Reference Guide

AuditLink

Tools for Blocking Member Activity

Member-level controls, product-level controls, and block lists

INSIDE THIS GUIDE:

This guide describes the CBX options available to block or limit a person/organization's activity, including member-level and product-level switches, block lists, account freezes, and available funds verification.

Last Revision date: November 17, 2025

Find other Reference Materials page on our website: https://www.cuanswers.com/resources/doc/cubase-reference/

Start your online help journey here:
https://help.cubase.org/cubase/Welcome.htm

Table of Contents

Introduction

CBX offers many different controls for blocking member transactions or enrollments based on member-level, product-level, or transaction-level attributes.

A single person or organization can be added to multiple blocking mechanisms. If you wish to block the person or organization from performing or enrolling in more than one service, then you should add that SSN/TIN to the blocking mechanisms that apply.

The CU*Answers AuditLink team is here to assist at any time. Find us, contact us, and learn more via The Store | The Website | Email

Available Funds

This is the most basic "stop and check" feature of all, as most, if not all, posting and transaction UI programs check for available funds (as well as freezes) before allowing activity to occur, although batch programs (like ACH and share drafts) have exception processes that can kick out the item for CU intervention.

NOTE: For ACH on-demand posting, available funds verification will be run against the savings/checking account from which the fee will be taken. If configured, the fee can be drawn from the base deposit (99) account, regardless of available funds.

Account Freezes

The biggest blunt instrument of all, a freeze effectively stops all deposit and/or withdrawal activity on a specific sub-account. An account freeze applies to all transactions through all activity channels for the frozen account, depending on the freeze code.

There are options to freeze just withdrawals/disbursements, just deposits/payments, or both deposits and withdrawals. Frozen accounts should be backed up with internal policies and instructions from a collections officer so that front-line and other personnel know how to handle the account.

Learn how to freeze an account and remove a freeze status in Show Me the Steps.

Member/Account-Level Controls

The core offers many on/off flags at the member or account level that control whether a member can use a particular feature or not. These parameters target specific products for a specific member to block enrollments, transactions, or data maintenance.

Examples of member/account-level controls (not all-inclusive):

- Activate online banking or audio response
- Allow shared branch transactions (flag on the member record)
- Deny new memberships (flag on the non-member record)
- ARU/OLB transfer controls
- PIB controls
- Stop pay orders
- ANR limits
- ATM/debit spending limits & supported features (**Tool #11 *ATM/Debit Card Maintenance***)
- Plastic block codes and status codes
- **Tool #1870 *Block Accounts for In-House Checks***
- Block from skip-pay programs

Product Service Parameters

Within the core, you have some options to configure global controls at the product-level that provide boundaries for "normal" acceptable activity with either error messages or exception handling for any activity outside of those boundaries.

Examples of product-level controls (not all-inclusive):

- Max # of RDC deposits and $ per day or per 30 days
- Max A2A transaction $ amount per day or per 30 days
- Max transfer amounts via online/mobile/audio banking
- Skip-pay program qualifications

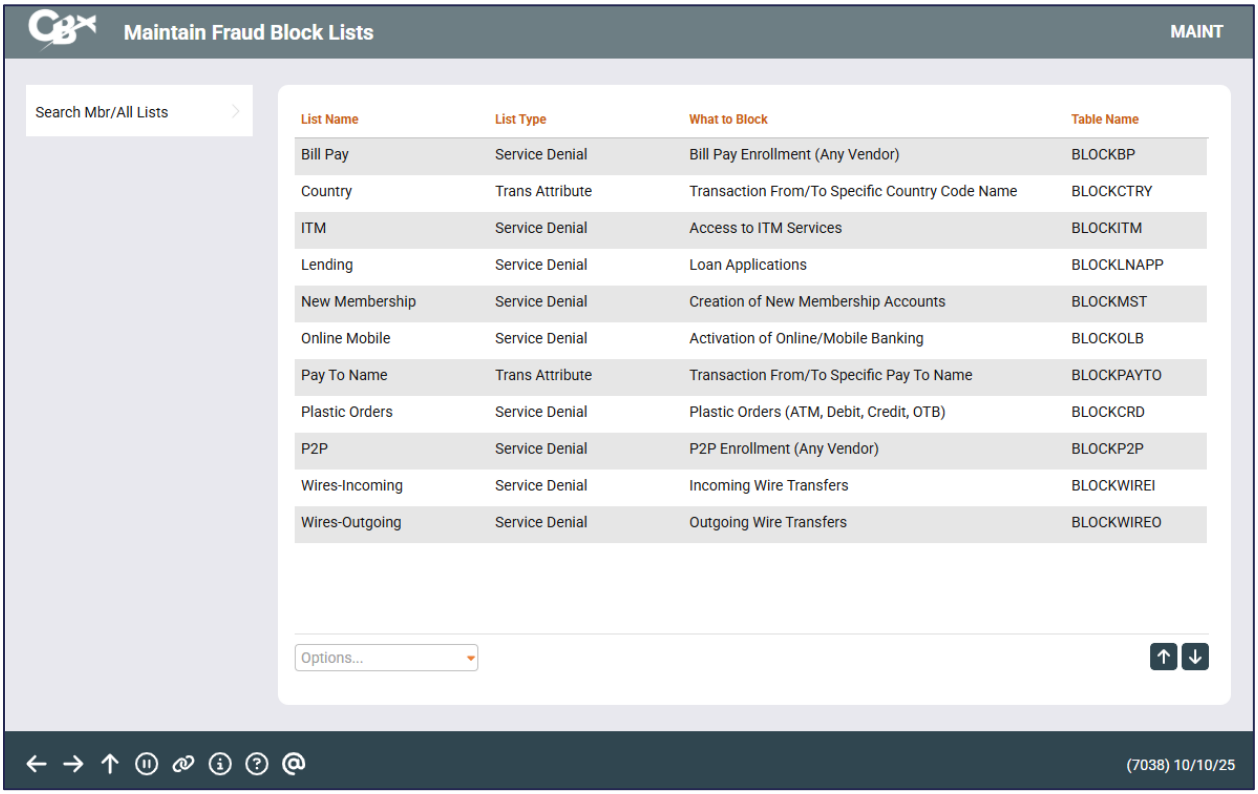
Fraud Block Lists

Block lists are product-specific controls to prevent transactions or enrollments. More granular than freezes and on/off switches, these were designed to supplement product service parameters at a specific member/account level.

There are two main categories of block lists: denial-of-service and transaction attribute.

All block lists are located in **Tool #892 *Update Fraud Alert/Blocked Persons List***. Use this tool to log member accounts where you've seen fraud in the past. Your Auditors can access the Block List Database Inquiry via **Tool #1892 *View Fraud Alert/Blocked Persons List***.

Maintain Fraud Block Lists (Tool #892)



You can use **Search Mbr/All Lists** to search for denial-of-service block lists a person/organization is on. This inquiry does not list the entries made on the transaction attribute block lists. A separate review of the transaction attribute fraud block lists will be needed.

Denial-of-Service Block Lists

A denial-of-service block is a single service block that blocks an SSN/TIN from enrolling in a service (such as bill pay) or using a particular feature or service (such as an outgoing wire transfer).

There are lists to block:

- Bill Pay enrollment (all vendors)
- P2P (Person to Person) enrollment (all vendors)
- Outgoing wire transfers (performing a wire transfer)
- Incoming wire transfers (performing a wire transfer)
- Online/mobile banking (enrollment)
- Lending (creating a loan application or opening a loan)
- Plastic orders (new and reorders)
- New membership (opening a new membership)
    - Override available

Denial-of-service block lists, except the New Membership Block List, require an entry to include an SSN/TIN that is in the MASTER/membership.

When adding an entry to these lists, you can enter either the SSN/TIN or name. If you enter the SSN/TIN, the name will populate and a message displaying 'SSN/TIN number found in Master file'. If you enter a name, a warning message will display 'Name exists in Membership/Non-Member file. Check SSN/TIN #'. Verify the name and SSN/TIN and select **Update** to add the new entry. If the SSN/TIN or name are not found within the MASTER/membership files, the warning message will read either 'No master record found' or 'Membership SSN not found'.

The New Membership Block List differs from all the other denial-of-service block lists in its requirements for entries and the ability to override a suspected match. Learn more about entry requirements for the New Membership Block List on page 8 below.

Bill Pay Block List

The **bill pay block list** prevents a member from being enrolled in bill pay. (All bill pay vendors are supported.) You may need to first unenroll the member from the service.

If the member is already enrolled in bill pay, unenroll them through the core (using **Tool #14** ***Member Personal Banker***) and the vendor website. Then, the block list will prevent them from re-enrolling. It will also prevent them from enrolling in bill pay from another membership with the same SSN/TIN.

If a person or organization is added to the bill pay denial-of-service block list, an employee cannot enroll any membership with this SSN/TIN into bill pay. If the employee tries (via **Tool #14** or during the membership open process), they will see messaging that the "SSN/TIN appears on block list".

If membership with an SSN/TIN added in the bill pay block list selects *Enroll in bill pay* in online/mobile banking, the member will see the following messaging: "We're sorry, but your account has been blocked from enrolling in this service. Please contact the credit union for more information."

If a match is found on a block list, follow your credit union policies and procedures. (In order to remove the block, you will need to remove the SSN/TIN from the appropriate block list. Learn how in Show Me the Steps.)

P2P Block List

The **P2P block list** prevents a member from being enrolled in Person to Person (P2P). (All P2P vendors are supported.) You may need to first unenroll the member from the service.

If the member is already enrolled in P2P, unenroll them through the core (using **Tool #14 *Member Personal Banker***) and the vendor website. Then, the block list will prevent them from re-enrolling. It will also prevent them from enrolling in P2P from another membership with the same SSN/TIN.

If a person or organization is added to the P2P denial-of-service block list, an employee cannot enroll any membership with this SSN/TIN into P2P. If the employee tries to enroll the member in P2P (via **Tool #14** or during the membership open process), they will see messaging that the "SSN/TIN appears on block list".

If a membership with an SSN/TIN in the P2P denial-of-service block list selects *Enroll in P2P* in online or mobile banking, the member will see the following messaging: "We're sorry, but your account has been blocked from enrolling in this service. Please contact the credit union for more information."

If a match is found on a block list, follow your credit union policies and procedures. (In order to remove the block, you will need to remove the membership from the appropriate block list. Learn how in Show Me the Steps.)

Outgoing Wire Transfer Block List

The **outgoing wire transfer block lists** blocks outgoing wire transfers for members.

If a person or organization is added to the outgoing wire denial-of-service block list, an employee cannot send an outgoing wire for any membership with that SSN/TIN. If the employee tries to send an outgoing wire via **Tool #73 *Post Wire Transfer to Member Account*** and selects Outgoing, they will see messaging that the "SSN/TIN appears on block list".

If a match is found on a block list, follow your credit union policies and procedures. You may consider also adding the member to the incoming wire fraud block list. (In order to remove the block, you will need to remove the membership from the appropriate block list. Learn how in Show Me the Steps.)

Incoming Wire Transfer Block List

The **incoming wire transfer block list** blocks incoming wire transfers for members.

If a person or organization is added to the incoming wire denial-of-service block list, an employee cannot send an incoming wire for any membership with that SSN/TIN. If the employee tries to send an incoming wire via **Tool #73 *Post Wire Transfer to Member Account*** and selects Incoming, they will see messaging that the "SSN/TIN appears on block list".

If a match is found on a block list, follow your credit union policies and procedures. You may consider also adding the member to the outgoing wire fraud block list. (In order to remove the block, you will need to remove the membership from the appropriate block list. Learn how in Show Me the Steps.)

Online/Mobile Fraud Block List

The **online/mobile fraud block list** prevents a member from being enrolled in online/mobile banking. You may need to first unenroll the member from online/mobile banking.

If a person or organization is added to the **online/mobile block list**, an employee cannot enroll any membership with this SSN/TIN into online banking via **Tool #14**, during the membership open process, or directly via the OLBPIN shortcut. When they try to check the *Activate Online Banking* checkbox on the Audio/Online Banking screen, they will see messaging that the "SSN/TIN appears on block list".

If a match is found on a block list, follow your credit union policies and procedures. (In order to remove the block, you will need to remove the membership from the appropriate block list. Learn how in Show Me the Steps.)

IMPORTANT: With the online/mobile block list, you need to remove any prior access granted (via online, mobile, or jump) for any memberships owned by the SSN/TIN.

To remove all of these access points, first research all accounts owned by the SSN/TIN. Then, uncheck the *Online Banking* checkbox on the ARU/Online Banking Access screen (accessed via **Tool #14**) for all accounts. Unchecking this box prevents online, mobile, and jump access to this account. Being on the block list prevents this box from being rechecked. Be sure to do this for all accounts.

- NOTE: While unchecking *Online Banking* blocks jump access to the account, the CBX screen showing jump access granted is not changed by default. Your credit union may also elect to uncheck *Jump* on the Manage Member See/Jump Access screen (accessed by **Tool #14** and selecting *See/Jump relationships*).

Lending Block List

The **lending block list** presents a warning to loan officers when a loan application is submitted by one of the blocked members or created in the core for a blocked member. (TIP: The lending block list file can also be included in a Query to exclude these members from self-service lending products such as 1Click Offers.)

If a person or organization is added to the **lending block list**, an employee cannot open a loan under any membership owned by that SSN/TIN. They will see messaging that the "SSN/TIN appears on block list" directly after selecting the membership when attempting to create a loan application for that SSN/TIN in CBX. If the loan officer makes it to the loan creation screen, they will be blocked from opening the loan on that screen.

Memberships on the lending block list will be able to apply for a loan online or via an indirect channel, but the loan officer will see messaging "On Fraud Block List" when working the incoming loan application and will not be able to create the loan.

If a match is found on a block list, follow your credit union policies and procedures. (In order to remove the block, you will need to remove the membership from the appropriate block list. Learn how in Show Me the Steps.)

Plastic Orders

The **plastic orders block list** blocks orders for ATM/debit or credit/OTB cards for members.

An employee will be unable to order an ATM, debit, or credit card for a membership with an SSN/TIN that appears on the plastic orders block list. If the employee tries to order a card (via **Tool #11** or **Tool #12**,

during the membership open process, when creating a credit card loan, or when adding an OTB credit card), they will see error messaging that the "SSN/TIN appears on block list".

If a match is found on a block list, follow your credit union policies and procedures. (In order to remove the block, you will need to remove the membership from the Plastic Orders block list. Learn how in Show Me the Steps.)

New Membership Block List

The **new membership block list** blocks an SSN from opening a new membership. It also blocks a credit union employee from creating a non-member record or pre-membership loan request for that SSN/TIN. Overrides are available with matches to this list.

This fraud block list is designed as a supplement to the *Deny Membership* check box available on the non-member record.

A person or organization can also be added to the new membership block list when a loan is written off or a loan or share draft is charged off by checking *Add member to blocked persons list*.

When the Block List is Run

The membership block list scan can be run manually while a change is made to a member or non-member record by clicking (variously named) block scan buttons:

- Creating a new membership via **Tool #3 *Open/Maintain Membership/Accounts***.
- Creating a non-member record via **Tool #997 *Work with Non-Member Database***.
- Creating a pre-membership loan request.
- Opening an online membership via **Tool #13 *Work Online Banking Apps/Requests***.
    - Additionally, any MOP request will be run past this list, and all "hits" will become a membership application instead of an automatic account.
- Adding a member or non-member as a secondary name to an account.

Your credit union can set your Membership Workflow Controls so that names are scanned against the block list automatically during the above processes. The one exception is the pre-membership lending, since then it is run regardless of the setting.

When the new membership fraud block scan is run, the employee is presented a window alerting them if "no match was found" or if "a suspected match was found."

If a suspected match was found, is it recommended that the employee follow credit union policies and procedures. From the "Suspected match was found" window, the employee has the option to view the membership block list for any comments you may have added, to back up and enter a new name, to create a denial form, or to override the warning.

Block List Entries and Matches

When making an entry to this block list, you have the option of adding an SSN/TIN and name, just an SSN, or just a name. You can enter a name/SSN without a match to the existing membership database.

Entry Recommendations:

- When entering just a name, it is recommended to enter the name in various formats to supply a match to whatever name might be provided when attempting to open a membership in the future.
- If you have an actual, valid SSN, it is usually best to enter that only with no name to avoid missing a match when a name happens to be spelled wrong or when an alias is used.
- If you add only an SSN to this block list, you can use the *Comment* fields to add the person's potential name as a cross reference.
- When entering organization names, it is recommended to leave out common words (e.g., inc, company, co) as the new membership's name will need to be an exact match to the block list entry to trigger a block.

This is how the matches are made:

If this data is entered...	***This is what will be matched...***
ID #/SSN	Must have an exact match to all digits to be considered a suspected match. NOTE: If an SSN/TIN is included along with a name in an entry, suspected matches will meet the matching requirements for both the SSN/TIN and the name entered.
Organization Name	Must have an exact match to all characters to be considered a suspected match. (Remember you can create as many entries as you wish for possible spelling variations.)
Last name only	Members with exact last name will be considered a suspected match, regardless of the first name. Name matches are exact; variations are not blocked (e.g., "Adamson" will not be considered suspect if "Adams" is on the blocked list).
Last name and full first name	Members with an exact match of both first and last name AND members with an exact match of the last name and the *same first initial* will be considered a suspected match. Name matches are exact; variations are not blocked (e.g., "Adamson" will not be considered suspect if "Adams" is on the blocked list).
Last name and first initial	Members with an exact match of the last name and the same first initial (first name beginning with that letter) will be considered a suspected match.

Below are examples of entries for the **new membership** block list and examples of which names will be blocked as a result of a suspected match. (These blocks can be overridden.)

Examples (Individuals)				
Database Entry		***Actual Member Name***		
First name	*Last name*	*First name*	*Last name*	*Blocked?*

<blank>	Michaels	F	Michaelson	No
		J	Michaels	Yes
		John	Michaels	Yes
		Clara	Jordan-Michaels	No
		Clara	Michaels-Hill	No
Sasha	Fredricks	S	Fredricks	Yes
		Sasha	Fredrickson	No
		Sophie	Fredricks	Yes
		Jane	Fredricks	No
<blank>	Christianson	Jane	Christian	No
		J	Christianson	Yes
Tom	Ericks	Thomas	Ericks	Yes
		T	Ericks	Yes
		T	Erickson	No
		Tom	Erickson	No
		Tony	Ericks	Yes
		Freddie	Ericks	No
T	Web	Tanya	Web	Yes
		T	Webster	No
		J T	Web	No

Examples (Organizations)		
Database Entry	***Actual Member Name***	
Name	*Name*	*Blocked?*
Thomas Home Care	Thomas Homecare	No
	Thomas Home Care (entered in DBA field)	No
	Thomas Home	No
	Thomas Home Care	Yes
John Freda Company	J Freda Company	No

	Jon Freda Company	No
	John Freda Company	Yes

Maple Inc	Maple Inc.	No
	Maple	No
	Maple Inc (entered in DBA field)	No
	Maple Inc	Yes

Transaction Attribute Block Lists

These fraud block lists are based on a particular data element and will stop specific transactions from occurring across various delivery channels and memberships. Scans against these block lists include an override option.

There are two transaction attribute block lists: the **Country Block List** and the **Pay To Block List**.

Country Block List

The **Country block list** prevents an account from posting an outgoing wire transfer if a blocked country name is used.

When the Block List is Run

This list is run when posting outgoing wire transfers. When the country block list is run, the employee is presented a window alerting them if "no match was found" or if "a suspected match was found."

If a suspected match is found, it is recommended that the employee follow credit union policies and procedures. From the "Suspected match was found" window, the employee has the option to view the block list for comments, to back up, or to override the warning.

(In order to remove the block entirely, you will need to remove the country from the appropriate block list. Learn how in Show Me the Steps.)

Block List Entries and Matches

An exact match to the block list entry is needed to flag an item. For example, if you enter "Freeland" in the field, an entry of "North Freeland" would not be a match.

When making an entry on the country block list, it is recommended to enter the name in various formats to supply a match to the attribute provided. (NOTE: The block list is different than the matching of the country name with an OFAC scan.)

Pay To Block List

The **Pay To block list** prevents an account from posting an Accounts Payable Quick Check, miscellaneous credit union checks, checks/money orders issued by teller or Phone Operator, loan disbursement checks, and outgoing wire transfers whenever the Pay To name matches an item in the block list.

When the Block List is Run

The "Pay To name" is run against the following attempts to disburse funds:

- Outgoing wire (**Tool #73 *Post Wire Transfer to Member Account*** and select *Outgoing*).
- Teller checks and money orders (Process Code Issue Check(s) Against Account (C) or Issue Money Order(s) Against Account (M))
- Phone Operator checks (Select an account and the *Check* option)
- Loan disbursements (**Tool #50 *Disburse Member Loan Funds***)
- AP Quick Checks (**Tool #1961 *AP3: Process Accounts Payable Payments***, then **Create Quick Check**. The messaging will appear when the vendor is selected.)
- Miscellaneous expense checks (**Tool #667 *Print Miscellaneous Checks***)

When the pay to name fraud block scan is run, the employee is presented a window alerting them if "no match was found" or if "a suspected match was found."

If a suspected match is found, it is recommended that the employee follow credit union policies and procedures. From the "Suspected match was found" window, the employee has the option to view the block list for comments, to back up, or to override the warning.

(In order to remove the block entirely, you will need to remove the pay to name from the appropriate block list. Learn how in Show Me the Steps.)

Block List Entries and Matches

A block list database entry including all of the characters entered as the Pay To name, in the same order, creates a match. The database entry must include the whole Pay To name string in the same order to display an alert, but it does not need to be an exact match. A match can still occur even if there are extra characters in the block list database entry not included in the Pay To entry. Extra characters in the database entry may appear at the end of the Pay To name string or wherever there is a space. There is no case sensitivity when matching.

> *For example, if 'ABC E HI' is entered as the Pay To name, then the system will search the database for: 'ABC[anything here]E[anything here]HI[anything here]'. This would match database entry 'ABCEFGHIJ' and 'abcd.efghijk'.*

If a match is found, an alert is displayed on the screen.

When entering a Pay To name with a common word, first enter the Pay to name without the common word to see if there is a match. (Fraud list entries including the full Pay To name entered along with the common word will still flag a match.) Then, if a match is not found but these words are required on the check or disbursement Pay To line, back up and enter the full "Pay To" name with the common word.

Entry Recommendations:

- Enter the name in various formats to ensure a match to the Pay To name provided is not overlooked. The block list database entry can contain excess characters as long as it includes all characters in the same order as entered for the Pay To name.
- For companies whose Pay To name includes common words such as Incorporated or Company, it would be beneficial to create separate entries using different spellings of the common word (e.g., incorporated and inc., or company and co.). This also applies to individuals with nicknames (e.g., Nicholas and Nick, or Katelyn and Katie).
- If database entries created already include the shortened version within the long spelling, a separate entry using the short spelling is unnecessary as a Pay To name using the short version would still flag a match with the entry.

- For example, Pay To name Kate M would still flag a match with database entry Katelyn Member, and Pay To name ABC Co would still flag a match with database entry ABC Company.

Below are examples of block list entries and examples of which Pay To names will be blocked as a result of a suspected match. (These blocks can be overridden.)

Examples (Individuals)				
Block List Database Entry		***Pay To Name***		
First name	*Last name*	*First name*	*Last name*	*Warning?*
Tom	Members	Thomas	Members	No
		T	Members	Yes
		Tom	Member	Yes
		Tom	Memberson	No
		Tony	Member	No
		Freddie	Member	No
T	Sam	Tanya	Sam	No
		T	Samster	No
		J T	Sam	No
		T	S	Yes

Examples (Organizations)		
Block List Database Entry	***Pay To Name***	
Name	*Name*	*Warning?*
Joe Smith Company Inc.	J Smith Company	Yes
	John Smith Company	No
	Joe Smith Company	Yes
	Paul Inc.	No
	Company	No
	Joe Incorporated	No
	Joe Smith INC	Yes
	Note: Words like Inc., Incorporated, Company, and LLC are not recommended entries. See note above.	
Thomas Builder Supply	Thomas BuilderSupply	No
	Thomas	Yes

	Thomas Builder	Yes
	Thomas Builder Supply	Yes

J A Nanny	JA Nanny	No
	J. A. Nanny	No
	J A Nannys	No
	J A Nanny	Yes
	J Nan	Yes