



Restriction of Products and Services to Members Based on Account Abuse or Fraud

Upon discovery that a member may be engaging in activity that increases the Credit Union's risk of loss or that may jeopardize member account security, the Credit Union will promptly review the situation and take any necessary action.

If any Credit Union employee determines that a member may be of higher risk to the Credit Union, the member will be referred to the Risk Management Department for further review of the situation. The Risk Management Department, in consultation with management as appropriate, will determine if further action is required.

The Risk Management Department will perform a review of the situation, which may include contacting a member, reviewing account records, reviewing online banking activity, and conferring with other Credit Union employees.

Based on review of the member's account and conduct, the Credit Union may restrict access to products and services that it has reason to believe may pose a greater risk to the Credit Union and/or to a member's account. The Credit Union will review each situation on a case-by-case basis and make a determination as to the appropriate resolution. This may include suspension of products and services to the extent that the Credit Union deems appropriate and where there is a logical relationship between the conduct and the services.

If the Credit Union restricts services based on activity and/or behavior, the Credit Union may restrict services for all accounts held in a member's own name or owned jointly by them. The Credit Union may restrict services based on the activity of any share holder for all shares held by a person, in their own name or held jointly.

The following list outlines some situations in which the Credit Union may choose to restrict a member's access to products and services. This list is not intended to be all-inclusive; rather, this list is intended to be illustrative and the Credit Union shall be authorized to impose restrictions for any behavior or conduct which it determines poses a higher risk to the Credit Union or to any member account.

- A member has negotiated, or attempted to negotiate, checks or other instruments that the Credit Union reasonably believes are fraudulent or otherwise non-negotiable
- The Credit Union has reasonable belief that a member has fallen for a scam or has done so in the past
- A member's online account access has been compromised. This may be a result of:
 - A member provided credentials to a third party
 - A member allowed a third party remote access to their computer
 - A member's electronic device is hacked or may have been otherwise compromised
- A member has a history of credit, debit, and/or ATM card fraud
- A member has had ACH fraud or abuse on their account
- There has been abuse of the ACCESS-A-Bill service on an account, such as initiating a payment when there are not sufficient funds in an account
- A member has provided personal, account, or other confidential information to a third party who the Credit Union reasonably believes may be involved in a scam, or who has no apparent and legitimate business need to have access to such information
- A member has put the Credit Union in a situation that results in, or reasonably may result in, loss of funds or exposure of data



Based on the Credit Union's review of the situation, services may be restricted or suspended. This may include, but is not limited to, restriction of some or all of the following products and services:

- Debit, Credit, and/or ATM Card
- Online Banking, including Mobile Check Deposit, ACCESS-A-Bill, POP Money, Bank 2 Bank
- Ability to negotiate checks for cash or deposit in any manner (e.g., in person, via night drop or ATM deposit, Mobile Check Deposit)
- Ability to receive ACH transactions
- Ability to apply for products electronically (e.g. MeridianLink)
- Ability to maintain Share Draft accounts
- Any other product or service that the Credit Union determines would not be prudent to permit the member to have access to

The Credit Union will take appropriate actions to reduce the Credit Union's exposure and risk. The Credit Union is committed to treating all members fairly and with respect and will not discriminate against any members based on prohibited classes. To this end, the Credit Union will comply with the Equal Credit Opportunity Act (ECOA) and all other policies, laws and regulations that protect consumers from unfair or unequal treatment.

The Credit Union is required, by the Federal Credit Union Act, to continue to allow members, who have caused the Credit Union a loss, to maintain a share account and to have a vote at any membership meetings (i.e., special and annual meetings), unless the Credit Union initiates expulsion proceedings as allowed in the Federal Credit Union Act.

Approval Process for Restriction of Products and Services

The decision to restrict services to a member will require approval of at least two of the following three employees: the President & CEO, the Chief Information Officer (CIO), and the Assistant Vice President of Risk Management.

Any Assistant Vice President, Vice President, the CIO, or the President & CEO may choose to place an administrative hold on access to certain products or services for a reasonable period of time to allow for appropriate review of the situation. This hold may be placed to the extent necessary to protect the Credit Union or a member's account.

The Credit Union will implement procedures to carry out this policy. This may include maintaining a list of scenarios and recommended actions. However, based on each situation, the Credit Union may impose more or less restrictive actions as deemed appropriate given the specific facts and review of each scenario.

At a later time, the Credit Union may choose to reconsider a member's access to services if it is determined that a member no longer poses an elevated risk. The Credit Union may choose to reinstate only those services that the Credit Union feels are appropriate given the risk level of a member.