Delaware River Port Authority
Office of the Inspector General

August 17, 2022

Audit of Employee Expense Reimbursement New ACH Payment Process

Performed by:
Angeleen Coppolino, CPA, Manager, Internal Audit

AUDIT OF EMPLOYEE EXPENSE REIMBURSEMENT

NEW ACH PAYMENT PROCESS

Contents

A. Objective / Scope / Methodology 1
B. Background 2
C. Audit Summary 4
D. Review of ACH Payment Process for DRPA Employee Expense Reimbursements 5
E. Privacy and Security of Sensitive Information……...……...…….……...…6

August 17, 2022

DELAWARE RIVER PORT AUTHORITY

OFFICE OF THE INSPECTOR GENERAL

AUDIT OF EMPLOYEE EXPENSE REIMBURSEMENT

NEW ACH PAYMENT PROCESS

A. Objective / Scope / Methodology

The Office of the Inspector General (OIG) conducted an audit of the new ACH (Automated Clearing House) payment process for reimbursing eligible employee expenses. Beginning on February 1, 2022, DRPA employees who utilize direct deposit for payroll are reimbursed for eligible approved expenses via ACH to the employee's "MAIN" bank account on record with payroll. Employees who receive a physical check from payroll will continue to receive a physical check for any reimbursable expenses. The audit was conducted by Angeleen Coppolino, Manager, Internal Audit. The audit objectives included:

- evaluating compliance with established policies, procedures, and guidelines;
- evaluating the effectiveness of controls over the access to and use of sensitive personal information, such as bank account details; and,
- evaluating the effectiveness of controls over processing and recording of employee expense reimbursements paid via ACH.

The scope of our audit covered DRPA employee expense reimbursements paid during the period from February 1, 2022, through March 31, 2022. Based on OIG's initial planning, total reimbursements were approximately $12,000 during this period.

To assist in the evaluation of the new ACH payment process for employee expense reimbursements, OIG was provided access to requested information and documentation, including:

- the established policies, procedures, and guidelines related to employee expense reimbursements;
- "read only" access to transactional detail for employee expense reimbursements (within SAP); and,
- a walkthrough of the process to initiate and pay eligible approved expenses including procedures within SAP and the banking online portal.

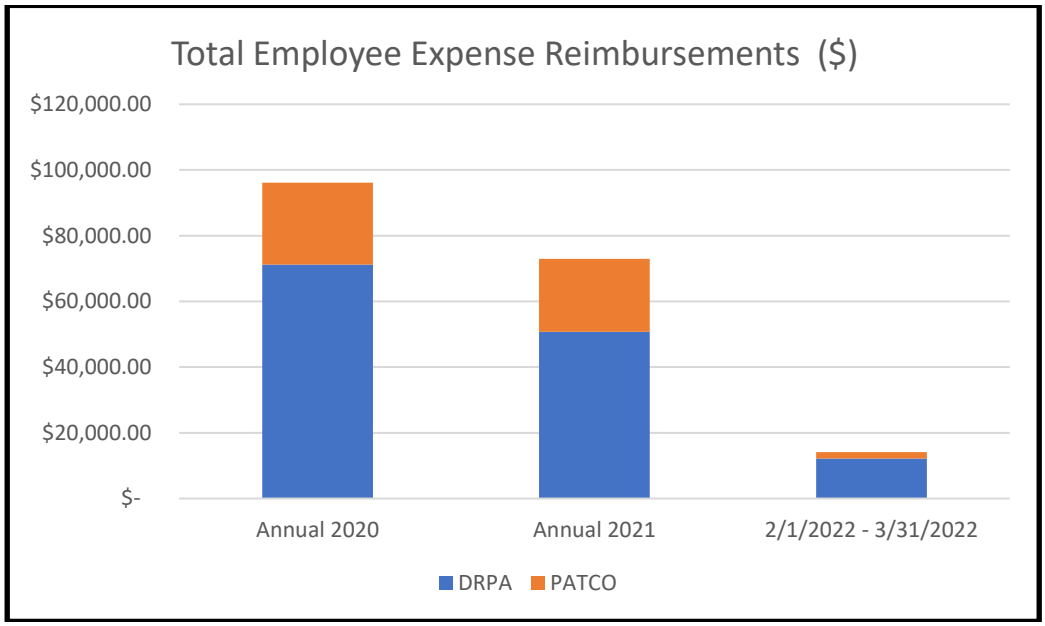
In addition to being provided the documentation noted, OIG communicated with the Director – Human Resource Services, Director of Finance (DRPA), Manager of Accounting (DRPA), Supervisor of Accounts Payable & Receivable, Senior Accountant, Accountants, Accounting Clerks, and various other Authority staff members during the course of the audit.

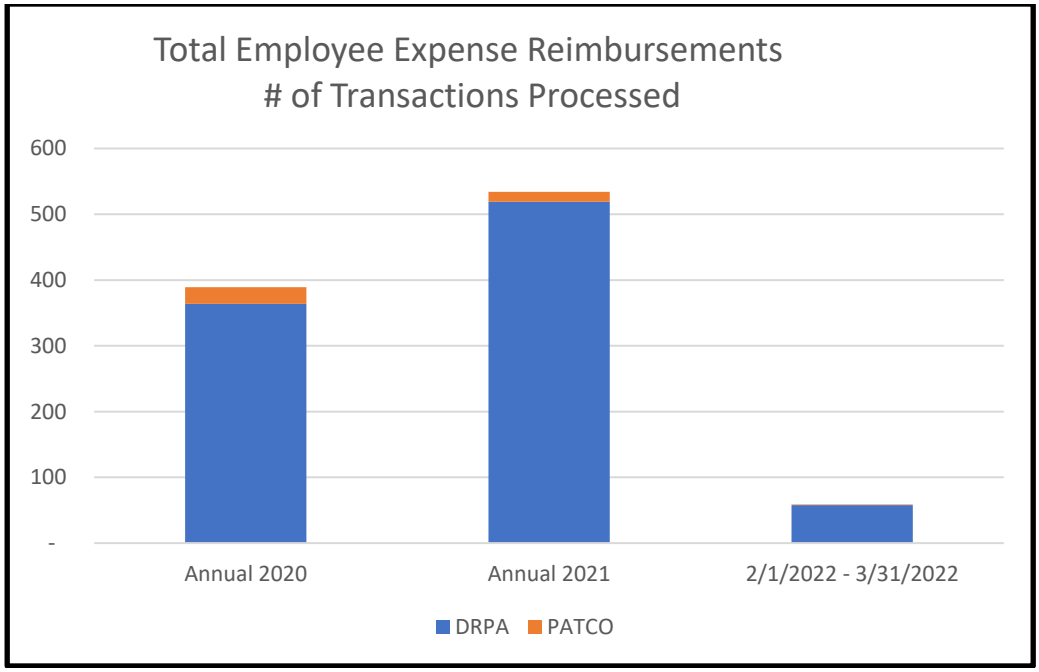
B. Background

The purpose of the employee expense reimbursement process is to allow employees to recover the cost of allowable business-related expenses that were paid by the employee. According to the Authority's Expense Accounts policy (Series No. 400), the Authority will pay for reasonable business expenses incurred in the course of transacting official business where proper documentation and/or approvals are submitted. When an employee incurs a business-related expense, he or she completes a standard employee expense report form (electronic I-Form). The completed form and required supporting documentation are forwarded to the proper approvers and payment is made to the employee.

Effective February 1, 2022, Finance implemented a direct deposit payment process for DRPA employee expense reimbursements. This process is now used for all DRPA employees that utilize the direct deposit method for salary payments. The expense reimbursement is sent via ACH to the "MAIN BANK" listed in the employee's personal profile in ESS – SAP (time entry). The expense reimbursement will show as a separate deposit in the employee's bank account, distinct from salary payments. Expense reimbursement checks will continue to be mailed for those employees not currently enrolled in direct deposit. The implementation of ACH for employee reimbursements will help improve the efficiency of processing the expenses for the Finance department, will reduce the number of uncashed checks and associated time and resources for handling escheated checks, and will eliminate the need for employees to cash or deposit checks.

PATCO employees will continue to be reimbursed via check and there are no plans to implement the ACH process in the foreseeable future. The volume of expense reimbursements for PATCO is much lower both in total dollars and number of transactions than for DRPA and consists primarily of tuition reimbursements.


Total Employee Expense Reimbursements ($)
$120,000.00
$100,000.00
$80,000.00
$60,000.00
$40,000.00
$20,000.00
$-
Annual 2020
Annual 2021
2/1/2022 - 3/31/2022
DRPA
PATCO


Total Employee Expense Reimbursements
# of Transactions Processed
600
500
400
300
200
100
-
Annual 2020
Annual 2021
2/1/2022 - 3/31/2022
DRPA
PATCO

C. Audit Summary

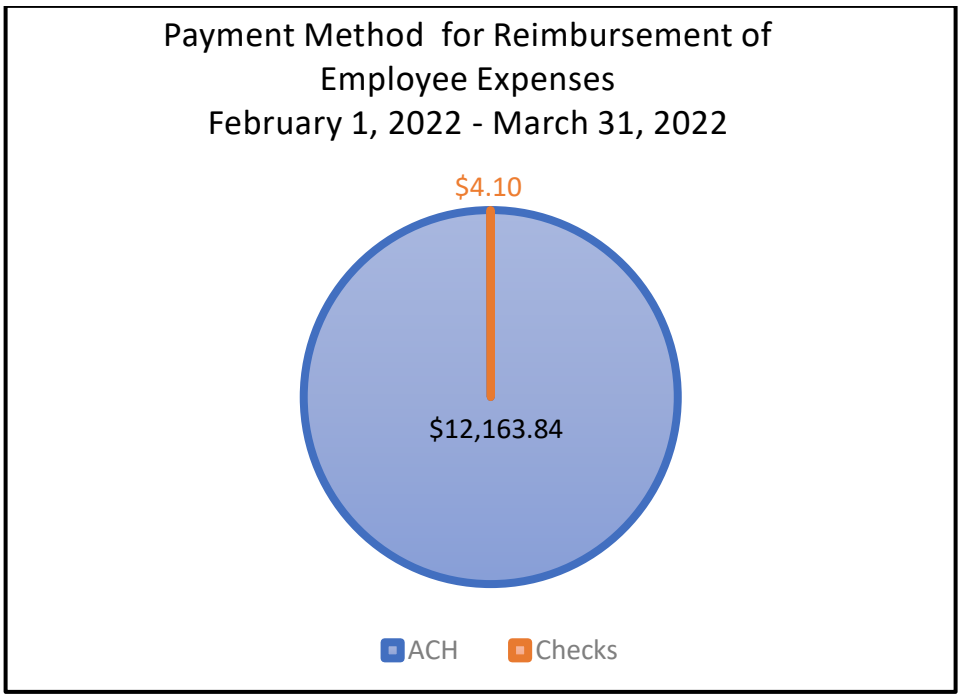
Based on conversations with Authority management and testing performed, OIG determined that the new process for reimbursing employee expenses via ACH is operating effectively and continues to be in compliance with established policies; however, additional opportunities were identified to improve the privacy and security of sensitive information. In summary, based on the completion of our audit, the following was determined and communicated to the CFO, Director of Finance (DRPA), Director of Human Resource Services (HRS), Manager of Accounting (DRPA), and the Accounts Payable and Receivable Supervisor:

- Established policies and procedures for employee expense reimbursements, including completion and approval of the Expense Report form and submission of supporting documentation, continue to be followed regardless of the method of payment to the employee.
- The ACH process has only been implemented for DRPA employees. Based on the significantly lower volume of employee expense reimbursements at PATCO, Finance has decided to not implement the ACH process for PATCO employees at this time.
- The majority of DRPA employees have a bank account designated for payroll direct deposit and can receive expense reimbursements via ACH. Only four DRPA employees still required check payment as of March 31, 2022.
- Procedures have been implemented to protect sensitive employee information from unnecessary disclosure. These include a process within SAP to redact bank account and routing numbers from reports and restricting access to process employee expense transactions to appropriate individuals.
- Additional opportunities were identified to improve the privacy and security of sensitive information. The Finance team reviewed a listing of user accounts with access to view and edit vendor bank information and requested Information Services (IS) to remove access for those employees that no longer require access as part of their ongoing responsibilities. In addition, Finance is in communication with IS to consider options for limiting access to edit and view banking information for vendors within SAP.
- Finance management is working with IS and other departments that utilize the vendor data in SAP to implement additional procedures related to data privacy and security. These include periodic reviews of user access rights and automatic expiration dates for contractor access.

These summarized findings are presented in more detail within the report.

D. Review of ACH Payment Process for DRPA Employee Expense Reimbursements

Through inquiry with Finance personnel, all but four DRPA employees have a "MAIN BANK" account identified within SAP – ESS which enables them to receive expense reimbursements via ACH. A list is maintained by Finance of those employees that require check payment. The Accounting Clerks identify which type of payment is appropriate while processing the expenses in SAP. A "T" indicates an ACH payment and is entered for all employees except the four on the list which require a "C" or check payment. If an expense is incorrectly entered as an ACH and no bank account information is available in SAP, an error message will be generated, and the transaction will not be able to move forward without correction. There was only one transaction for $4.10 for the period February 1, 2022, through March 31, 2022, that was reimbursed by check.



OIG observed the Finance team processing employee expense transactions in real time using the new ACH process. During the observation, OIG verified that existing policies and procedures related to the completion and approval of expense reports and submission of supporting documentation were being followed. In addition, responsibilities to approve, process transactions, and authorize payment are appropriately separated among various employees. Expense report forms are approved by the employee's Director, Chief, and the Budget Department. Responsibilities for processing the expense payments within SAP are performed by the Accounting Clerks and are reviewed by the Accounts Payable and Receivable Supervisor or the Senior Accountant. Approval is required by the Director of Finance, DRPA or CFO (or designee) prior to final payment. Access to the Wells Fargo bank portal to upload and approve the ACH payment is performed by the Accountants.

OIG reviewed a sample of expense reimbursement requests for five DRPA employees during the period from February 1, 2022, through March 31, 2022, that were reimbursed via ACH. Appropriate expense report forms, approvals, and receipts were scanned into SAP for each transaction selected. OIG also reviewed the data available, noting that there was no evidence of bank account or routing numbers within the screens supporting the entries in SAP.

E. Privacy and Security of Sensitive Information

OIG considered the privacy and security of sensitive information such as employee bank account and routing numbers during payment processing. It was observed that a specific layout and "variant" are selected within the SAP proposal process which redacts the bank account and routing numbers from being displayed on generated reports exported from SAP. OIG reviewed the reports both before and after the selection of the variant to confirm that appropriate data was redacted. These reports are circulated via email to the Finance team for review and approval prior to final payment processing in SAP. Once approval is received, the Accounting Clerks return to SAP to generate the final "text" file for upload to Wells Fargo. This file is then emailed to the Accountants, saved to a personal network file, and uploaded to the Wells Fargo online portal. This file is required to have the bank account and routing numbers visible in order for the bank to have the necessary information for payment. However, the information is not readily apparent based on the format of the file.

OIG also considered the privacy and security of sensitive information, such as employee bank account numbers, that can be viewed and edited as part of the vendor master file. OIG obtained a listing of individuals with access to view and edit vendor information in SAP from the Manager, ERP and Applications, Information Services (IS). SAP transaction codes (T-Codes) XK02 Change Vendor – Centrally and FK02 Change Vendor – Accounting allows users to both view and edit vendor information. There were approximately 124 user accounts in SAP that could access T-Code XK02 and 86 user accounts with access to FK02. This included 32 system accounts for T-Code XK02 and 17 system accounts for T-Code FK02 which are used in SAP for background processing and communication within SAP. OIG met with the Accounts Payable and Receivable Supervisor and observed that the bank account information was able to be viewed and edited for all vendors (including employees) through T-Code XK02. The ability to edit banking information in the vendor master file without appropriate internal controls can allow a user to commit fraud by rerouting the location to which payments are sent. In addition, the master source of information for employee payments is the "MAIN BANK" account identified within SAP – ESS. An automatic program runs every five hours to identify changes to the employee information in SAP-ESS and update the vendor files. The program only updates the vendor files for employee information that has changed within SAP - ESS. Therefore, changes made to the bank account information within SAP could result in a mismatch of the payment data between Human Resources/Payroll and Finance.

OIG recommends that the user list be reviewed by the Director of Finance and the Accounts Payable and Receivable Supervisor and access removed for those accounts/employees that do not need to edit this information as part of their current job responsibilities. There are other transaction codes, XK03 (Display Vendor – centrally) and FK03 (Display Vendor) that

can be used for those employees that only need to view vendor information. These codes do not allow access to view the banking details. Due to the sensitive nature of the information in the vendor master file, in addition to the possibility for fraud through the ability to make inappropriate changes to vendor information including the potential to reroute payments, access to T-Codes XK02 and FK02 should be limited to only those individuals that require this access for ongoing responsibilities.

Following the initial review, a biannual review of access rights should be performed to identify and remove any users that no longer require access. In determining whether access is necessary, consideration should be given to terminations, position changes, current projects, and the last date the system/transaction code was accessed. Finance should continue to review all requests for new access to vendor information before the access is granted by Information Services (IS).

Audit Finding #1: A review of users with access to view and edit sensitive vendor information within the SAP vendor master file, including bank account details for employees, identified 124 user accounts in SAP that could access T-Code XK02 Change Vendor - Centrally and 86 user accounts with access to FK02 Change Vendor - Accounting. The ability to edit banking information in the vendor master file without appropriate internal controls can allow a user to commit fraud by rerouting the location to which payments are sent. Changing details for employee vendors in the vendor master file can also result in a mismatch of bank account information between Human Resources/Payroll and Finance and cause any ACH payments for expense reimbursements to be sent to an incorrect bank account.

Audit Recommendation #1: OIG recommends that the DRPA user list be reviewed by the Director of Finance and the Accounts Payable and Receivable Supervisor and access removed for those accounts/employees that do not need to view/edit this information as part of their current job responsibilities. This review will require coordination with IS, Human Resources, and other department management for non-Finance employees and contractors that have access to the vendor master data. The principle of least privilege should be followed in all access decisions.

Following the initial review, a biannual review (at a minimum) of access rights should be performed by Finance management (DRPA and PATCO), in conjunction with IS, to identify and remove any users that no longer require access. In determining whether access is necessary consideration should be given to terminations, position changes, current projects, and the last date the system/transaction code was accessed. Access granted to contractors should have an automatic termination date consistent with the applicable project or contract, but no longer than one year. Finance should continue to review all requests for new access to vendor information before the access is granted by IS.

In addition, OIG recommends that Finance coordinate with IS to obtain documentation defining the various roles and T-codes within SAP and the related access rights. Roles should be specific to job functions and contain only the necessary T-codes. Finance

would benefit from guidance on typical roles and T-codes used for performing standard functions within the Finance department.

Management Response #1: Finance management concurs that there were issues with the number of individuals IS or the original integrator gave access to those two T-codes (FK02 and XK02). Finance was unaware of the access that was provided to employees outside of Finance. The T-code role Z_TRUSTED_RFC was removed with IS HelpDesk ticket (#40678). No other access roles were reviewed as part of this process. Another HelpDesk ticket (#36262) was opened to assess options for blocking the ability to edit bank information within the vendor files in SAP for employee vendors. As of this audit, based on IS input, the IS Department is not aware of a way to restrict access to the banking information in the vendor master data. Further research by IS and the SAP consultants is necessary to accomplish this goal. We are waiting for a response from IS to our HelpDesk ticket #36262.

DRPA Finance took the lead in coordinating the review of the current access to T-codes XK02 and FK02 and has removed all users except for the DRPA vendor masters, PATCO vendor masters and specific IS personnel. This initial review of all individuals with access to those two T-codes was completed by August 1, 2022. Only the Directors of Finance and/or the CFO can approve access to these two T-codes. IS has advised that all access for individuals working outside of the Authority will have a validity date.

The process and departmental responsibilities going forward regarding access maintenance for these two codes is ongoing with Finance (DRPA & PATCO) and IS. As part of this process review, Finance will request documentation to define the various roles that impact Finance and T-codes within SAP and the related access rights, as well as guidance on which T-codes are common for certain standard Finance functions/roles. This documentation will need to come from the external SAP consultants. Finance recommends a similar and more comprehensive review be performed with all core modules in SAP, i.e., "a best practices approach to role management". This would involve facilitation of such reviews by IS and SAP consultants and by the respective Chiefs/Directors that have staff with access to change, delete and create T-codes in those modules. In this regard, roles should be revised so that only approved personnel have the appropriate access. Finance will update OIG on a quarterly basis on the outcome of HelpDesk ticket #36262 and the agreed upon T-code maintenance process (specific to XK02 and KF02).

Audit Finding #2: OIG reviewed Policy #159 Separation Procedure and related communications from HRS advising management of an employee's termination. The procedure and related communications did not contain specific language or requested action to remove all system access for a terminated employee. In addition, procedures to assess and adjust access for employees changing positions within the Authority were not documented.

Audit Recommendation #2: OIG recommends that Policy #159 Separation Procedure is updated to include specific language regarding the removal of all system access for an employee who terminates employment. Access should be removed as timely as possible

following the employee's last workday. Policies and procedures should be formalized to address an access review process for employees who transfer positions within the Authority. In these cases, only the access required for current responsibilities should be granted and any additional access should be revoked.

Management Response #2: The Director of Human Resources Services concurs with the recommendation. Policy #159 Separation Procedure will be updated to include specific language regarding removal of SAP-ECC/HCM access by HRS and notification by HRS to IS to remove all other system access for terminated employees immediately following the employee's last day of work. HRS will coordinate with IS to formalize a process for adjusting access rights when employees transfer positions within the Authority. Targeted date for policy update is July 30, 2022. Targeted date for transfer process is August 31, 2022.