Fraud Block Lists

Supplemental Guide

INTRODUCTION

Block Lists create a *centralized* place to see and stop activity based on patterns the credit union sees as risky or potentially fraudulent. In addition, by using an infrastructure independent from membership and other key data tables, Block Lists give us maximum flexibility to add and alter block list options, without a large ripple effect when we expand the lists.

CONTENTS

FRAUD LIST "IN A NUTSHELL" 2

- SINGLE CHANNEL DENIAL OF SERVICE BLOCK 2
- MULTI-CHANNEL TRANSACTION ATTRIBUTE BLOCKS 2

FREQUENTLY ASKED QUESTIONS 3

- GENERAL QUESTIONS ON FRAUD BLOCK LISTS 3
- QUESTIONS ON DENIAL OF SERVICE FRAUD BLOCK LISTS 4
- QUESTIONS ON TRANSACTION ATTRIBUTE FRAUD BLOCK LISTS 11

Revision date: January 13, 2021

For an updated copy of this booklet, check out the Reference Materials page of our website:
https://www.cuanswers.com/resources/doc/cubase-reference/

FRAUD LIST "IN A NUTSHELL"

You will find a centralized location for all Block Lists using **Tool #892** ***Update Fraud Alert/Blocked Persons List*** as the access. Here you will access all the new block lists and log member accounts where you've seen fraud in the past.

Your Auditors can access the Block List Database Inquiry from ***Tool #1892 View Fraud Alert/Blocked Persons List.***

SINGLE CHANNEL DENIAL OF SERVICE BLOCK

These fraud block lists simply stop a person or organization (by SSN) from enrolling or using a particular feature or service altogether.

- The new membership block list blocks a member from opening a new membership. It also blocks a credit union employee from creating a non member record for the person and from creating a pre-membership lending loan.

- Other denial of service block lists prevents an employee from enrolling a member and a member from enrolling in bill pay, Person to Person (P2P), or online/mobile banking. (All bill pay and P2P vendors are supported.) You may need to first unenroll the member from the service.

- Three additional block lists allow you to block a member from making incoming or outgoing wire transfers, and block a member from ordering an ATM, debit, or credit card.

- Additionally, the new lending block list presents a warning to loan officers when a loan application is submitted by one of the blocked members. (*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.)*

MULTI-CHANNEL TRANSACTION ATTRIBUTE BLOCKS

These fraud block lists are based on a particular data element and will stop specific transactions from occurring across various delivery channels.

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

- The **Pay To** block list prevents an account from posting an Accounts Payable Quick Check, miscellaneous credit union checks, checks issued by teller or Phone Operator, money orders, Loan disbursement checks, and wire transfers (outgoing only), whenever the Pay To name matches an item in the block list. (Unlike other blocks, this one includes an override function. If the Pay To name is not an exact match to the name in the block list, but the system detects a partial match to some of the characters, the user can view the list and perform an override if needed.)

FREQUENTLY ASKED QUESTIONS

GENERAL QUESTIONS ON FRAUD BLOCK LISTS

How do I access all the fraud block lists in CU*BASE?

Access all the fraud block lists by selecting **Tool #892** ***Update Fraud Alert/Blocked Persons List***. This will take you to the entry dashboard where you can see all the denial lists.

Can and should I add a person or organization to multiple block lists at the same time?

The system allows you to add the same person to multiple block lists. Access all the fraud block lists by selecting **Tool #892** ***Update Fraud Alert/Blocked Persons List***.

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 as many block lists as apply.

How do I remove a person or organization from a fraud block list?

To remove someone from any fraud block list, use **Tool #892 Update** ***Fraud Alert/Block Persons List***, then *Search Mbr/All Lists* to view the comprehensive listing of fraud lists and find where that member appears. Then return to the original Maintain Fraud Block Lists screens, select the appropriate list and then Edit. Use the Search fields at the top of the screen for the name you want to remove and select Delete. A confirmation window will appear prior to deleting the record.

- NOTE: Be sure to delete the person or organization from all appropriate lists. Each entry is deleted separately.

What can be denied with a "denial of service" or "transaction attribute" fraud block list?

The following services and transactions can be denied with a denial of service block list or transaction attribute block list. All lists are accessed from **Tool #892** ***Update Fraud Alert/Blocked Persons List***.

Denial of Service Block Lists

- 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)
- Membership (opening a new membership)
- Plastic orders (new and reorders)

Transaction Attribute Block Lists

- Pay to Name (being the "pay to" line when disbursing a teller check or money order, teller/phone check or money order, loan disbursement check, making an outgoing wire, creating an Accounts Payable Quick check and Miscellaneous CU check).
- Country (outgoing wires)

How can I tell if a member is on more than one fraud block list? For example, I may want to remove a membership from all block lists.

Use the Search fields at the top of the Block List Inquiry to filter the listing and view all service denial fraud block lists to which a person or organization has been added. You may do this if you wish to remove someone from all service denial fraud block lists.

To access the Block List Inquiry, use **Tool #892** ***Update Fraud Alert/Blocked Persons List*** and then *Search for Member/All Lists* (F10) or use **Tool #1892** ***View Fraud Alert/Blocked Persons List.*** This inquiry lists all the entries on all the service denial fraud block lists.

This Inquiry does not list the entries made on the transaction attribute block lists, however. A separate review of the transaction attribute fraud block lists will be needed to ensure that the member's name has not been added to that list. These lists can be viewed by using **Tool #892** ***Update Fraud Alert/Blocked Persons List*** and looking for lists described as transaction attribute list type.

Does the Fraud Block List Inquiry list the transaction attribute block list entries in addition to entries on service denial block lists?

To access the Fraud Block List Inquiry, use **Tool #892** ***Fraud Block Lists*** and then *Search for Member/All Lists* (F10) or use **Tool #1892** ***View Fraud Alert/Blocked Person List***. This inquiry lists all the entries on all the service denial fraud block lists. This Inquiry does not list the entries made on the transaction attribute block lists.

QUESTIONS ON DENIAL OF SERVICE FRAUD BLOCK LISTS

How is a denial of service fraud block list different than a transaction attribute fraud block list?

A denial of service block is a single service block that blocks a person or organization from enrolling in a service (such as bill pay) or performing a service (such as an outgoing wire transfer). A transaction attribute fraud block list allows the credit union to enter a data element that is used to determine if an activity should be blocked for any member (such as the "pay to name" when disbursing funds or the country when performing an outgoing wire).

What are the rules for making an entry on a denial of service fraud block list (that is not the new membership fraud list)?

The rules for adding an entry to any of the **denial of service** fraud block lists (other than new membership), require the SSN/TIN to be in MASTER/Membership file. If you enter the SSN/TIN and enter, the name will populate and the message displays, *SSN/TIN number found in Master file. Please verify name*. Verify the name to confirm and Update (F5). Or if you enter the name and enter, a warning message displays, *Name exists in Membership file. Check SSN/TIN #.* Verify the name and SSN/TIN to confirm and Update (F5).

How are the rules for making an entry on the new membership denial of service fraud block list different than the rules for the other service denial fraud block lists?

The rules for adding an entry to **new membership denial block list** are different than the rules for other service denial fraud lists.

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

Because of this, 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.

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. CU*TIP: If you have an actual, valid SSN, it is usually best to enter only that with no name, to avoid missing a match when a name happens to be spelled wrong or an alias is used.
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).

If this data is entered...	*This is what will be matched...*
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 denying a person or organization a **new membership** at your credit union.

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	No
	Thomas Home Care (entered in DBA field)	No
	Thomas Home	No
	Thomas Home Care	Yes
T F House	TF House	No
	T.F. House	No
	TF Housewares	No
	T F House	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

How does the new membership denial of service fraud block list work? Is the employee blocked from opening a new membership for the member? What happens when a match is made to an entry on the new membership denial of service fraud block list?

You can add an entry to the new membership fraud block list as an individual or organization. This fraud block list is different than other service denial lists in that it allows you to enter a name on the list without a Social Security Number.

- 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 person's list."

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.
- Opening an online membership via **Tool #13 *Work Online Banking Apps/Requests***.
- 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 all these 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 following options: to view the membership block list for any notes you may have added, to back up and enter a new name, to create a denial form, or to override the warning.

How does the bill pay denial of service fraud block list work? Is an employee blocked from enrolling a member in bill pay? Does the member see "Enroll in bill pay" online/mobile banking?

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 to enroll the member in bill pay (via Member Personal Banker (Tool #14) or during the membership open process), when the employee tries to check the "Enroll in bill pay" checkbox, they will see messaging that the "SSN/TIN appears on block list."

If a person or organization is added to the bill pay denial of service block list, and a membership with this SSN/TIN clicks "Enroll in bill pay" 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 SSN/TIN from the appropriate block list.)

If the member is already enrolled in bill pay, you will first need to unenroll them using CU*BASE (**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.

How does the Person to Person (P2P) denial of service fraud block list work? Is an employee blocked from enrolling a

member in P2P? Does the member see "Enroll in P2P" in online/mobile banking?

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 Member Personal Banker (Tool #14) or during the membership open process), when the employee tries to check the "Enroll in P2P" checkbox, they will see messaging that the "SSN/TIN appears on block list."

If the member is already enrolled in P2P, you will first need to unenroll them using CU*BASE (**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, and a membership with this SSN/TIN clicks "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.)

How does the online/mobile denial of service fraud block list work? Is an employee blocked from enrolling a member in online/mobile banking? Can the member log into online/mobile banking?

If a person or organization is added to the online/mobile denial of service block list, an employee cannot enroll any membership with this SSN/TIN into online banking via the Member Personal Banker, during the membership open process (for example via Tool #3), or directly via PIN shortcut. When they try to check the "Online Banking" checkbox on the Audio/Online Banking screen, they will see messaging that the "SSN/TIN appears on block list."

- Because of this, the member will not be able to login to online or mobile banking, unless the member has previously been given access and has logged in already.

- Being on the block list does not affect access made prior to the addition to the block list. If the member is already enrolled in online banking, the addition to the block list will not prevent the member from logging into that account *with the already created access points*. If a member on the block list has already logged into online banking, is subsequently added to the block list, and then tries to login using mobile banking (a new method of login they haven't used before), the member will be blocked from logging in via Mobile Banking.

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.)

If the member has already been granted access to online banking, you will first need to remove that access them by unchecking the "Online Banking check box on ARU/Online Banking Access" screen (which is also used for password resets). This screen is accessed via **Tool #14 *Member Personal Banker*** and the PIN shortcut. Then the block list will prevent this box from being rechecked. It will also prevent online banking access from being granted to another membership with the same SSN/TIN.

How does the lending denial of service fraud block list work? Is an employee blocked from creating a loan application or from opening a loan for a member? Can the member still submit an online loan application?

If a person or organization is added to lending denial of service 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 CU*BASE. If the loan officer makes it to the loan creation screen, they wil be blocked from opening the loan on that screen.

Additionally, for online loan applications, the loan officer will see messaging "On Fraud Block List" when working an incoming loan application using **Tool #2 *Work with Loan Request*** or **Tool #53 *Process Loan Applications***, then "Work with Existing Loan Request." Additionally, they will receive the messaging 'SSN/TIN appears on block list' when trying to create the loan.

If a membership is added to the lending denial of service block list, they will be able to apply for a loan online or via an indirect channel, but as covered previously, the loan officer will not be able to create their loan in CU*BASE.

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.)

How does the plastics denial of service fraud block list work? Is the employee blocked from opening an ATM, debit, or credit card for the member?

If an employee attempts to order an ATM, debit or credit card for a membership with a SSN/TIN that appears on the plastic orders denial of service block list, an employee cannot order the card. If the employee tries to order a card (via ***ATM/Debit Card Maintenance*** **(Tool #11)** or ***Update/Order Online Credit Cards*** **(Tool #12)**, during the membership open process), or when creating a credit card loan, or when adding an OTB credit cards (via Member Inquiry (F1), then OTB/Cards (F17)), 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 Plastic Orders block list.)

How does the outgoing wire denial of service fraud block list work? Is the employee blocked from creating an outgoing wire for the member?

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 select *Outgoing*," they will see messaging that the "SSN/TIN appears on block list."

You may consider also adding the member to the incoming wire fraud 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.)

How does the incoming wire denial of service fraud block list work? Is the employee blocked from creating an incoming wire for the member?

If a person or organization is added to the incoming 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 incoming wire via **Tool #73 *Post Wire Transfer to Member Account***, and select *Incoming*," they will see messaging that the "SSN/TIN appears on block list."

You may consider also adding the member to the outgoing wire fraud 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.)

What vendors are supported with the bill pay or P2P (person to person) denial of service fraud block list?

All bill pay vendors and P2P vendors are supported.

QUESTIONS ON TRANSACTION ATTRIBUTE FRAUD BLOCK LISTS

How is a denial of service fraud block list different than a transaction attribute fraud block list?

A denial of service block is a single service block that blocks a member from enrolling in a service (such as bill pay) or performing a service (such as an outgoing wire transfer). A transaction attribute fraud block list allows the credit union to enter a data element that is used to determine if an activity should be blocked for any member (such as the "pay to name" when disbursing funds or the country when performing an outgoing wire).

What rules should be followed when entering a name or organization to a "Pay to Name" transaction attribute fraud block list?

When making an entry on a transaction fraud block list, it is recommended to enter the name in various formats to supply a match to the attribute (such as pay to name) provided.

A match of any of the words in the Pay To entry, creates a match. The word must be the whole word and not a part of a word.

It is not recommended that you use words such as Company or Inc. in the name since all entries with those words would then be flagged.

When entering a pay to name with a common word, as mentioned above, first enter the Pay to name without the common word to see if there is a match. Then back up to enter if it is needed.

Below are examples of entries.

Examples (Individuals)

Database Entry		**Actual Member Name**		
First name	*Last name*	*First name*	*Last name*	*Warning?*
Tom	Members	Thomas	Members	Yes
		T	Members	Yes
		T	Memberson	No
		Tom	Memberson	No
		Tony	Member	Yes
		Freddie	Member	No
T	Sam	Tanya	Sam	Yes
		T	Samster	No
		J T	Sam	No

Examples (Organizations)

Database Entry	**Actual Member Name**	
Name	*Name*	*Warning?*
Joe Smith Company Inc.	J Smith Company	Yes
	John Smith Company	Yes
	Joe Smith Company	Yes
	Paul Inc.	Yes
	Company	Yes
	Joe Incorporated	No
	Note: Words like Inc., Incorporated, Company, and LLC are not recommended. See note above.	
Thomas Builder Supply	Thomas BuilderSupply	No
	Thomas	Yes
	Thomas Builder Supply (entered in DBA field)	No
	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

My "pay to" name that I am running against a fraud list has a common word, for example LLC, Co., Inc., Incorporated, or Company. What should I enter in the Pay to line?

The Pay to fraud block list allows for these words to be entered in an entry, but it is not recommended since every entry with these words will be a match. For this reason, it is recommended that you first enter the "Pay to" name without these words to see if you receive a match on the fraud list. Then if a match is not found but these words are required on the check or disbursement Pay to line, then back up and enter the full pay to name with the common word.

What rules should be followed when entering a country name to a "country" transaction attribute fraud block list?

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

An exact match 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.

What happens when a match or partial match is found to an entry on a pay to name or country denial fraud block list?

When the pay to name or country 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, is it recommended that the employee follow credit union policies and procedures. From the "Suspected match was found" window, the employee has the following options: 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 or country from the appropriate block list.)

How does the "pay to name" transaction attribute fraud block list work? What kind of disbursements is the employee blocked from issuing if a match is found on this list? What other special caveats are there for this type of transaction attribute block?

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 - *Check* (C)
- Loan disbursements (**Tool #50 *Disburse Member Loan Funds***)

- AP Quick Checks (**Tool #1961 *AP3: Process Accounts Payable Payments***, then Create Check (F6)). The messaging will appear when the vendor is selected.
- Miscellaneous expense checks (**Tool #667 *Print Miscellaneous Checks***)

The employee is then presented a window alerting them if "no match was found" or if "a suspected match was found."

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

How does the "country" transaction attribute fraud block list work? What kind of activity is the employee blocked from issuing if a match is found on this list?

The county attribute fraud block list is used when an employee makes an outgoing wire. If a match is found the employee will move to a window alerting them that a suspected match was found.

It is recommended that the employee follow credit union policies and procedures. The member can back up, view the block fraud list for comments, or override the block.