GAO Topic of the Month – April 2022

ELEVATED USER RIGHTS IN US BANK

Background

This month's topic is elevated user rights in the US Bank system. Individuals within your organization who have administrative privileges with the ability to open and close cardholder accounts and make changes to existing accounts in the US Bank system for purchasing and travel cards, also known as Purchasing and Travel Card Administrators, have elevated user rights. While these roles are necessary, they also have inherent risk. It is important that each agency identify who has elevated user access and provide proper oversight of their actions. This topic will discuss some of these risks and identify how your agency can conduct some basic reviews to mitigate these risks.

What Are The Risks?

1. Unauthorized purchasing and/or travel card accounts opened
2. Unauthorized purchases
3. Unauthorized changes to cardholder accounts
4. Unauthorized changes of single purchase limits, credit limits, and merchant authorization controls

All increased risk can result in increased liability and cost to the agency and the State.

Best Practices for Monitoring Elevated User Access

1. Close any accounts that are no longer being utilized or are not needed
2. No active cards for Card Administrators/elevated access users
3. Review card activity for elevated access users activity
4. Monitor card changes for proper authorization and documentation

Reports to Assist with Elevated User Monitoring

Four US Bank reports can assist with Elevated User Monitoring:

1. System User List W/Account Details Report – This report identifies all active US Bank users at your agency. Active system users can have elevated user access, cardholder access, and view only access. This report can be filtered to identify the different levels of access.
2. Account List Report – This report identifies all individuals with open purchasing and/or travel cards.
3. Transaction Detail Report – This report identifies all purchasing and/or travel card transactions that have occurred.
4. Account History Report – This report identifies all changes made in the system by those with elevated user access.

These reports can be used for a variety of reasons however; majority of this topic's focus is on how these reports can be used to effectively monitor those with elevated user access. This topic will provide

ELEVATED USER RIGHTS IN US BANK

some basic information about how to identify and monitor all levels of access at your agency, including how to utilize these reports to provide sufficient oversight of those with elevated user access. Additional steps may be necessary to monitor all cardholders and the related activity.

Identifying Employees with Active User Status in US Bank

The first step to monitor elevated user rights is to run a report to identify all those with an active user status in the US Bank system. Using this report an agency can identify and verify all active system users. Active system users include individuals with cardholder access, view only access, and elevated user access. If a user has left your agency, moved to another unit or position, has different responsibilities, or may no longer need access, their access should be removed as soon as possible. It is possible that a user who should not have access is still active. A best practice is to generate the System User List report on a regular basis (for both purchasing and travel cards, 1425 or 7129 and 3046 respectively) and verify that all users with an "active" user status in US Bank are in fact still current employees and should have active system access. Leaving unneeded accounts active, invites the possibility, that the account could be used for unauthorized activity or charges that could result in the need to address fraud or employee misuse, which will require much more time, effort, and cost.

US Bank has pre-built reports in their system that can be utilized by Card Administrators or View Only Access Users (see Access Roles in US Bank TOM) to identify access levels of all system users. In the US Bank system, follow these steps:

1. Click on Reporting, then Administration.
2. Under the User Management section, select "System User List w/Account Details."
3. Under User Status, select "Active."
4. Leave Entitlement Group at the default of "All."
5. Leave Account Information at the default of "All."
6. Leave Sort Report By: Processing Hierarchy, Account Number, User ID, and No Sort at the defaults of "Ascending Order."
7. Select "Excel" under Output Type.
8. Under the Group Report By (Processing Hierarchy Position) section enter Bank "1425" or "7129" for purchasing cards; or "3046" for travel cards.
9. Click "Run Report." See the example below:

ELEVATED USER RIGHTS IN US BANK

Users Included

User ID(s): To limit the results from the default of "all," enter a value. Separate multiple IDs by a comma and no spaces.

[   ]   Search for User(s)

User Status:

- ☐ All
- ☑ Active
- ☐ Admin Locked
- ☐ Expired
- ☐ Failed Self Service
- ☐ Password Failed
- ☐ To Be Removed

Entitlement Group(s):

Note: Hold down the Ctrl key to make multiple selections.

```
All
pal_test_client (Global)
testlpj (Global)
vvl upload (Global)
Acct_Prof_Only (Global)
```
Search for Group(s)

Account Information

Account Status:

Note: Hold down the Ctrl key to make multiple selections.

```
All
Open
Closed
Blank
```

Sort Report By

Processing Hierarchy ▾	Account Number ▾	User ID ▾	No Sort ▾
◉ Ascending Order	◉ Ascending Order	◉ Ascending Order	◉ Ascending Order
○ Descending Order	○ Descending Order	○ Descending Order	○ Descending Order

Report Output

Output Type:

[Excel ▾]

Output Parameter Page Placement:

Selection defines the location of the Parameter Page details on the report output.

[End ▾]

ELEVATED USER RIGHTS IN US BANK

Group Report By

◉ Processing Hierarchy Position: *
  If selected, a processing hierarchy position is required.

Bank:	Agent:	Company:	Division:	Department:	
1425					Search for Position or Add Multiple

○ Account Number(s):*
  If selected, at least one account is required. Separate multiple accounts by a comma and no spaces.

	Search for Accounts

Run Report   **Reset**   **Create Scheduled Report**

The report generated will identify all users with active user rights as denoted by the bank code.

Filter Active User Status to Identify Employees with Elevated User Access

The next step is to identify and review the level of access each user has in the US Bank system. The same System User List w/Account Details report can be filtered to identify those individuals who have an "elevated user status." Individuals with elevated user status have a greater inherent risk due to their ability to make administrative changes in the US Bank system.

To identify and filter for "Elevated User Access" utilize the "Entitlement Group" field, and change the filter to include only the following three entitlement groups PAF001, MAC, and USER_SM.

Individuals with this access in US Bank are "elevated users" due to the administrative rights granted with these entitlement groups and your agency should determine if the elevated users have any open purchasing or travel cards. To reduce risk and to have good internal controls, the Administrator role should only be assigned to an individual who does not have a purchasing or travel (CTA or ETC) card. Administrators should not establish cards for themselves, and they should not have the ability to incur charges on any purchasing or travel cards where they are the Administrator.

Identifying Elevated Users with Open Purchasing or Travel Cards

The Account List Report lists all open purchasing and travel cards. In US Bank, select Reporting, Program Management, and Account List. Enter the following parameters:

1. Leave Date as defaulted "Last Maintained Date Range."
2. Under Account Information, Account Status, select "Open" from the dropdown.
3. Leave all other options as defaulted.
4. Under Report Output, Output type, select "Excel" from the dropdown.
5. Under Group Report By, Processing Hierarchy Position, enter 1425 or 7129 for purchasing cards, or 3046 for travel cards (3046 includes both central travel accounts and employee travel cards).
6. Leave all other options blank.
7. Click Run Report.

ELEVATED USER RIGHTS IN US BANK

This report generates a list of all individuals with open purchasing and/or travel cards. Compare this Account List Report against the filtered elevated user System User List Report to determine if any individuals with an elevated user status also have an open purchasing and/or travel card.

Identifying Card Transactions for Elevated Users

Because individuals with elevated user rights can change their card status (open, closed, limits, etc.), confirmation should occur that no purchasing or travel card transactions have occurred for an Administrator or an unauthorized cardholder. The Transaction Detail Report can be used to identify all purchasing and travel card transactions for all cardholders, including those with elevated user status.

To generate this report, select Reporting, Financial Management, and Transaction Detail. Specify the period being reviewed by selecting the transaction date range radio button, and enter the transaction start and end dates. Next, leave all following fields as default, specify the bank code for either purchasing cards (1425 or 7129) or travel cards (3046), and select run report. The Transaction Detail Report will identify all card transactions for the specified type of card during the specified period of review. Use this report to verify that elevated user access individuals do not have purchasing or travel card transactions, especially for a closed/inactive card account.

Identifying Changes for Elevated Users

The Account History Report identifies all changes made to all cardholder accounts, including changes to single purchase limits, credit limits, merchant authorizations, cardholder accounts, and any other change made in the US Bank system. A best practice is to review this report regularly to confirm that all card changes made are properly authorized and documented.

To access this report, click on Reporting, Program Management, and then under the Administration header, select "Account History – Request Status Queue." Enter the following information:

Date:
Choose Request Start Date Range
Enter the Start Date and End Date for the desired period for your review.

Account History Information:
Request Category: Select All
Request Status: Select Complete
Account Request Started By: Leave Blank
Update Method: Select ALL

Sort Report By: Leave as default (Ascending Order)

Report Output:
Output type: Select Excel from the dropdown
Excel Option:

ELEVATED USER RIGHTS IN US BANK

Include Field Maintained: Click the box "Display what fields were maintained with the previous and new values."

Group Report By:
Click the box "Processing Hierarchy Position."
Under the Bank Code field, enter 1425 or 7129 (for purchasing cards) or 3046 (for travel cards).
Click Run Report.

The Account History Report identifies all changes that have occurred for the specified period of review including identifying which specific accounts were modified, what field was changed (including the previous and new value of each change), and the user credentials responsible for the change. Agencies should regularly review changes made to ensure that all changes are valid, approved, and that required documentation is maintained to support any change made.

Conclusion

Someone other than the elevated user should regularly review the authority and actions of elevated users by reviewing and comparing the described reports. First, verify that all individuals with system access are currently in a role that requires this access. Next, verify card administrators/elevated user access users do not have an active purchasing or travel card or related transactions by reviewing the Account List Report and the Transaction Detail Report. Third, ensure that active cards have only been issued to individuals who should currently have a card. Last, review the Account History Report to verify that all changes are valid, approved, and supported by appropriate documentation.

If you have any questions about this topic, reach out to your agency contact who can contact the agency's AFIS Liaison or GAO Internal Audit if any questions remain.