees and access was appropriate based on job duties. CashNet access was held by the Director, Assistant Director and the previous Financial Manager who separated on October 16, 2021. Once notified by A&AS, the Director processed a request to have the separated Financial Manager’s access removed.

Recommendation: Management should ensure that when a CTO employee separates from the University that all their access to CTO systems is removed.

Response: Management agrees and has revised the Separation Checklist we follow when employees separate to include removing ticketing system access, removing financial system access and removing DACSS access.

1. PCI Compliance:

PCI Compliance requires that card data is encrypted from the start to the end of a card transaction. CTO remains in compliance with this requirement by utilizing Paciolan for all credit card transactions. Paciolan utilizes Point-to-Point Encryption (P2Pe) that guarantees PCI Compliance. P2Pe encrypts credit card data immediately upon swipe or entry into the payment terminal.

In accordance with the PCI DSS, the University of California requires all employees involved with payment cards (credit and debit cards) in any capacity to complete SAE training upon hire and at least annually. A sample of 10 CTO staff members were chosen to verify that each individual completed and passed his or her SAE training.

For seven of the ten staff members selected for review, A&AS was able to verify that they completed training by reviewing their training certificates. Management was unable to pull the training certificates from the Learning Management System (LMS) for three of the staff members, two of which recently separated from the University. As a consequence, we were unable to verify that those two employees completed their training. For the employee who is still employed by CTO, CTO confirmed the employee had been trained.

Recommendation: PCI certificates for each staff member that completed his or her security awareness training should be maintained.

Response: Management agrees and will maintain a file of PCI certificates showing completion of the required training for all employees.

220714-2

REP