Security tips for Digital Business Banking

Florida Credit Union

Account Signatories & Contact Information

First, ensure that Florida Credit Union has updated contact information for your business. This includes the contact information for all the signers of the account. To update account signatories, please contact Member Services or your Business Relationship Manager.

Usernames & Passwords

Review and change your username if necessary. Your username should be a unique set of at least eight characters and *should not contain* any confidential information, such as your *Member Number, TIN, SSN* (full or partial), etc.

Furthermore, your password must be at least 8 characters in length and contain upper-case letters, lower-case letters, numbers, and special characters. The platform will require that your password contain at least three of these components. The longer and more complex the password, the better! For additional security, change your password every six months. This can be completed on the Security Tab within Settings.

FCU recommends that you utilize a password manager or vault to create and store passwords. Avoid replacing letters with special characters as this tactic is known to fraudsters, i.e. replacing any "A/a" with @, "S/s with $, or "E/e with 3.

We also recommend that all users register and login with a username assigned to the individual user. *Do not share usernames and passwords with others to access FCU Anywhere.*

Authentication

FCU Anywhere uses Two-Factor Authentication (2FA) or Step-up Authentication based on login conditions and specific transaction requests. We offer four types of verification methods, where a code is provided, when 2FA or Step-up Authentication is required: Authenticator App, SMS Text Message, Phone Call or Email. You have the option to enable or disable each method. You can also set a preference causing the platform to display that method as the first choice.

FCU recommends using the Authenticator App method when configuring Two-Factor Authentication. Download the app of your choice (Google Authenticator, Microsoft Authenticator, Authy, Duo, Etc.), complete the steps in FCU Anywhere and set it as your preferred method. Furthermore, set up SMS Text Message or Phone Call as a secondary method in case there is an issue with the authenticator app. Don't forget to disable Email, as it is the least secure method, and disable any other unused or undesired methods. For more information on Authentication Methods, please visit flcu.org/account-security.

Ensure that all users with access to your business account have enabled their contact methods (Settings > Contact) and configured authentication methods (Settings > Security).

Alerts

We offer a wide variety of alerts to assist you in maintaining your account. Alerts range from general, required alerts regarding profile and security changes, to optional transaction alerts. Alerts can be delivered via Email, SMS text message or Push Notification. Please see below for a list of alerts that we believe you will find useful in maintaining your account.

- **General Alerts -** Sent when changes to personal information or other important events occur. These alerts are required and automatically turned on (via email notification) for everyone. You can set additional delivery preferences.
- **Account Alerts -** These alerts notify the user of specific transactions types, transaction amounts or balance alerts. Configuration and delivery options are available with each alert.
- **Authentication Alert -** This alert notifies the user when the account is accessed. Remember if you use

aggregation services (such as QuickBooks) where you have provided the company with login credentials, you may be notified of logins made when the aggregation service is collecting data.

- **Business ACH Alerts -** If you use Business ACH to originate ACH transactions to vendors and employees, alerts can be configured to provide Business ACH transaction statuses like when a transaction needs to be authorized, or when the transaction has been approved, denied, etc.
- **Business Admin Alerts -** Available for when new Business Sub Users have been added for access to your business account and when a Business ACH or Business Wire payee's information has changed.
- **Business Wire Alerts -** If you use Business Wires to originate wire transactions, alerts can be configured to provide Business Wire transaction statuses like when a transaction needs to be authorized, or when the transaction has been approved, denied, etc.
- **Transfers Alerts -** Sent when external accounts are added or when transfers are submitted, fail or succeed.

The more alerts that you setup, the more vigilant you can be with your accounts without the need to login every day. If you did not make a change to your account or perform a transaction, but received an alert that information was updated, you should notify FCU immediately, and allow us to review your online activity for anything suspicious or out of the ordinary.

Business Admin Sub Users & Payees

Within Business Admin, members enter payees for the Business ACH and Business Wire services. The list of payees should include payees that have been paid within the last six months. Delete payees to whom that the business no longer sends funds. Also, ensure that payee information is up-to-date. This will ensure that payments are delivered to the correct recipient and mitigate potential losses.

The Business Admin widget also provides the Master Business User with control over User Roles and Sub Users. We *strongly recommend* that Roles and Users are set up to allow for "dual control." For example, a user role can be configured to submit Business ACH, Business Wire and External Transfer transactions, but another user role can be configured to authorize the transmission of those transactions (over user-defined amounts). It provides an approval process, which protects the funds in the account, as large transactions will need two users to transmit funds.

Make sure that user lists are kept current. Block users that should no longer be accessing the account. Carefully maintain user roles to ensure sub users only have the desired access. Ensure that usernames follow the same recommendations as listed above in User Names & Passwords and change passwords regularly to maintain security. Sub users should also maintain updated contact information within the platform and utilize the recommended authentication and alert methods.

Settings Review

When logging in to FCU Anywhere, all users should view their profile periodically. Recent Activity provides dates and times of recent system logins. In addition to Username, Password and Multifactor Authentication settings, the Security tab allows the user to view Remembered Devices. We recommend that old devices no longer in use should be removed from this section immediately. Review your contact information and ensure that contact numbers and emails are up-to-date, preferred contact selected and opted-in to available communication methods.

Positive Pay Services

Florida Credit Union will be implementing Positive Pay services in 2023 for both check and ACH transactions. Commercial clients will have the opportunity to enter an approved list of outstanding checks and ACH vendors to ensure only authorized transactions clear the business account. Furthermore, our business members who use our Business ACH credit origination services will have additional features to approve outgoing transactions as well as electronically receive Notice of Change and Return information. Businesses utilizing our wire origination service will have ability to verify outgoing wires using voice biometrics. Contact your Business Relationship Manager if you are interested in these services to review pricing and implementation information.

Current Fraud Trends

Finally, visit our fraud trends page at flcu.org/account-security or our blog at flcu.org/blog to stay abreast of the ways scammers are committing fraud in today's financial environment. Ensure that anyone connected to your business account is aware of current fraud trends so they don't fall prey to scams that can negatively affect your business account.