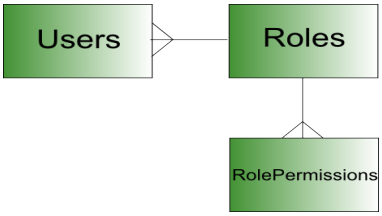
GAO Topic of the Month – March 2022

Access Roles in US Bank



Background

This month's topic addresses the different user access roles in the US Bank system to manage purchasing and travel card accounts and the associated risks. There are three basic access roles when establishing access in the US Bank system: cardholder access, elevated user (full) access, and view only access.

US Bank Access Roles

1) Cardholder Access – This type of access allows a cardholder to view only their specific account information including monthly billing statements, account profile, and other account specific information. These users do not have the ability to make changes in the system.
2) Elevated User (Full) Access – This type of access is provided to Purchasing Card and/or Travel Card Administrators. These users can open and close cardholder accounts and make changes to existing accounts within the system.
3) View Only Access – This type of access provides a user with view only rights that allows them to view all transaction and account related information within the agency.

Access Roles and Separation of Duties

When an employee is issued a purchasing or travel card, they are provided cardholder access (view only) rights that allow the user/cardholder access only to their specific account information within the US Bank system.

When elevated user access or an Administrator is established at the agency, the user can provide maintenance and oversight over the agency's cardholder accounts. Elevated users/Administrators can set up new accounts, close existing accounts, make changes to existing accounts, and can view transaction details.

View only accounts can be established to provide a user with view-only access to view all transaction details and account related information at the agency. This role should be given to an individual who provides oversight and monitoring, but is neither a cardholder nor an Administrator. This view-only access role is critical in providing necessary oversight to those with elevated user access in the system to reduce associated risk at your agency.

What Are The Risks Associated with Elevated User Access?

1) Opening purchasing and travel card accounts without proper authorization
2) Making unauthorized purchases

3) Making unauthorized changes to cardholder accounts
4) Bypassing card restrictions and limitations by making unauthorized changes to single purchase limits, credit limits, and merchant authorization controls

How to Establish View Only Access in US Bank

View-only access can be established by submitting a completed GAO-3C form located on the GAO website: https://gao.az.gov/publications/forms to GAO for processing.

Why Should My Agency Establish a View-Only Access Role?

This role allows users to provide oversight of changes made in the system by Card Administrators (Elevated User Access). This individual should NOT be an employee with a state issued purchasing or travel card nor a Card Administrator. View-Only Access Users should review reports in US Bank to identify changes made to existing accounts, including changes to credit and single purchase limits, merchant authorization controls, and the creation of new accounts to verify that all approvals and related documentation are present. Users in this role should report to someone other than the Card Administrator(s).

Account History Report (Identifying Changes in the US Bank System for Elevated Users)

The Account History Report is available in US Bank and identifies 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. It is a best practice to regularly review the report to confirm that all card changes that have occurred are properly authorized and documented. It is critical that an individual other than the Administrator or cardholder conducts this review. This provides separation of duty and is a good internal control. If inappropriate or unauthorized actions have occurred, this individual should raise the issue with the proper individuals for further action.

To access this report, click Reporting, Program Management, and 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)

GAO Topic of the Month – March 2022

Access Roles in US Bank

Report Output:
Output type: Select Excel from the dropdown
Excel Option:
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 statewide purchasing cards) or 3046 (for statewide travel cards).
Click Run Report.

This report identifies all purchasing card and/or travel card 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 changes. The agency 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

GAO strongly recommends that agencies with Purchasing Card or Travel Card Administrators establish this view-only access role at your agency to provide necessary oversight within the US Bank system. All agencies can establish users with the view-only access role to monitor activity for their agency.

Please contact your AFIS Liaison or GAO Internal Audit if you have any questions regarding this topic.