Arizona State University
Office of University Audits
Purchasing Card Program Audit
February 22, 2019

This page intentionally left blank

Arizona State University
Purchasing Card Program
Audit Report
February 22, 2019

Summary: The Purchasing Card Program audit was included in the Arizona State University (ASU) FY2019 audit plan approved by the Arizona Board of Regents (ABOR) Audit Committee and ASU senior leadership. The audit focused on the overall design and effectiveness of the Purchasing Card Program for the period October 2017 through September 2018. This audit is in support of ASU's mission of effective management of financial resources and focus on efficient operations of all levels of the university.

Background: A Purchasing Card (PCard) is a type of commercial card that allows organizations to utilize existing credit card infrastructure to make business-to-business (B2B) electronic payments for business expenditures. PCard programs generally allow organizations to streamline procure to pay processes, improve procurement time, and reduce transaction costs while taking advantage of supplier discounts and program rebates. ASU implemented the existing PCard program in 2015 through JPMorgan. The program is a corporate liability card that gives colleges and business units the ability to spend funds directly from their established budget. Annual spend for FY2018 was $64.8M of which ASU earned $1.3M in rebate revenue.

The PCard program is centrally managed through the Procurement department, which is responsible for the relationship with JPMorgan, card issuance including applications, card set up and distribution, and managing card controls related to transaction limits and card balances. They also manage JPMorgan system access and provide ongoing cardholder support for the program. Formal training and guidelines have been implemented to drive appropriate use of the PCards.

Once the card has been issued, fiscal responsibility for the card is owned by the college or business unit including ensuring procurement rules are followed, ensuring compliance with the PCard program, maintaining adequate supporting documentation for all transactions, and implementing appropriate review and approval controls. With the implementation of Workday, supporting documentation and approval is now captured at the transactional level within the Workday application.

PCards are generally issued to an individual; however, the university is responsible for financial settlement with JPMorgan. The Financial Services team is responsible for ensuring all transactions are recorded into the Workday financial system for financial settlement with JPMorgan. Payments are typically made on a weekly basis for the prior week's activity.

Arizona State University
Purchasing Card Program
Audit Report
February 22, 2019

Audit Objectives: The objectives of the engagement were to assess the design and operating effectiveness of the ASU Purchasing Card program including training. Specifically, the following areas were included:

- Assess the design and effectiveness of the PCard program including training
- Ensure appropriate controls are in place for card management including card issuance, lost/stolen, cancellation and employee termination
- Assess procedures for transaction disputes and unauthorized purchases
- Ensure appropriate controls are in place for exception processing
- Assess controls in place for recording transactions to the financial system
- Assess management oversight of the program and relevant third parties
- Identify opportunities for improvement

Scope: The scope of the audit focused on the operating processes of the ASU Purchasing Card Program for the period October 2017 through September 2018. The audit focused on the overall PCard program and did not include coverage related to transactional compliance or monthly reconciliations. These areas are already assessed as part of the recurring PCard reviews performed quarterly by the financial controls team.

Methodology: Our audit consisted of tests and procedures necessary to provide a reasonable basis for expressing our opinion. Specifically, audit work consisted of interviews with the PCard and Financial Services teams, observation of work processes, review of documented policies and procedures, and substantive tests including the following areas:

- Assessing the design of the PCard program including required training to ensure the program is designed appropriately.
- Confirming the defined card issuance process was followed by performing the following validation for a sample of 24 new PCards issued during the review period and 25 PCards reissued as part of the Workday implementation:
  o A completed Cardholder Agreement/Account Application form exists and was approved by an appropriate fiscal manager
  o PCard training was completed with a 100% quiz score (as required by the PCard policy) prior to card issuance (new cards only)
  o Fingerprinting was cleared prior to card issuance
  o Cardholder provided documented confirmation of card receipt
- Ensuring PCards are closed in a timely manner for terminated employees by validating all active cards are associated with an active ASU employee or appropriate affiliate. In

addition, for a selection of 30 cards associated with terminated employees, reviewing activity for the month before and the month following termination to ensure transactions were valid and had supporting documentation.

- Confirming appropriate business purpose and approval exists for default exceptions related to card activity and limits for the following:
    - 24 cards with transaction amount limits higher than the defined default limit of $10,000
    - 25 transactions where the transaction amount exceeded the single transaction default limit of $10,000
    - 15 cards with a card limit higher than the defined monthly default limit of $20,000
- Verifying administrative/privileged access to JPMorgan (PaymentNet) is appropriately restricted by performing an access review based on title/job function.
- Confirming access to JPMorgan (PaymentNet) was removed timely for individuals terminated during FY2018.
- Validating payments made to JPMorgan are supported by complete and accurate transaction reconciliations for a sample of 5 weeks (Pre-Workday). In addition, Workday processes were also assessed including validating payments made July-December 2018 and two subsequent payments in January 2019 once the revised reconciliation process had stabilized.
- Confirming accuracy of the annual rebate received for FY2017 and FY2018 by re-performing the calculation defined in the contract.
- Validating that the restricted Merchant Category Codes (MCC) per the contract were appropriately restricted from MCC groups utilized in card set up.

Conclusion: Overall, the PCard program has been designed and implemented to provide an efficient and cost-effective method of purchasing and paying for small-dollar transactions. The program is supported by detailed online training and documented procedures to provide cardholders and financial leaders guidance on the appropriate use of the PCard. The PCard team follows a defined process for card issuance, which ensures cards are authorized prior to issuance and are appropriately controlled until the cardholder confirms receipt of the physical card. While the program is generally operating effectively, improvement is required related to managing card default settings and managing access to the JPMorgan PaymentNet system utilized with the program. In addition, the PCard team should explore other options for storing cardholder applications and subsequent support. The existing manual process to store supporting documentation using a folder on the network is not effective given the overall size of the program and volume of cards.

Default limits related to single transaction amounts and monthly card limits have been implemented along with processes to allow exceptions as needed; however, these processes require additional improvement. Specifically, the current process does not require a documented business purpose when the cardholder application includes limits that exceed defined default limits provided the unit's fiscal manager approves the application. In one instance, it was noted that a card was issued with a limit of $300,000 with no documented business purpose. In addition, other exceptions were noted related to transaction specific exception requests including missing approvals, temporary increased limits not being removed and missing supporting documentation related to granted exceptions. There were also multiple instances noted where default limits did not convert accurately as part of the Workday card reissue.

Processes governing access to the JPMorgan PaymentNet system are not operating effectively. Testing indicated that 57% (44 of 77) of the users assessed that were terminated in FY2018 did not have access removed or access was not removed timely. Access will generally allow the ability to review and modify account coding for transactions as well as view cardholder data including Personal Identifiable Information (PII). Depending on access, this may be for their own card or multiple cards involving other employees.

Finally, it was noted that the cardholder application, which may include the full credit card number and employee PII data including social security number, was not stored in compliance with the ASU Data Handling Standard. Prior to the audit being finalized, the PCard team worked with the Information Technology team to correct this issue and program documents are now stored in a secure environment.

The control standards we considered during this audit and the status of the related control environment are provided in the following table.

General Control Standard (The bulleted items are internal control objectives that apply to the general control standards, and will differ for each audit.)	Control Environment	Finding No.	Page No.
Reliability and Integrity of Financial and Operational Information			
• PCard transactional activity is recorded in the financial system and reconciled to payments made to JPMorgan.	Reasonable to Strong Controls in Place	N/A	N/A
• The annual rebate is paid in accordance with the contract with JPMorgan.	Reasonable to Strong Controls in Place	N/A	N/A

Effectiveness and Efficiency of Operations			
• The PCard program was implemented to provide an efficient and cost effective method of purchasing and paying for small-dollar transactions.	Reasonable to Strong Controls in Place	N/A	N/A
• PCards are issued with an approved application after the cardholder has successfully completed training.	Reasonable to Strong Controls in Place	N/A	N/A
• Exceptions to the default limits are granted with appropriate approval and valid business need.	Opportunity for Improvement	1	6
Safeguarding of Assets			
• PCards are issued to authorized individuals.	Reasonable to Strong Controls in Place	N/A	N/A
• PCard application support is stored securely and in compliance with the ASU Data-Handling Standard.	Opportunity for Improvement	N/A	N/A
• Fingerprinting is completed prior to issuing a card to a new cardholder.	Reasonable to Strong Controls in Place	N/A	N/A
• JPMorgan system access is restricted to appropriate individuals.	Opportunity for Improvement	2	8
Compliance with Laws and Regulations	Not Applicable	N/A	N/A

We appreciate the assistance of The PCard Team and Financial Services representatives during the audit.

Lisa Grace, Executive Director, University Audit and Advisory Services
Gordon Murphy, Internal Audit Senior, University Audit and Advisory Services

Audit Results, Recommendations, and Responses

1. Processes for exceptions to defined card default values (monthly card limit and single transaction amount) require further improvement to ensure exceptions are made for valid business purposes and have appropriate approval.

Condition: The existing cardholder application includes defined default values for monthly card limits and single transaction amounts. As part of the application, cardholders can request limits to be set at higher rates; however, a defined business purpose is not required to ensure the request is justified. In addition, documentation to support exception requests and related approvals is not consistently maintained.

Criteria: Exceptions to defined default limits are made for valid business purposes and include appropriate fiscal and procurement approval.

Cause: While defined processes have been implemented that require exceptions to default limits to include a valid business purpose, fiscal approval, procurement approval and at times accounting approval, the processes were not implemented for new card applications. As a result, new card applications that request exceptions to the defined default limits are being processed without proper justification and approval.

In addition, manual processes are utilized to store account and cardholder support on a network share using a specific naming convention. This manual process is prone to errors especially as cards are replaced or names changed.

Effect: Multiple exceptions were noted where exception transaction and card settings do not have a defined business justification or did not have the required approval. Specifically, testing resulted in the following:

- 13 of 24 (54%) cards with a single transaction amount limit value greater than the default did not have documented business purposes or were missing required approval(s).
    - 5 selections were incorrect limits updated by JPMC during the Workday conversion.
    - 4 selections did not have supporting documentation related to the exception.
    - 2 selections were missing one or more required approval based on the transaction amount.
    - 2 selections were intended to be temporary increases; however, were not updated appropriately to revert to the default limit.

- 4 of 25 (16%) of transactions tested that exceeded the single transaction amount did not have appropriate support or approval.
    - 3 selections did not have supporting documentation related to the exception.
    - 1 of the selections was missing one of the required approvals.
- 11 of 15 (73%) cards with monthly limits greater than the default limit of $20,000 did not have a documented business purpose to support the increased card limit.
    - In 8 instances, the increased limit was requested as part of the original application with no documented business purpose.
    - 3 of the selections were intended to be temporary increases; however, were not updated appropriately to revert to the default limit.

Recommendation: The existing card application form should be modified to require a defined business justification and the same approvals that one-time exception requests would require after initial setup (which may include a buyer, procurement manager and individuals from accounting). In addition, further review processes should be implemented to ensure temporary increases are appropriately handled.

It is also recommended that the Procurement department perform further validation on accounts that have limits greater than default limits to determine if there are additional accounts that did not convert appropriately.

In addition, the PCard team should explore other options for storing cardholder applications and subsequent support. The existing manual process to store supporting documentation using a folder on the network is not effective given the overall size of the program and volume of cards.

Management Response: All existing cardholders that have a single transaction amount limit higher than $9,999 or a monthly card limit higher than $20,000 will be required to provide an updated business justification for the increased limit. Existing processes will be followed for subsequent requests related to transaction amount and card limits exceptions. As part of these actions, the existing approval requirements will be reviewed with Financial Services to ensure appropriate.

We will also work with Business and Finance IT to establish a more efficient and accurate repository for required documentation.

2. JPMorgan PaymentNet system access is not appropriately restricted.

Condition: The PCard team is responsible for managing access to PaymentNet; however, they were not receiving the full listing of terminations on a daily basis resulting in access not being removed timely or at all. Access will generally allow the ability to review and modify account coding for transactions and to view cardholder data, which includes PII. Depending on the employees' access, this may be for their own card or multiple cards involving other employees.

Criteria: Access to PaymentNet should be removed on or before the effective date of the termination.

Cause: The PCard team was not receiving a complete listing of employee terminations. As such, access was only being removed for a small subset of terminated employees. In addition, periodic access reviews have not been implemented to ensure access is appropriately restricted.

Effect: Access was not removed in a timely manner or at all for the vast majority of terminations. Specific testing was done related to access associated with employees that were terminated during FY2018. Of the 77 individuals tested, 40% (31 of 77), still had access at the time of our review with an additional 17% (13 of 77) not having access removed in a timely manner.

Recommendation: The PCard team should utilize the existing reports that are generated daily through the Identify and Access Management team related to terminations and transfers. This request has already been made and they are currently receiving the daily reports.

In addition, a full comprehensive access review should be performed to ensure all access is appropriate.

Opportunities to standardize account information should also be explored. The system currently does not utilize Single Sign On nor does it use the standard 10 digit ASU id as part of the data elements. This combined with the limited reporting available from JPMorgan results in manual review processes.

Management Response: The PCard team was relying on transfer notifications related to Advantage access. Immediately upon discovery that this was the case, we changed our source

notification system to PeopleSoft. We are currently receiving these emails daily and updating both the cardholder and PaymentNet access upon receipt.

In addition, we pulled a list of all employees currently in an "Inactive" state and are going back through all cardholders and PaymentNet access users to confirm that the PCards have been closed, and the access to PaymentNet has been removed. The anticipated completion date for this activity is March 31, 2019.

It is important to note that PaymentNet access poses no financial risk as the visible data is read only and the system provides no ability to transact business.

Distribution:

Arizona Board of Regents Audit Committee
Michael M. Crow, President
Morgan R. Olsen, Executive Vice President, Treasurer and Chief Financial Officer
Nichol Luoma, Associate Vice President, University Business Services
Marilyn Mulhollan, Assistant Vice President, Financial Services
Jamon Hill, Executive Director Supply Chain/Deputy Proc. Officer
Michael Baumert, Associate Director Financial Services
Patricia Taylor, Manager Supply Chain Systems
Internal Audit Review Board