COLUMBIA BANK

Security Procedures in Commercial Online Banking

Commercial Online Banking has multiple layers of available security controls to assist in reducing fraud related to payments leaving Columbia Bank. This document will explain security controls we have in place and provide recommendations for additional controls to help protect your company from fraudulent activity and any related financial loss.

Required Security

The following security controls are required.

Advanced Login Authentication

Advanced Login Authentication is a standard and required part of every login to Commercial Online Banking. It includes the requirement for unique credentials (a Company ID, a User ID, and a Password) and also uses complex device identification processes at each login. If the device cannot be identified, then the individual logging in is required to perform additional authentication, called step-up authentication.

When a user is stepped up, they are required to confirm a one-time, single-use security code using either a voice-recorded call or a text message. This is called out-of-band authentication. Once the code is successfully confirmed, the user may enter their password and complete the login.

Transaction Monitoring

We use transaction monitoring to identify and establish typical transaction patterns for our customers. Our transaction monitoring service runs each outgoing ACH and wire transaction through transaction monitoring to validate that the transaction fits within acceptable parameters of your typical usage. For transactions that might be unusual, the system will seek additional approval behind-the-scenes from the bank before releasing the transaction. As part of this process, we may call your Primary Contact to validate the transaction.

Out-of-Band Transaction Approval

Out-of-Band Transaction Approval is the standard for added authentication when approving outgoing monetary transactions, such as ACH or wires. When a user is approving a transaction, they are required to confirm a one-time, single-use security code using either a voice-recorded call or a text message. Once the code is successfully confirmed, the transaction is approved.

Some customers may use tokens as an alternative to the standard out-of-band authentication process. Customers who currently use tokens may continue to do so.

Recommended Security – Dual Control

The following security controls are recommended for customers. As noted in Columbia's Terms & Conditions as applied to Commercial Online Banking, if you elect to use security procedures other than those we recommend, and those security procedures provide less protection against unauthorized transactions or activity than the security procedures offered by Columbia:

- The security procedures you choose to use will be considered "commercially reasonable" to the same extent as the security procedures offered by Columbia that provide greater protection; and
- You shall indemnify and hold Columbia harmless from and against all losses and liabilities relating directly or indirectly to your use of such security procedures.

Columbia reserves the right to issue new security procedures and/or to cancel or change any security procedures from time to time.

Introduction to Dual Control

Dual control can be implemented in a number of ways depending on what works best for your company. Most dual control options utilize a combination of the three User Roles available in Commercial Online Banking to enforce a separation of duties and require at least two individuals to be involved in any outgoing transaction. The User Roles are defined below:

- **Setup Role**: Allows user to setup templates – This entitles the user to template setup capabilities for only those services and accounts to which the user has been entitled.
- **Approval Role**: Allows user to approve transactions – This entitles the user to transmit capabilities for only those services to which the user has been entitled.
- **Administration Role**: Grants administration privileges – This will allow the user to add, modify, copy and delete users, modify their roles, services and account access, rename accounts, and modify the number of approvers required for requests.

Dual Control - Administration

Dual control of administration will ensure that no administrative duties can be completed without at least two individuals from your company.

- **How to set it up**: Create an additional user with the Administration Role in addition to yourself. Then proceed to the Manage approval settings screen and enter a '2' in the Administration field. This will ensure adding, removing, and modifying all other users and permissions in Commercial Online Banking will be handled under dual control.
- **How it can help mitigate fraud**: Dual control prevents any one user from having complete system access with no additional oversight. Without it, a user with a compromised login could create additional users, change permissions, and lock other users out, for example. Enabling Dual Control for administration means that you will have at least two sets of eyes on every user that is created, every password changed, every additional permission given, etc.

Dual Control – Template Maintenance

Dual control of ACH and wire templates will ensure that no templates are created or altered without input from at least two individuals from your company.

- **How to set it up**: Create one user with the Setup Role and another user with the Approval Role. The Setup Role user will be in charge of creating and maintaining the templates. The Approval Role user will be in charge of reviewing the template changes and approving them.
- **How it can help mitigate fraud**: Dual control prevents any one user from having complete system access with no additional oversight. Without it, for example, a user with a compromised login could alter the routing and account number on a wire template, and no other users would be informed. Enabling Dual Control for template maintenance means that you will have at least two sets of eyes on every template that is added, or changes made, such as changes to dollar amounts, destination accounts, etc.

Dual Control – Transaction Approval

Dual control of outgoing ACH and wire transactions will ensure that no funds are released from your accounts without input from at least two individuals from your company.

- **How to set it up**: There are two ways to set up dual transaction control. The first way is to simply have a user with the Administration Role edit approval requirements so that ACH and wire transactions require separate entry from approval. This option requires one user to create the transaction and a separate user to approve and transmit. The second way is to create one user with the Setup Role and another user with the Approval Role. The Setup Role user will be in charge of creating and submitting the transactions. The Approval Role user will be in charge of reviewing the transactions and approving them.
- **How it can help mitigate fraud**: Dual control prevents any one user from having complete system access with no additional oversight. Without it, for example, a user with a compromised login could submit fraudulent ACH or wire transactions, and no other users would be informed. Enabling Dual Control for transaction approval means that you will have at least two sets of eyes on every outgoing ACH or wire transaction.

Questions

If you have any questions or would like assistance in setting up recommended security, contact us at 866-563-1010 or securely using Commercial Online Banking.