Reference Guide

AuditLink

Abnormal Activity Monitoring

Transaction Patterns, Member Groups, and Stop-No-Go Patterns

INSIDE THIS GUIDE:

This guide describes the abnormal activity monitoring toolset, which automatically sifts through member transactions to flag those that are abnormal or high risk according to the parameters set by your credit union. Learn about the process of configuring and monitoring abnormal activity by member groups, transaction patterns, and stop-no-go patterns.

Last Revision date: November 5, 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

There are three main configuration options within the abnormal activity monitoring toolset: member groups, transaction patterns, and stop-no-go patterns. You can configure each option to run simultaneously to monitor different aspects of your member transactions.

Member groups compare individual member activity against norms for the entire membership group.

Transaction patterns allow you to run three different series of patterns to flag abnormal member transaction activity by comparing to the member's norms.

Stop-no-go patterns review incoming transactions against the configured thresholds to stop transactions before they post to the member account.

FFIEC guidance urges financial institutions to perform this abnormal activity monitoring but proving that it is being done is even more critical. By incorporating the use of other CBX features such as the Member Tracker System and Due Diligence Codes, your credit union can document and evidence the review of suspicious activity—all within the system.

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*

Configuring Abnormal Activity Settings

Learn how to configure abnormal activity settings for member groups, transaction patterns, and stop-no-go patterns using **Tool #101 *Abnormal Activity Monitoring Config***.

> *IMPORTANT NOTE ABOUT WHAT THE TOOL IS **NOT** DESIGNED FOR: Use of the abnormal activity monitoring tool is **not** intended to replace monitoring of accounts that are already known to the credit union. The purpose of the tool is to uncover new suspicious activity.*

Configuring Member Group Abnormal Activity Settings

Learn how to define abnormal activity for member groups.

Before You Begin

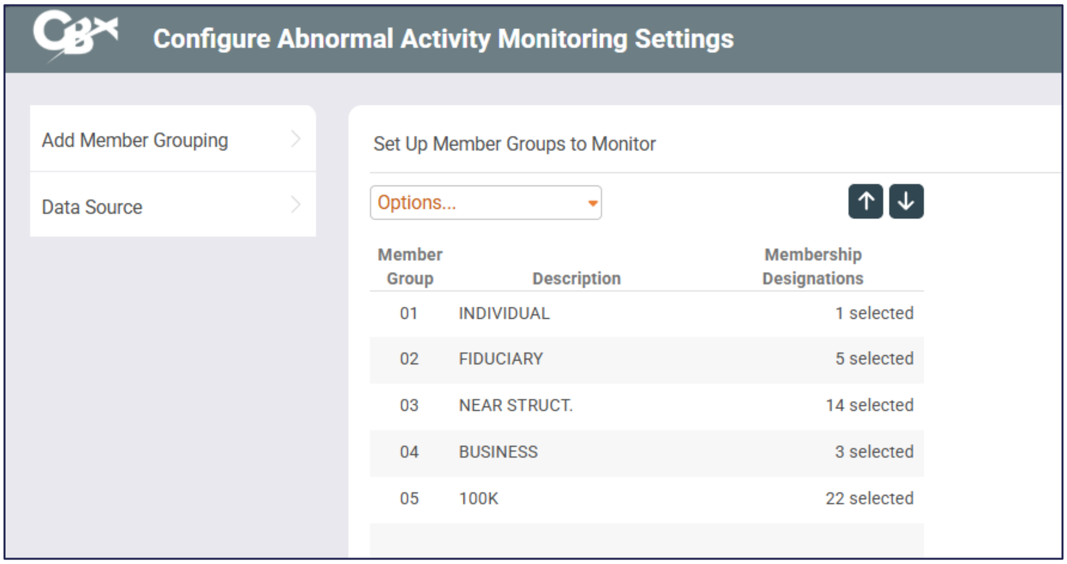
To configure abnormal activity criteria for member groups, first you'll need to categorize your members into specific groups by membership designations with similar patterns of activity. Individual and organizational accounts should be grouped accordingly. Then, you'll define the transaction criteria deemed abnormal.

1. Based on the composition of your membership, determine which member designations need to be added to a member group. The following member groups are recommended (as applicable): Individual, Business, and Fiduciary. (See page 4.)
2. Determine which types of transactions (origins) you would like to monitor for each member group. (See page 6.)
    - Additional origin codes can be added at your discretion, but at a minimum, the following origins should be setup for each member group: ACH, ATM, Debit Card, Credit Card (if online), Audio Response, and Wire Transfers.
3. Determine the ranges (number of transactions and dollar amount) you would consider normal and abnormal activity. (See page 9.)

Setting Up Member Groups

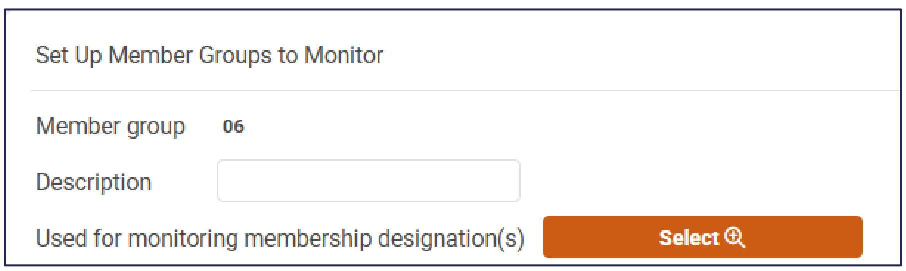
To set up member groups, access **Tool #101 *Abnormal Activity Monitoring Config***. Select to configure *Member Groups (compare members to norms for the group)*.

Configure Abnormal Activity Monitoring Settings (Tool #101 > Member Groups)



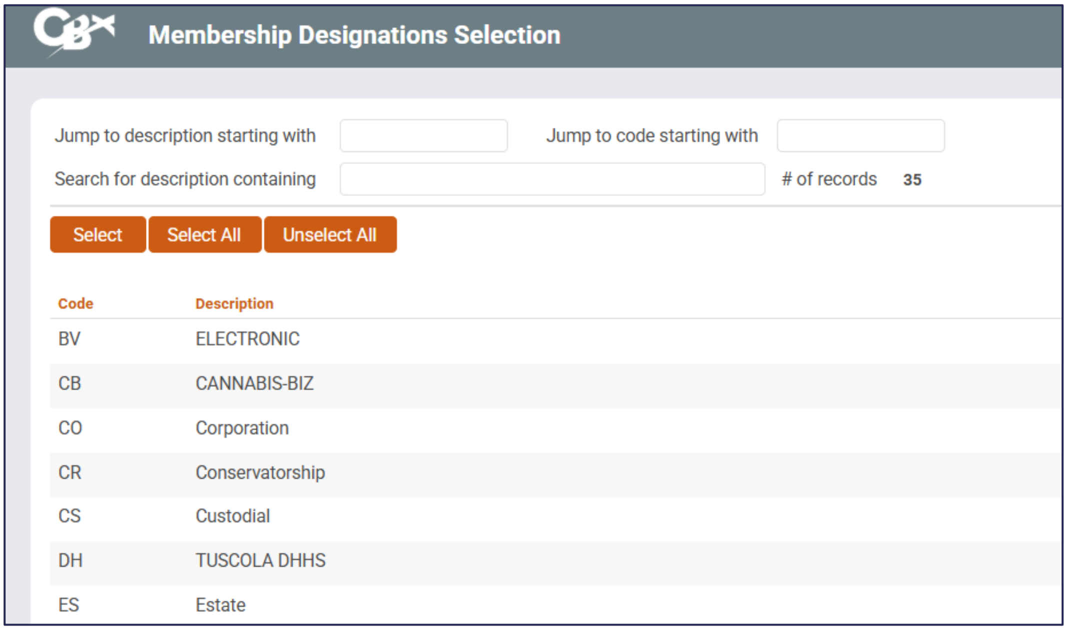
1. Select **Add Member Grouping**.
2. In the *Description* field, enter the name you would like to give the group.
   - For example, if you'd like to monitor memberships that have a fiduciary obligation such as members who are managing an account for someone who is elderly, disabled, or a minor, then you might enter a description of "Fiduciary."

Configure Abnormal Activity Monitoring Settings (Tool #101 > Member Groups > Add Member Grouping)



   - The *Member group* number is automatically assigned by CBX and represents the number of member groups set up for your credit union. If a member group is deleted, CBX will reuse the old number, and the next member group created will be assigned that old number.
3. Use **Select** next to the Used for monitoring membership designation(s) field.
   - The groups should be set up to include membership designations that have similar patterns of activity. For example, you wouldn't want to put both organizational and individual accounts in one member group because the transaction numbers for organizational accounts will typically be much higher than those for individual accounts.

Membership Designations Selection (Tool #101 > Member Groups > Add Member Grouping > Select)



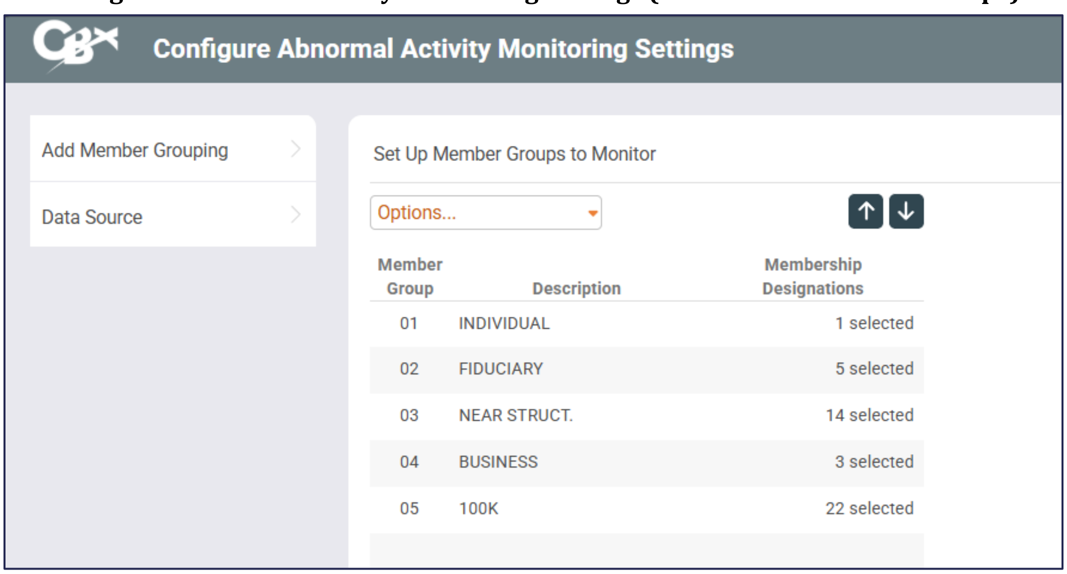
In order to be as efficient as possible when monitoring members, a best practice is to avoid including the same Membership Designation Code in more than one group. This ensures you do not monitor the same member more than once.

Adding Origin Groups

After you have set up the member groups, you can now add origin types.

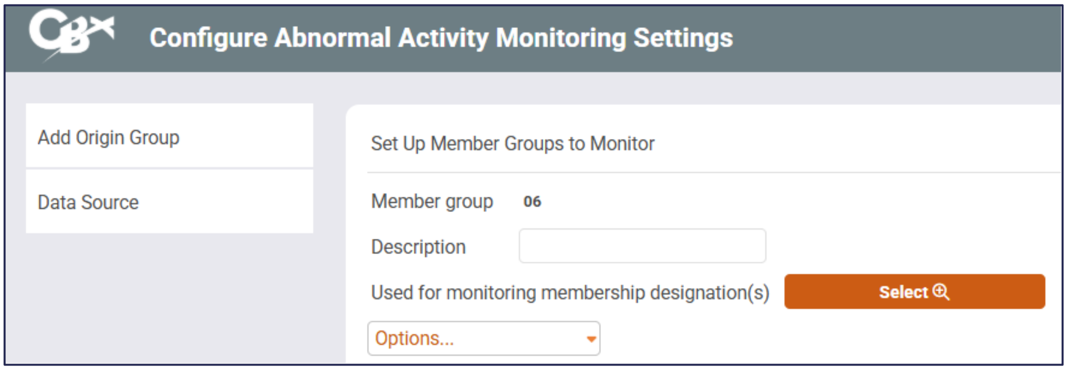
1. Double-click on the member group (or select the group and the *Edit* option).

Configure Abnormal Activity Monitoring Settings (Tool #101 > Member Groups)



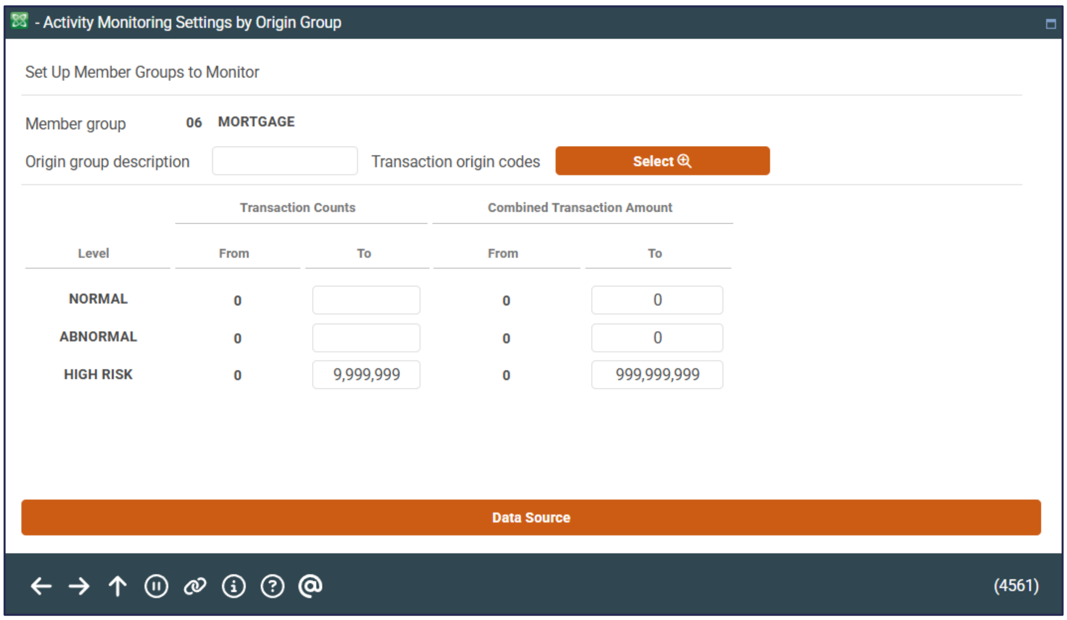
2. Select **Add Origin Group** to select the origin (transaction type) you would like to monitor.

Configure Abnormal Activity Monitoring Settings (Tool #101 > Member Groups > Add Member Grouping)



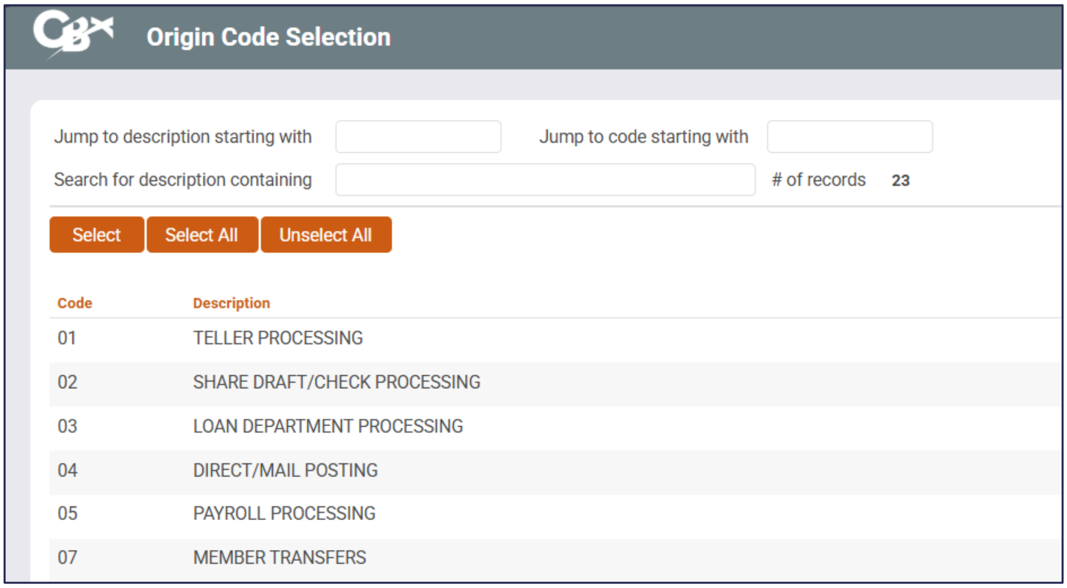
3. Use the **Select** button next to the *Transaction origin codes* field.

Tool #101 > Member Groups > Add Member Grouping > Add Origin Group



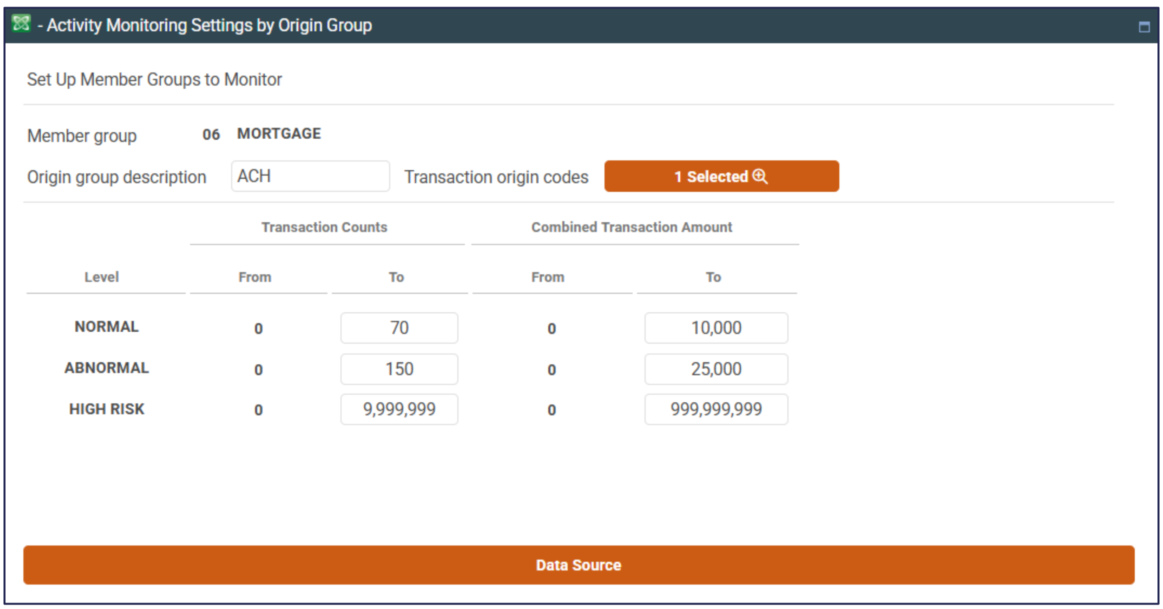
4. **Select** the origin code(s) (transaction type). It is recommended that you set up the same origins for each member group that you create.

Tool #101 > Member Groups > Add Member Grouping > Add Origin Group > Select



5. In the *Origin group description* field, enter a description for your origin group.

Tool #101 > Member Groups > Add Member Grouping > Add Origin Group

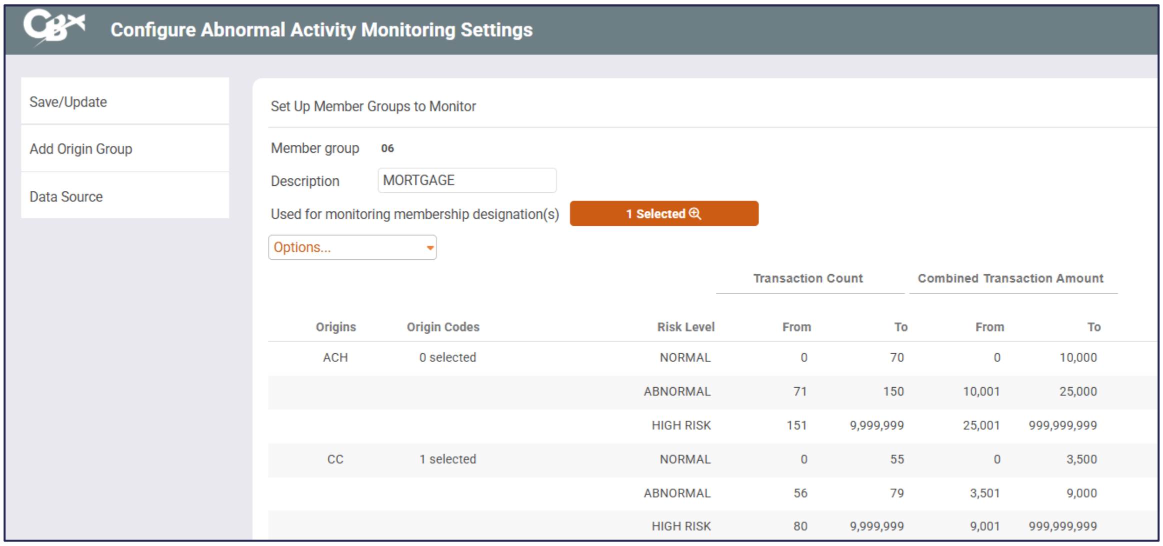


6. In the *To* fields under the Transaction Counts heading, enter the highest number of transactions that your credit union considers to be normal, abnormal, and high-risk.

7. In the *To* fields under the Combined Transaction Amount heading, enter the highest dollar amount of transactions that your credit union considers to be normal, abnormal, and high-risk for the type of membership(s) and transaction(s) you're planning to monitor.

8. Use Enter to save your changes.

Configure Abnormal Activity Monitoring Settings (Tool #101 > Member Groups > Add Member Grouping)



Origins	Origin Codes	Risk Level	Transaction Count From	Transaction Count To	Combined Transaction Amount From	Combined Transaction Amount To
ACH	0 selected	NORMAL	0	70	0	10,000
		ABNORMAL	71	150	10,001	25,000
		HIGH RISK	151	9,999,999	25,001	999,999,999
CC	1 selected	NORMAL	0	55	0	3,500
		ABNORMAL	56	79	3,501	9,000
		HIGH RISK	80	9,999,999	9,001	999,999,999

9. Add the rest of your origin groups by again selecting **Add Origin Group**. If you are satisfied with your configuration settings, click **Save/Update**.

Determining Accurate Transaction Ranges

For assistance in figuring out the transaction ranges that your credit union considers “normal,” “abnormal,” and “high-risk,”, refer to the Sample/Comparison Dashboard outlined below.

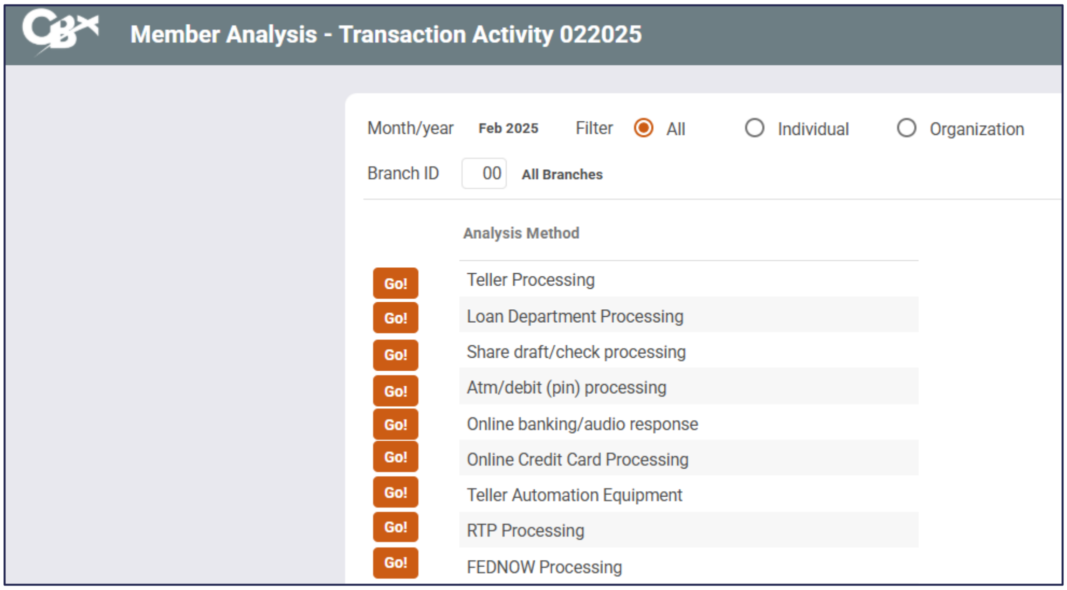
- When considering transaction numbers for a normal range, keep in mind that the Combined Transaction Amount fields count all debits and credits together. For example, a credit of $100 and a debit of $100 will equal two transactions and $200 of money moved.
- Also keep in mind that different membership types will have different amounts, and for this reason, the norms must be set up differently. For example, organizational accounts typically deposit significantly more checks than individual members do.
- Figuring out your ranges may require multiple adjustments. As you begin using the monitoring tool, you will learn more about how many "hits" you get. With this information, you may need to either narrow to minimize false positives or expand to catch a broader range of activity.

Sampling/Comparison Dashboard

A useful tool in helping you determine transaction ranges is the Transaction Activity Summary Compare sampling dashboard.

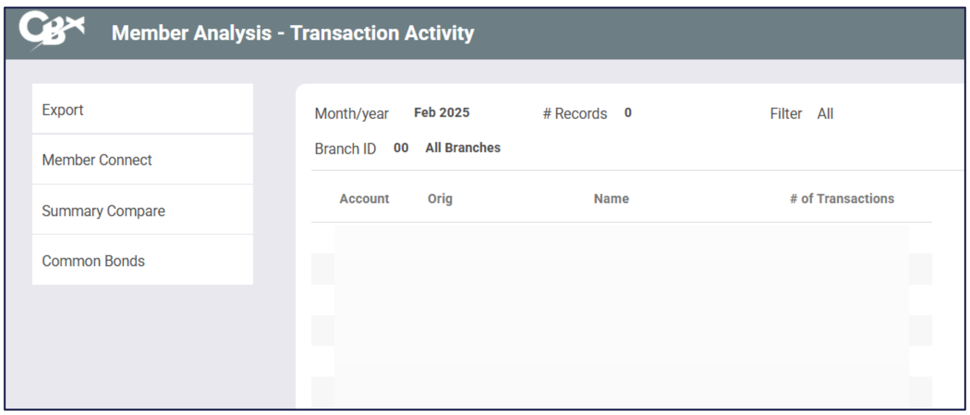
1. To access this dashboard, use **Tool #775 *Sample Transactions by Delivery Channel***.

Member Analysis – Transaction Activity (Tool #775)



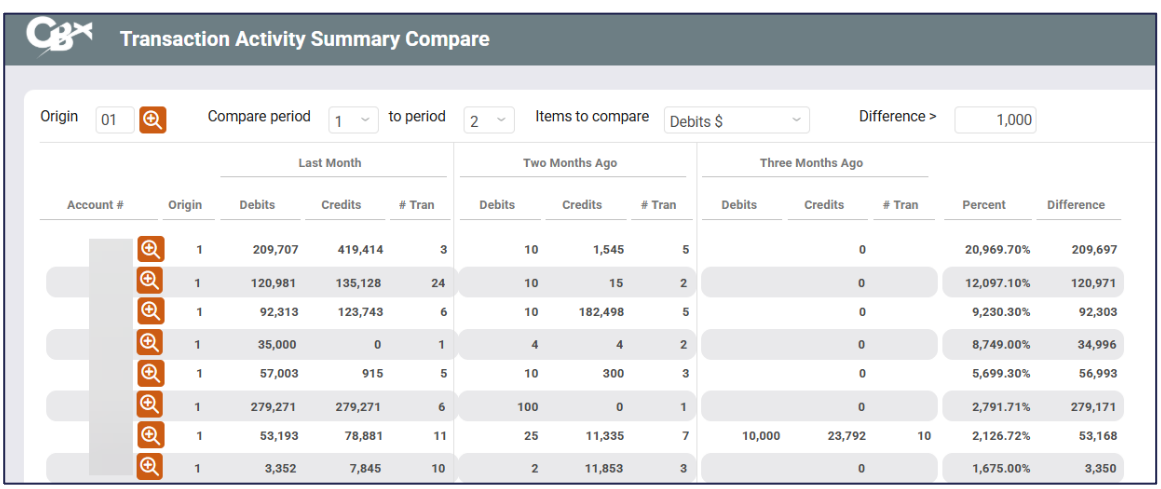
2. Drill down by origin code to see the number of transactions by member during the previous month by selecting **Go!** next to the origin.

Member Analysis – Transaction Activity (Tool #775 > Go!)



3. Select **Summary Compare**. You will then be brought to the Transaction Activity Summary Compare dashboard shown below. This screen provides a range of transactions by dollar amounts.

Transaction Activity Summary Compare (Tool #775 > Go! > Summary Compare)



		Last Month			Two Months Ago			Three Months Ago				
Account #	Origin	Debits	Credits	# Tran	Debits	Credits	# Tran	Debits	Credits	# Tran	Percent	Difference
	1	209,707	419,414	3	10	1,545	5		0		20,969.70%	209,697
	1	120,981	135,128	24	10	15	2		0		12,097.10%	120,971
	1	92,313	123,743	6	10	182,498	5		0		9,230.30%	92,303
	1	35,000	0	1	4	4	2		0		8,749.00%	34,996
	1	57,003	915	5	10	300	3		0		5,699.30%	56,993
	1	279,271	279,271	6	100	0	1		0		2,791.71%	279,171
	1	53,193	78,881	11	25	11,335	7	10,000	23,792	10	2,126.72%	53,168
	1	3,352	7,845	10	2	11,853	3		0		1,675.00%	3,350

Configuring Abnormal Activity Transaction Patterns

Abnormal activity monitoring groups and patterns are configured via **Tool #101 *Abnormal Activity Monitoring Config***. With transaction patterns, transaction activity is compared to the norms for the individual member. Dependent on the pattern type, these patterns can flag activity that appears excessive in transaction amount or quantity, occurs after a period of inactivity, or appears as an unusually higher transaction amount or count for that member. Monitoring transaction patterns can help identify potentially compromised accounts as well as other threat vectors.

Pattern Types

There are with three pattern type options to choose from: velocity, idle activity, and out-of-the-ordinary. Each pattern type presents a unique opportunity to trigger alerts based on different forms of transaction activity.

Velocity Triggers

The velocity trigger will flag accounts which surpass the defined number of transactions and/or total daily transaction amount ($) within the defined period. These triggers can be particularly helpful for monitoring daily activity.

Scenarios where velocity triggers are helpful for identifying:

- Accounts with an excessive number of transactions per day/week/month
- Accounts with an excessive total daily transaction amount per day/week/month
- Potential account takeovers
- Check kiting
- High-risk gambling activity

Idle Activity Triggers

The idle activity trigger will flag accounts which surpass a defined number of transactions and/or total daily transaction amount ($) following a defined period of inactivity.

Scenarios where idle activity triggers are helpful for identifying:

- Sudden resurgence of activity in inactive accounts
- Account takeovers
- Check kiting
- Elderly exploitation

Out-of-the-Ordinary Triggers

The out-of-the-ordinary trigger will flag accounts which surpass the defined minimum percentage increase in the average number of transactions and/or average daily transaction amount.

Unlike the other triggers which compare transaction activity to fixed numbers, out-of-the-ordinary triggers flag accounts whose transactions surpass the calculated member average by a defined percentage.

Sometimes, a member's transaction activity might not meet your configured velocity threshold to be flagged as abnormal; however, that does not mean it is normal activity for that member. Out-of-the-ordinary triggers allow you to compare transaction activity directly against the member's averages to identify significant increases in behavior.

Scenarios where out-of-the-ordinary triggers are helpful:

- Comparing transaction activity against the norms for the member
- Recognizing abnormal activity in accounts with little activity
- Identifying potential account takeovers
- Detecting elderly exploitation
- Identifying money mules

With out-of-the-ordinary triggers, pay attention to the calculation method chosen for calculating the average daily transaction amount (i.e., dividing by the number or days or the number of transactions within the defined period). The calculation method chosen will affect the thresholds you configure. (You will likely need higher thresholds when calculating the average based on the number of days.)

Pre-Configured Patterns

When you first access **Tool #101,** you may notice that AuditLink has already uploaded several pre-configured patterns to your library. Please note that some of these pre-configured patterns may not be useful for your credit union, and the majority of these patterns will need to be adjusted according to your credit union's unique dataset.

Default Configuration Adjustments

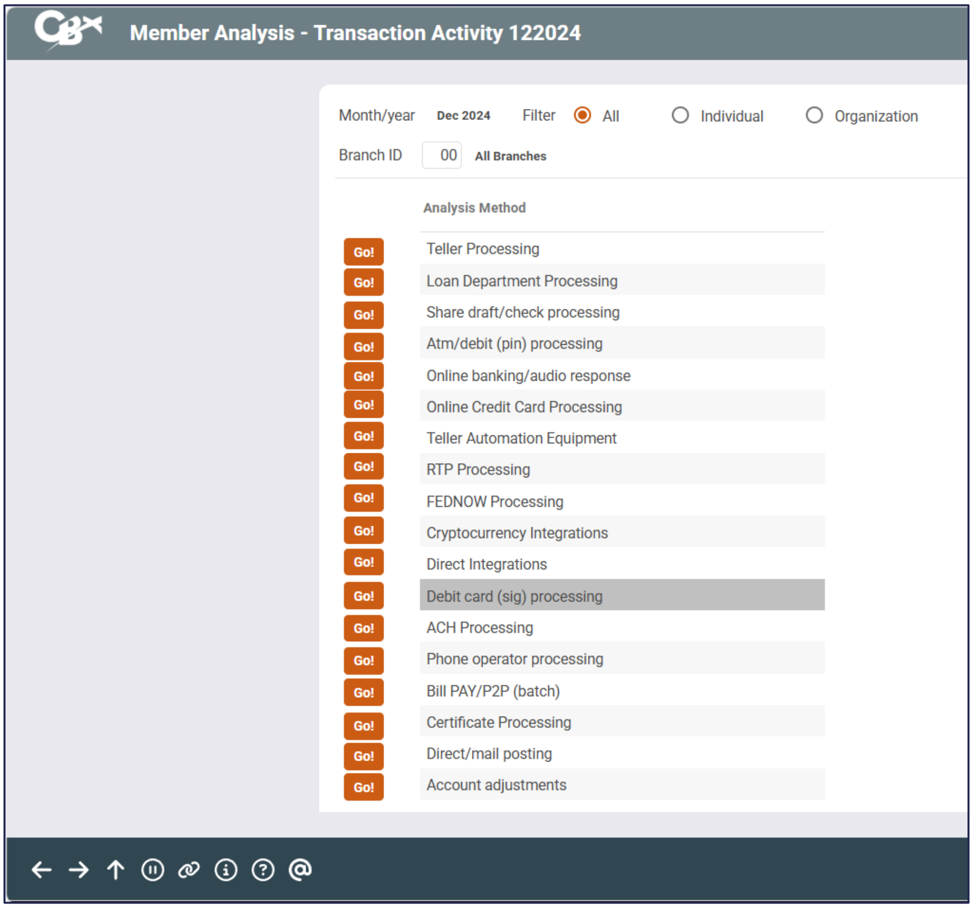
Every credit union has a different membership composition, risk profile, and complexity level.

The first step is to adjust the default pattern configurations to better align with the transaction behavior of members specific to your credit union.

Configuration Starting Point

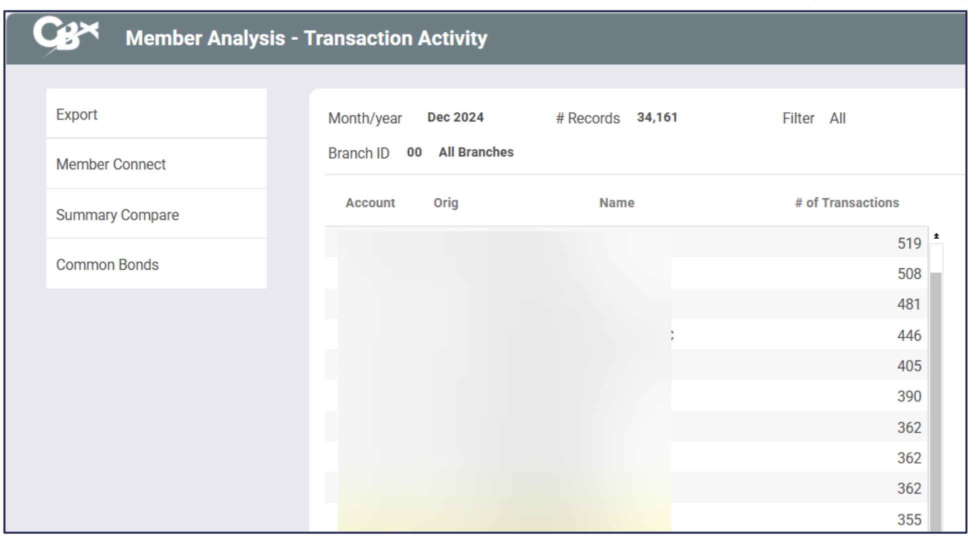
Determine a starting point for adjusting each of the 30 patterns by using **Tool #775 *Sample Transactions by Delivery Channel***. This will assist you in establishing average activity levels on which to base pattern thresholds.

Member Analysis – Transaction Activity (Tool #775)



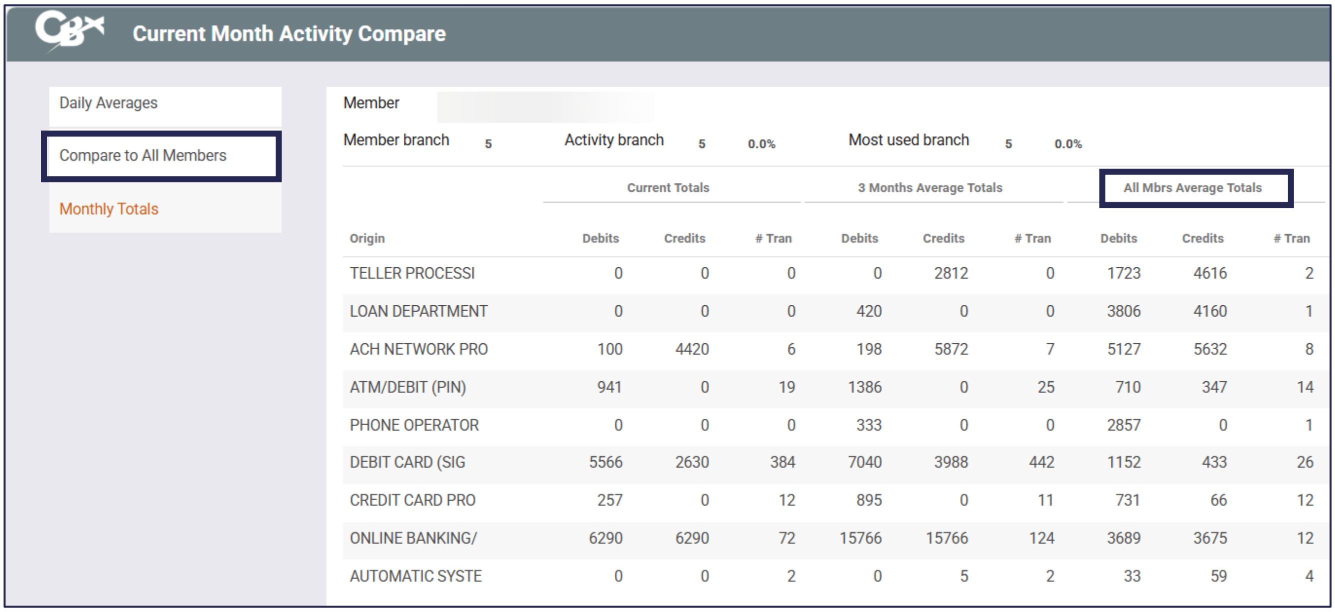
For example, the graphic below shows the highest number of debit card transactions for any member was 519 during the month of December. That breaks down to about 16.7 debit card transactions per day.

Member Analysis – Transaction Activity (Tool #775 > Debit card (sig) processing)



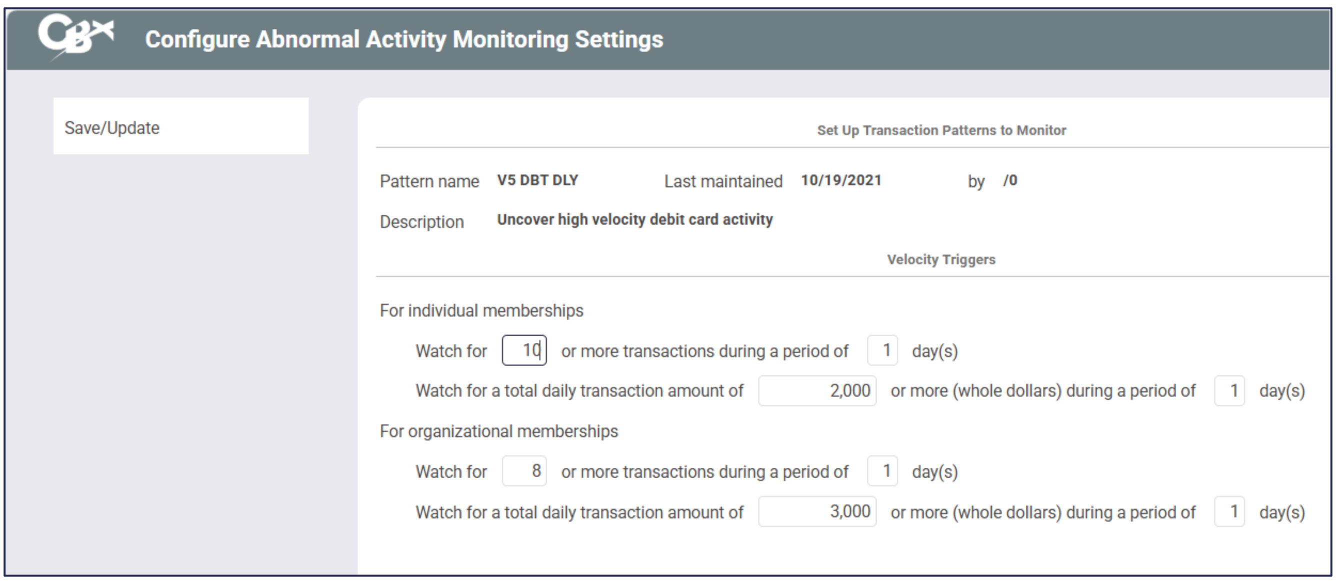
You will need to dig a little deeper to learn more about average transaction amounts. Note the account number of the member with the highest number of transactions. Search this account in member inquiry, select the Participation/Products tab, and select **Transaction Activity**. The dashboard shows the member's activity over the past three months. Select **Compare to All Members**. The All Mbrs Average Totals column displays each origin's average amount/number of transactions for all memberships.

Current Month Activity Compare (Inquiry > Participation/Products > Transaction Activity)



Use these statistics to determine how to set the number of transactions to watch for in the configuration settings. Below, we show an example of a velocity trigger pattern, setting the threshold for the number of transactions slightly higher than the average we calculated for the member with the most transactions.

Configure Abnormal Activity Monitoring Settings – Transaction Patterns (Tool #101)



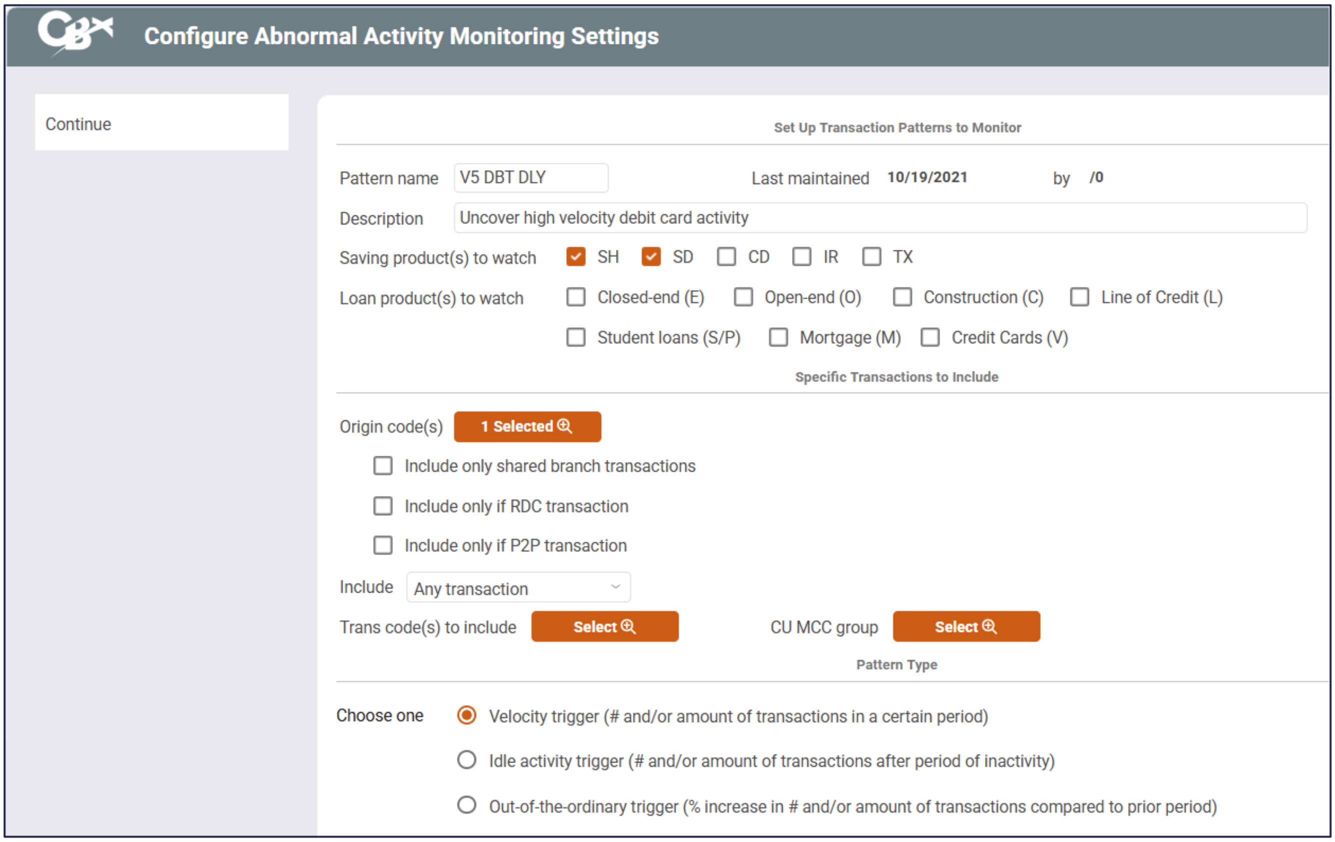
Setting Up New Transaction Patterns

To set up transaction patterns from scratch, follow the directions below.

1. Launch **Tool #101 *Abnormal Activity Monitoring Config*** and select *Transaction Patterns (compare members to norms for that member)*.

2. Select **Add Pattern**.

Configure Abnormal Activity Monitoring Settings – Transaction Patterns (Tool #101)



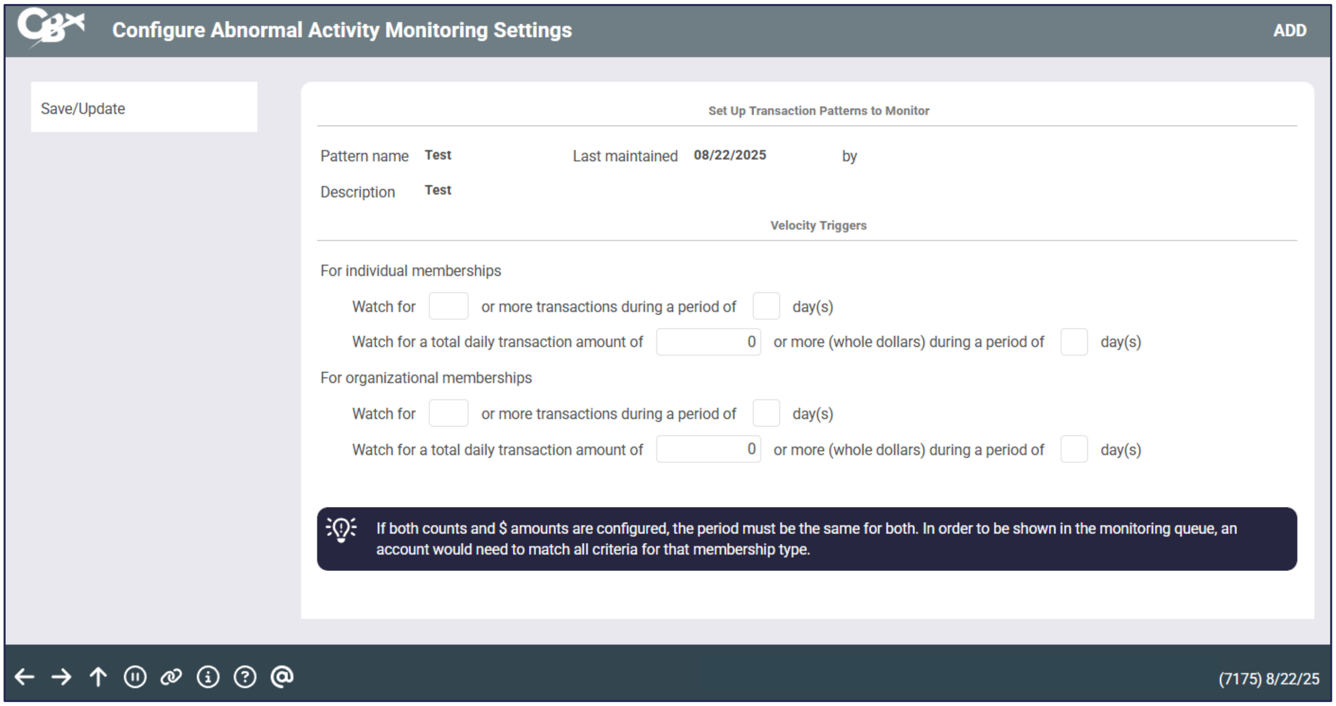
3. Input a *Pattern name* and *Description*.
   - We recommend inputting a descriptive pattern name since these appear within the monitoring dashboard.
4. Select the Saving/Loan product(s) to watch for this pattern.
5. You then have options to filter the pattern to monitor only specific types of transactions.
   - You can limit the pattern to monitor only P2P, RDC, or shared branch transactions. (You cannot check multiple boxes.)
   - You can filter the pattern to monitor only specific origin code(s). (When monitoring only P2P, RDC, or shared branch transactions, you cannot filter by specific origin codes.)
   - You can select to monitor withdrawals only, deposits only, or specific transaction codes. (In order to select specific transaction codes, you must set the *Include* field to *Select by trans code*.)
   - With the last filter option, you can monitor only transactions with specific merchant category codes (MCC). (You will need to set up the MCC monitoring groups separately via **Tool #1024 *Configure Credit Union MCC Groups***.)
6. At this point, choose which pattern type (velocity, idle, or out-of-the-ordinary) to configure.

Velocity Trigger

Velocity patterns are helpful for identifying an excessive number or amount of transactions over a configured period of time.

After selecting Velocity trigger as the Pattern Type and selecting **Continue**, you will be brought to the configuration detail screen shown below. Configure the trigger to flag accounts which surpass the defined number of transactions and/or total daily transaction amount ($) within the defined period.

Tool #537 > Transaction Patterns > Add Pattern > Velocity Trigger

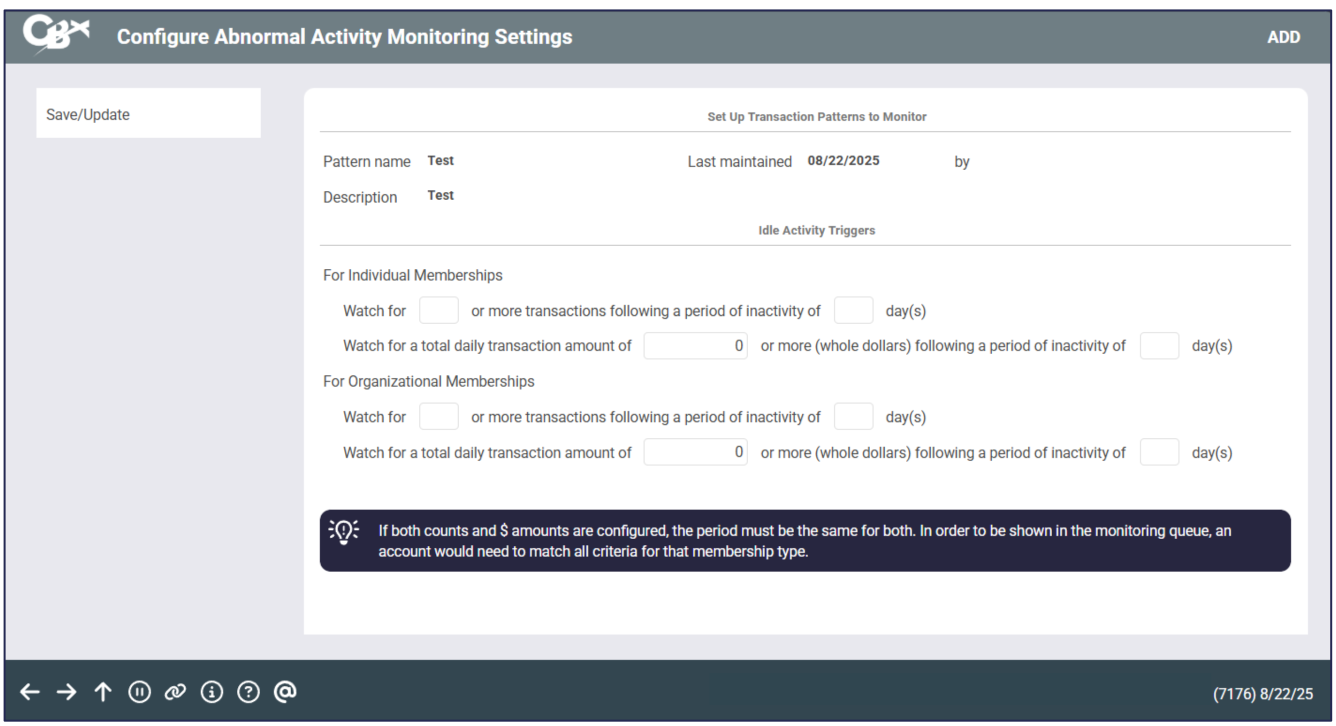


Idle Activity Trigger

Idle activity patterns flag accounts with abnormally high transaction activity after a period of inactivity.

After selecting Idle activity trigger as the Pattern Type and selecting **Continue**, you will be brought to the configuration detail screen shown below. Configure the trigger to flag accounts which surpass a defined number of transactions and/or total daily transaction amount ($) following a defined period of inactivity.

Tool #537 > Transaction Patterns > Add Pattern > Idle Activity Trigger

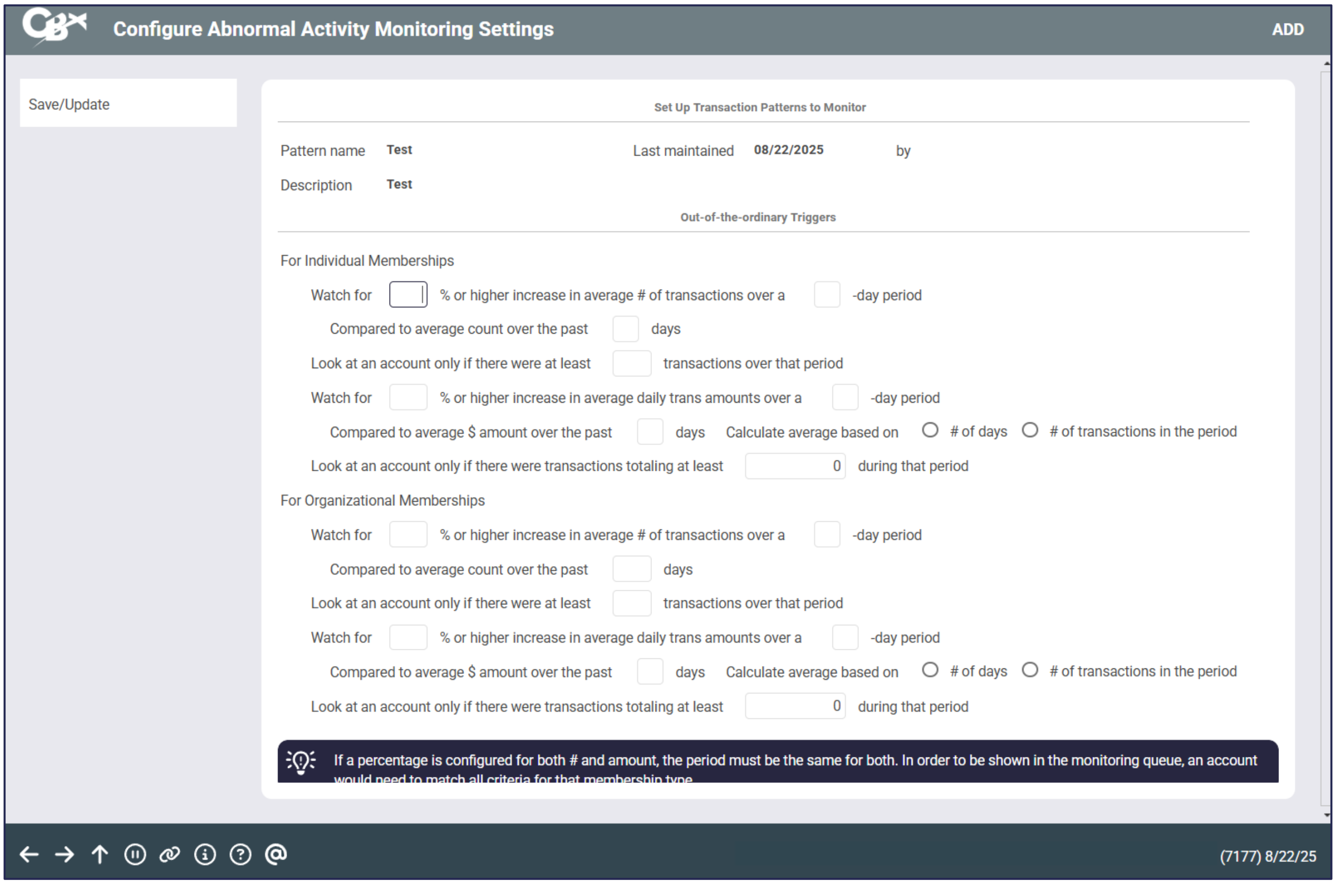


Out-of-the-Ordinary Trigger

Out-of-the-ordinary patterns are useful for identifying abnormal increases in transaction activity over a period of time.

After selecting Idle activity trigger as the Pattern Type and selecting **Continue**, you will be brought to the configuration detail screen shown below. Configure the trigger to flag accounts which surpass the defined minimum percentage increase in the average number of transactions and/or average daily transaction amount.

Tool #537 > Transaction Patterns > Add Pattern > Out-of-the-Ordinary Trigger



Pattern Configuration Test Run

Use the *Run a test* option in **Tool #101 *Abnormal Activity Monitoring Config*** to test how the changes you made affect the accounts that populate the dashboard.

Configure Abnormal Activity Monitoring Settings (Tool #101)

After running a test, you may select to *Edit* a pattern to change the configured parameters to better represent abnormal activity for your credit union.

Repeat this process until you are comfortable you have a reasonable review population for each pattern.

Configuration Tracking Template

For each applicable pattern, document the existing configuration prior to making adjustments. Maintaining a record of changes provides written support for when and why a pattern configuration was changed. It also enables the credit union to revert back to a prior configuration if necessary.

> ***IMPORTANT NOTE:*** *It is not necessary to document the default configuration; in many instances, they are wide open casting a broad net. This process is intended to record the initial and subsequent manual adjustments to the configuration.*

The **Configuration Tracking Template** is used to document the existing configuration and any subsequent changes made to the configuration.

Configuration Tracking Template

ABC Credit Union										
	Changed by	Pattern	Origin Code(s)	Description		Initial Configuration Date				Date of Change
1		I1 SB #	n/a	Idle account activity for shared branching	60 days	Enter the number of accounts returned	1	or more transactions following a period of inactivity	120 days	
					60 days		$ 1,000.00	or more following a period of inactivity of	120 days	
					60 days		1	or more transactions following a period of inactivity	120 days	
					60 days		$ 1,000.00	or more following a period of inactivity of	120 days	
2		I2 RDC #	4	Idle account activity for RDC transactions	60 days		2	or more transactions following a period of inactivity	60 days	
					60 days		$ 250.00	or more following a period of inactivity of	60 days	
					60 days		2	or more transactions following a period of inactivity	60 days	
					60 days		$750	or more following a period of inactivity of	60 days	
3		I3 ATMPOS#	13	Idle account activity ATM/POS	90 days		2	or more transactions following a period of inactivity	90 days	
					90 days		$ 500.00	or more following a period of inactivity of	90 days	
					90 days		2	or more transactions following a period of inactivity	90 days	
					90 days		$ 500.00	or more following a period of inactivity of	90 days	
4		I4 P2P #	11	Idle activity on P2P transactions	60 days		2	or more transactions following a period of inactivity	90 days	
					60 days		$ 500.00	or more following a period of inactivity of	90 days	
					60 days		2	or more transactions following a period of inactivity	90 days	
					60 days		$ 500.00	or more following a period of inactivity of	90 days	
5		I5 Debit #	16	Idle activity on debit card	30 days		2	or more transactions following a period of inactivity	60 days	
					30 days		$ 500.00	or more following a period of inactivity of	60 days	
					30 days		2	or more transactions following a period of inactivity	60 days	
					30 days		$ 500.00	or more following a period of inactivity of	60 days	

(To access the templates mentioned in this booklet, *place a FREE store order*.)

Configuring Abnormal Activity Stop-No-Go Patterns

The hard-coded Stop-No-Go ACH Deposit pattern can be adjusted to define your acceptable limits for the automated posting of ACH deposits. When the configured thresholds are met, any additional ACH deposits that day for that member will be sent to your exceptions for review, with a reason code of ABNL, allowing you to look for name mismatches, nature and purpose of the account, etc. From there, you can elect to manually post or return the ACH items.

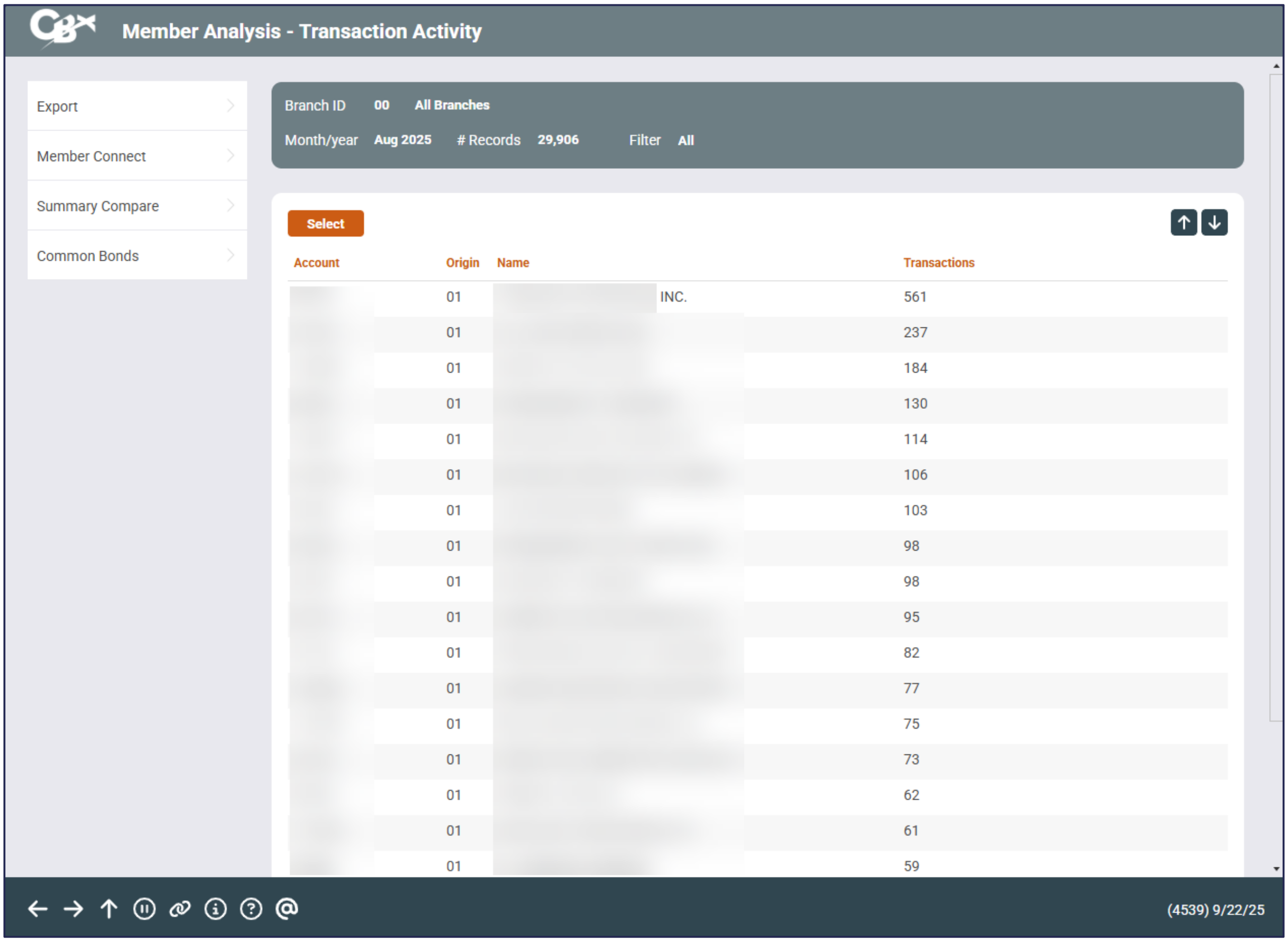
Before you begin configuring ACH stop-no-go patterns, be sure to consider that ACH items exceeding configured thresholds will go into your ACH exceptions. These exceptions will need to be worked by your internal teams. Prior to activating this feature, it is important to consider your thresholds and the impact they may have on back-office teams that are tasked with working ACH exceptions.

Determining Accurate Transaction Ranges

Before configuring the pattern, you'll want to know appropriate ranges for what your credit union considers abnormal ACH activity.

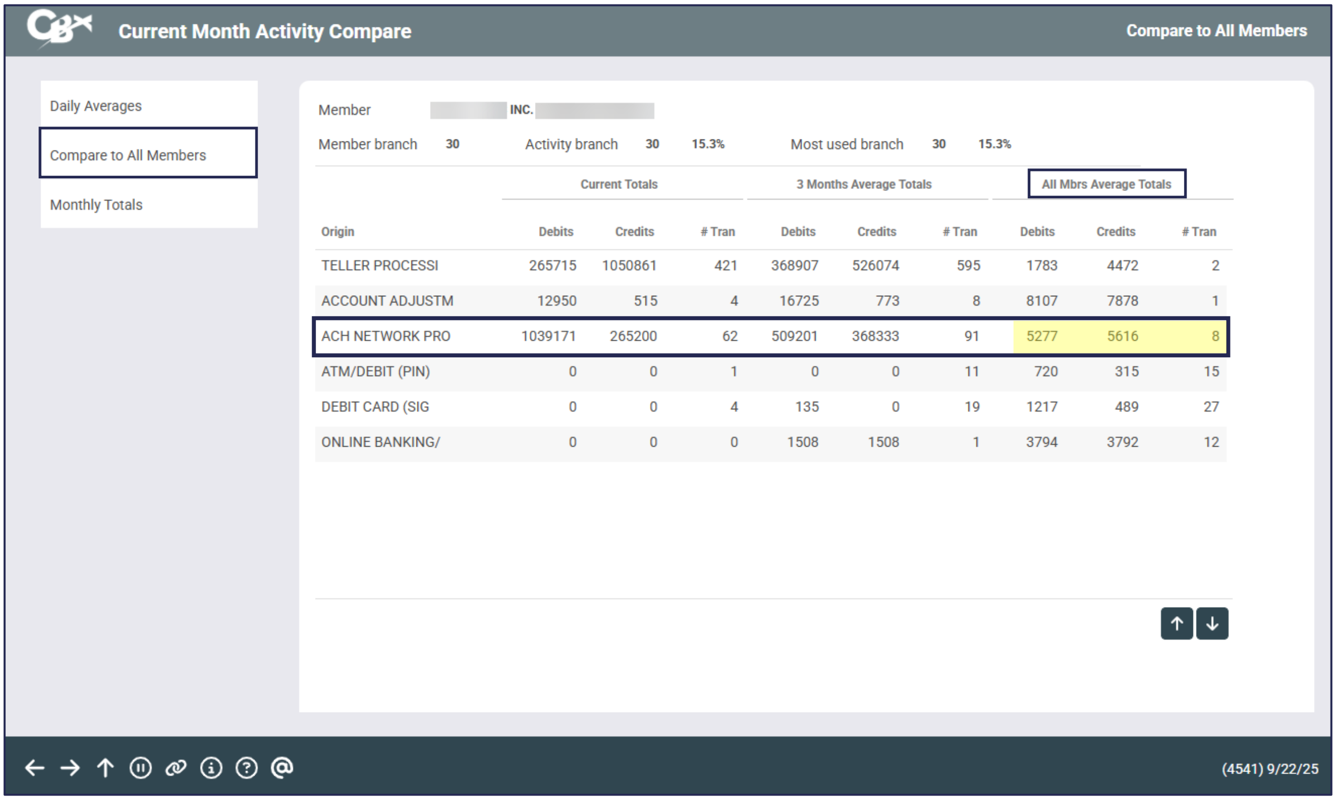
Launch **Tool #775 *Sample Transactions by Delivery Channel*** and select ACH Processing. You'll be able to see which accounts had the highest transaction activity that month. This will give you an idea of the average transaction numbers, but you will need to dig a little deeper to learn more about average transaction amounts.

Member Analysis – Transaction Activity (Tool #775 > ACH Processing)



Note the account number of the member with the highest number of transactions. Search this account in member inquiry, select the Participation/Products tab, and select **Transaction Activity**. The dashboard shows the member's activity over the past three months. Select **Compare to All Members**. The All Mbrs Average Totals column displays each origin's average amount/number of transactions for all memberships. Focus on the ACH Network Processing origin.

Current Month Activity Compare (Inquiry > Participation/Products > Transaction Activity)

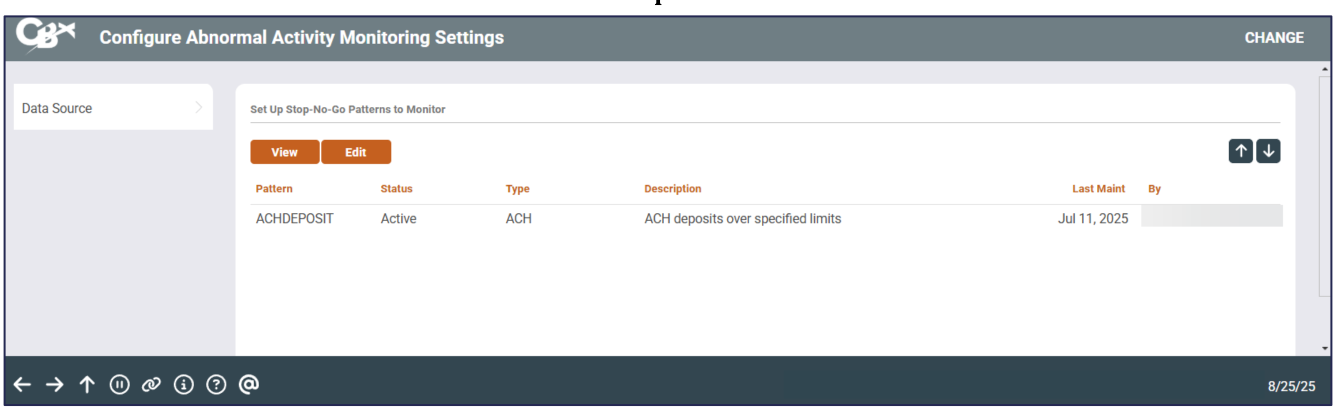


Use these statistics to determine abnormal thresholds for appropriate configuration settings.

Setting Up ACH Stop-No-Go

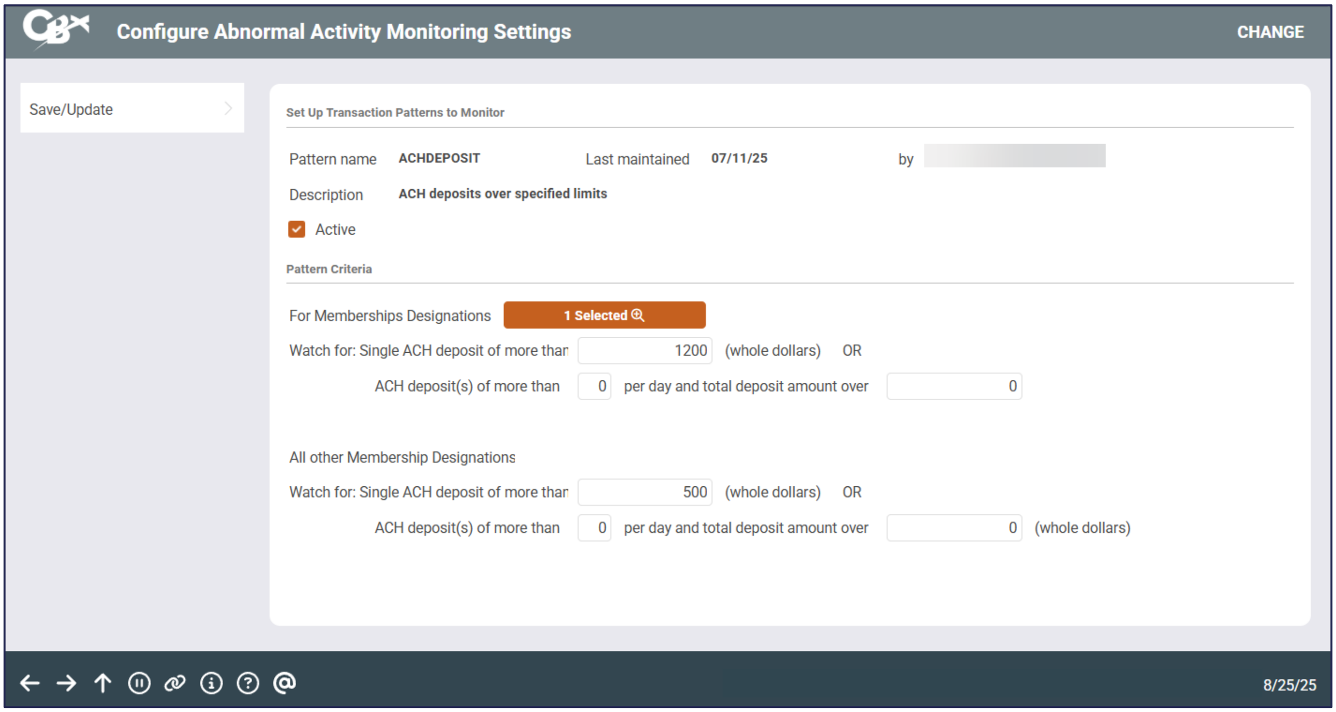
To configure ACH Stop-No-Go, launch **Tool #101 *Abnormal Activity Monitoring Config*** and select *Stop-No-Go Patterns*. Then, select to **Edit** the ACHDEPOSIT pattern.

Tool #101 > Stop-No-Go Patterns



You can set up the pattern to trigger when an ACH deposit exceeds the defined amount allowed and/or when the number of deposits and cumulative amount total exceeds the configured threshold. You're able to configure two separate limit sets for select membership designation(s) and all other membership designations.

Tool #101 > Stop-No-Go Patterns



Once you are confident with your settings, you can configure the system to begin monitoring ACH deposits against the specified criteria prior to posting by checking the *Active* checkbox.

Be sure your pattern criteria are reasonable prior to activating the monitoring pattern. Once the pattern is activated, when a deposit exceeds the configured thresholds, that deposit and all other ACH deposits that day for that member will not post and will appear in exceptions for review.

Monitoring Abnormal Activity

Monitor abnormal activity for member groups and transaction patterns via **Tool #537 *Monitor Abnormal Transaction Activity***. For Stop-No-Go patterns, monitor your ACH exceptions via **Tool #1875 *Work ACH Exceptions***.

Monitoring Options Available to Both Member Groups and Transaction Patterns

After configuring your abnormal activity monitoring settings, you can monitor accounts flagged according to your member group or transaction pattern settings via **Tool #537 *Monitor Abnormal Transaction Activity***. You'll have several options of how to view and what to do with the information on the Abnormal Activity dashboard. These options are explained below.

Learn how to access the dashboard for member groups on page 25.

Learn how to access the dashboard for transaction patterns on page 29.

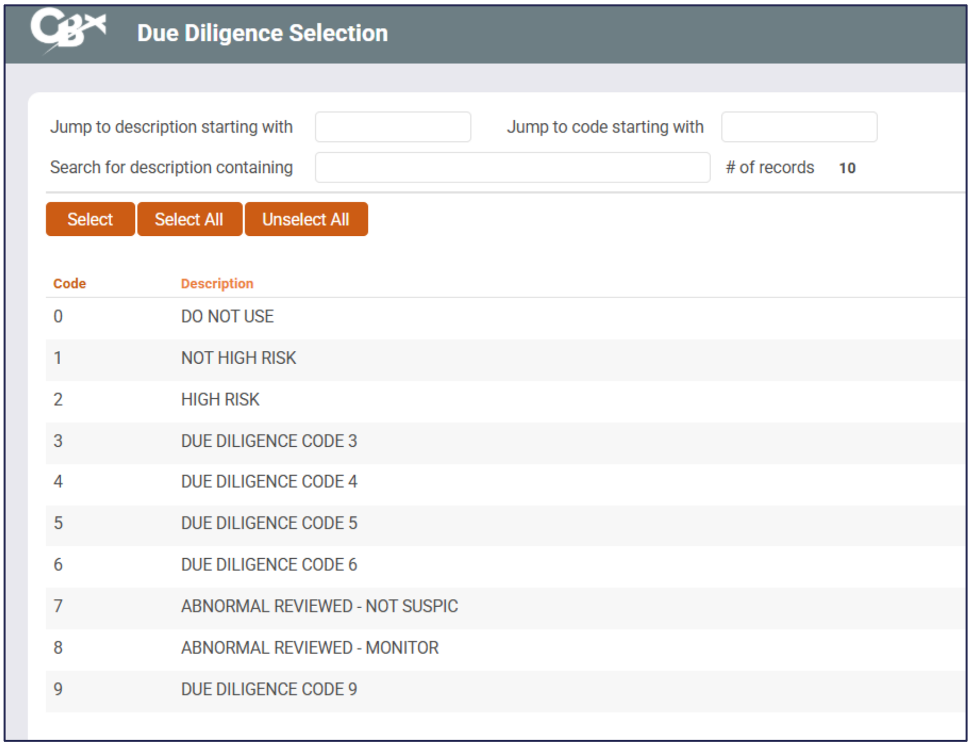
View Members with Certain Due Diligence Flag

Monitor activity for memberships you have marked for special attention using the configurable Due Diligence flag. Select which members to view, and the system will display just those members within the member group with the due diligence flag you select.

Additionally, feature will show all transaction activity for those members, even if the counts/dollar amount of transactions fell within your configured “normal” range.

1. Click the **Select** button next to the field Include all activity for members with Due Diligence flag.

Due Diligence Selection (Tool #537 > Member Groups/Transaction Patterns > Due Diligence Flag Select)



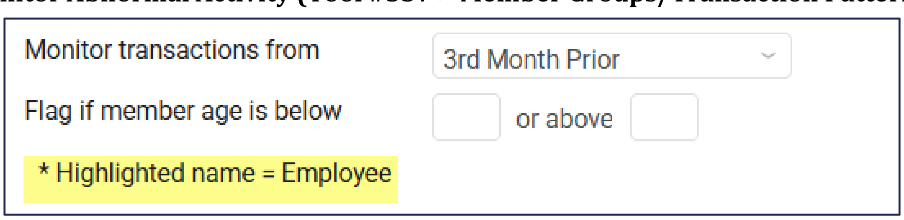
2. From the list of Due Diligence codes, either double-click the code you would like to filter by or select the code and click **Select**.

   - Due Diligence Codes can be configured via **Tool #247 *Configure Due Diligence Codes***.

Flag Members in a Certain Age Range

This feature was developed to help you identify members that may be more susceptible to fraud, such as minors or elderly members.

Monitor Abnormal Activity (Tool #537 > Member Groups/Transaction Patterns)



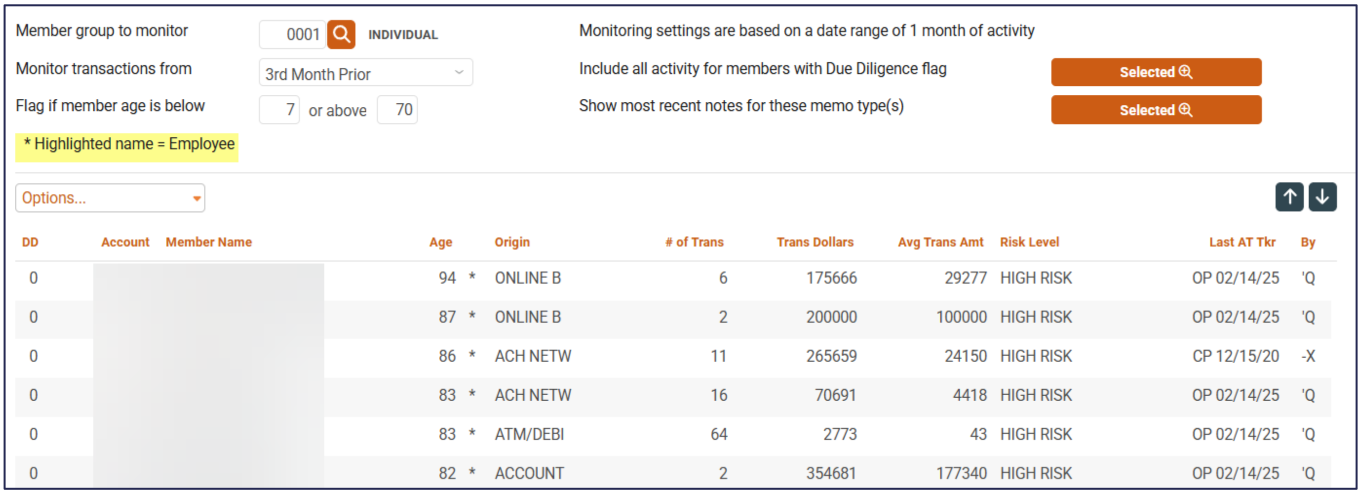
To flag (put an asterisk next to) members in a certain age range:

1. Enter the age range in the field *Flag if member age is below XXX or above XXX*. Since there are certain age ranges more at risk than others, it's recommended to always flag those age ranges in all your member groups that you monitor.

2. Use Enter.

3. Members in the age range you selected will have an asterisk next to their age.

Monitor Abnormal Activity (Tool #537 > Member Groups/Transaction Patterns)

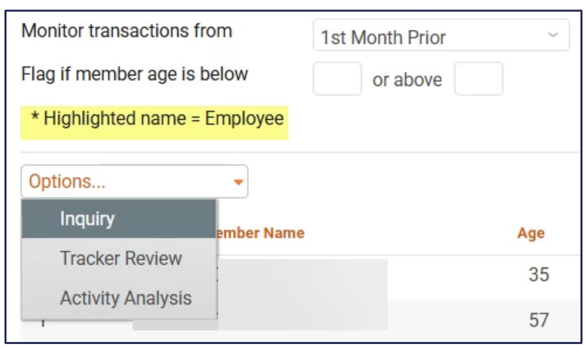


CU*TIP: Click the Age column heading to change the sort order so that the flagged members appear at the top of the list.

Go to Inquiry Screen of a Specific Member on List

This feature, accessible by selecting Inquiry, allows you to look at a member's actual transaction history, view other miscellaneous details about the member, etc. This is a very valuable feature because it allows you to ascertain whether or not the activity you are seeing is actually typical for the member.

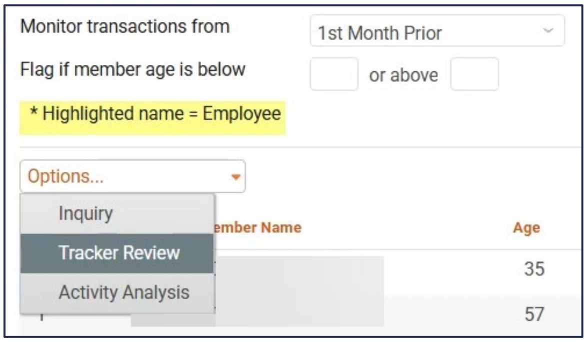
Monitor Abnormal Activity (Tool #537 > Member Groups/Transaction Patterns)



Review Tracker Conversations of a Specific Member on List

By selecting Tracker Review, you can create or review Tracker conversations for one of the members on your list.

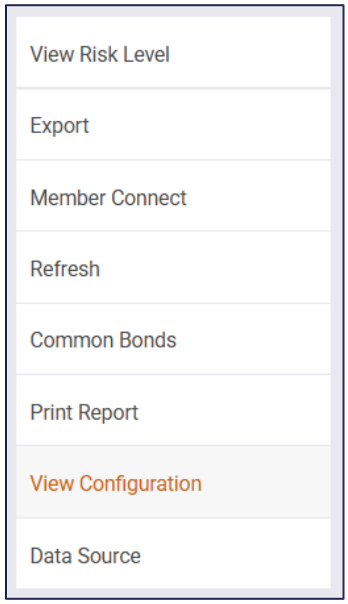
Monitor Abnormal Activity (Tool #537 > Member Groups/Transaction Patterns)



View Configuration Settings

By selecting **View Configuration**, you can view the configuration settings for the member group listed.

Monitor Abnormal Activity (Tool #537 > Member Groups/Transaction Patterns)

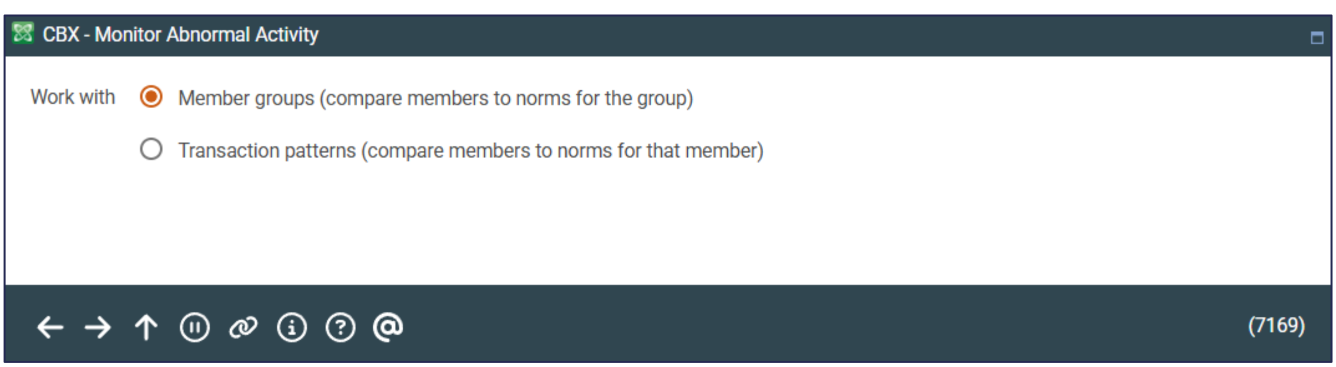


Monitoring Activity for a Member Group

After setting up your member groups, you can monitor any flagged accounts within **Tool #537 *Monitor Abnormal Transaction Activity***.

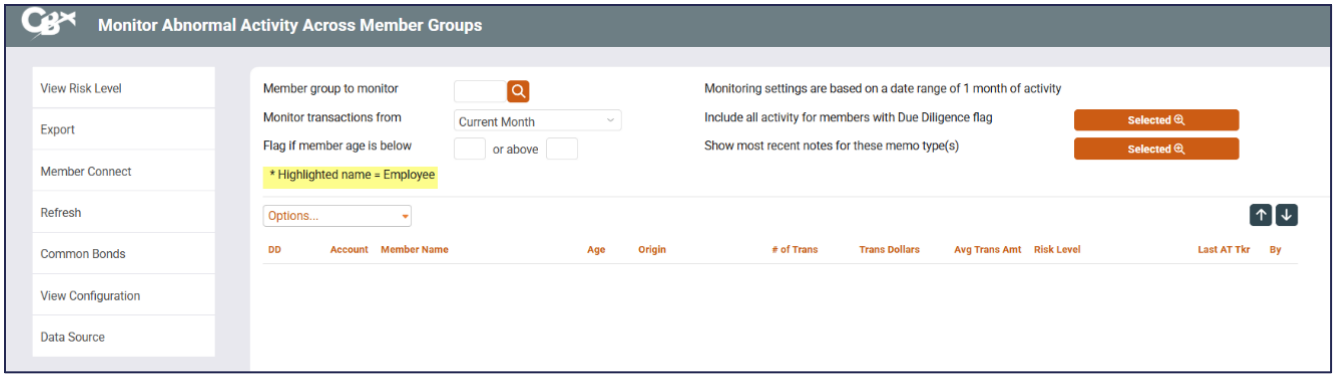
1. Launch **Tool #537 *Monitor Abnormal Transaction Activity***.
2. Select the *Member groups (compare members to norms for the group)* option.

Monitor Abnormal Activity (Tool #537)



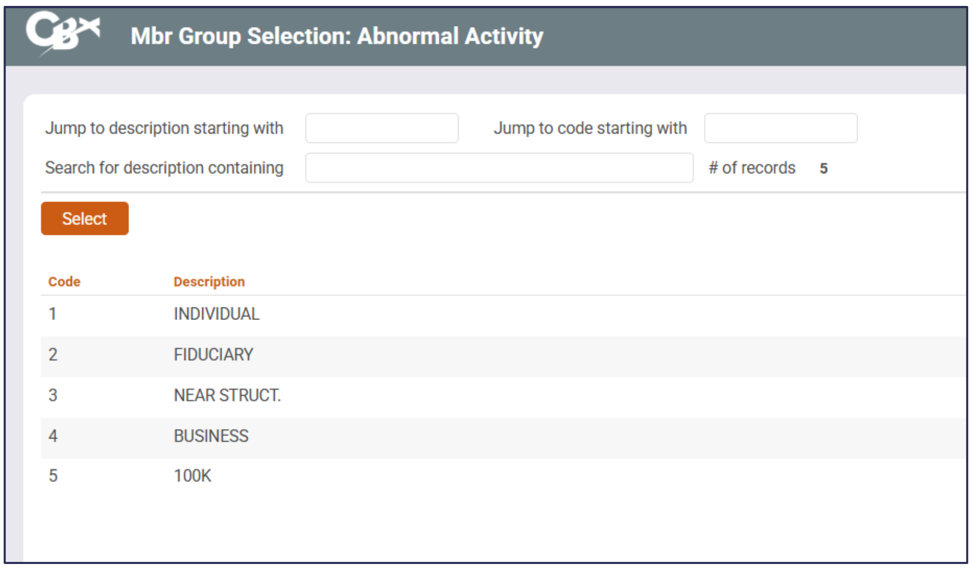
3. Use the lookup button next to the *Member group to monitor* field.

Monitor Abnormal Activity Across Member Groups (Tool #537 > Member Groups)



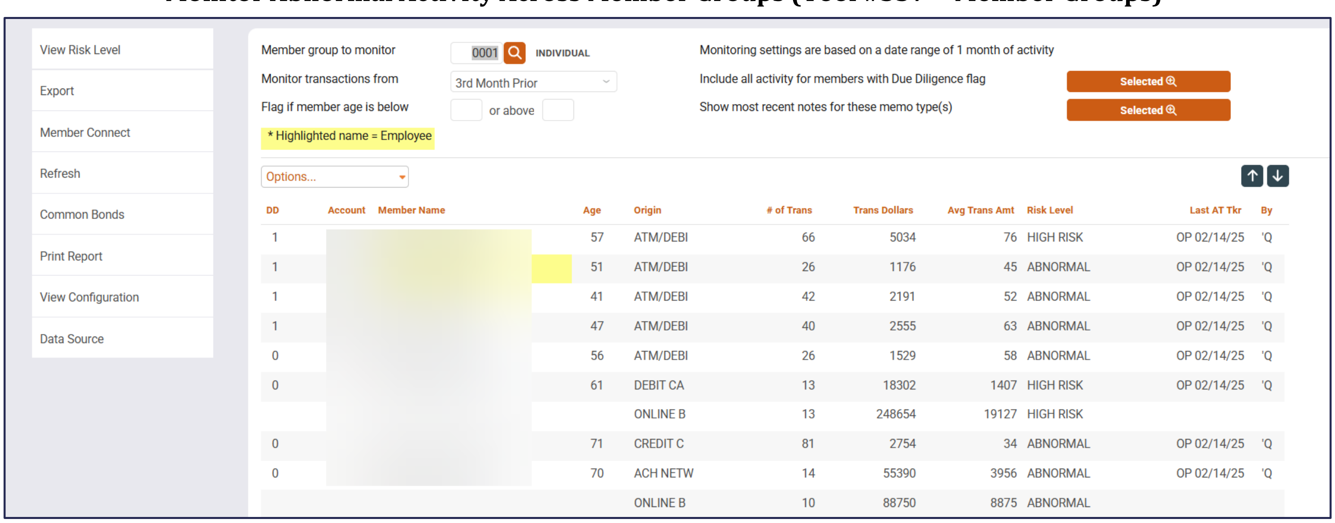
4. Select the member group. Either double-click the member group on which you would like to run the tool or highlight the member group and use **Select**.

Mbr Group Selection: Abnormal Activity (Tool #537 > Member Groups > Member Group to Monitor Lookup)



On the next screen, Monitor Abnormal Activity Across Member Groups, you are now able to view transaction information (total transactions, total dollar amounts, and average dollar amounts) for the transaction(s) and membership type(s) configured for this member group.

Monitor Abnormal Activity Across Member Groups (Tool #537 > Member Groups)



DD	Account	Member Name	Age	Origin	# of Trans	Trans Dollars	Avg Trans Amt	Risk Level	Last AT Tkr	By
1			57	ATM/DEBI	66	5034	76	HIGH RISK	OP 02/14/25	'Q
1			51	ATM/DEBI	26	1176	45	ABNORMAL	OP 02/14/25	'Q
1			41	ATM/DEBI	42	2191	52	ABNORMAL	OP 02/14/25	'Q
1			47	ATM/DEBI	40	2555	63	ABNORMAL	OP 02/14/25	'Q
0			56	ATM/DEBI	26	1529	58	ABNORMAL	OP 02/14/25	'Q
0			61	DEBIT CA	13	18302	1407	HIGH RISK	OP 02/14/25	'Q
				ONLINE B	13	248654	19127	HIGH RISK		
0			71	CREDIT C	81	2754	34	ABNORMAL	OP 02/14/25	'Q
0			70	ACH NETW	14	55390	3956	ABNORMAL	OP 02/14/25	'Q
				ONLINE B	10	88750	8875	ABNORMAL		

Member activity will appear on the dashboard as “abnormal” or “high risk” based on the member’s transaction count and/or total transaction dollars. If a member’s activity under any particular Origin group happens to fall within two different risk level ranges (e.g., the transaction count shows it as “abnormal” but the $ amount makes it fall into the “high risk” range), the higher of the two levels will be shown.

- By default, the data is sorted by due diligence code with the highest number at the top of the screen. To update a member’s Due Diligence flag, go to **Tool #15 *Update Membership Information***.
- Members that have more than one row (the corresponding rows will be partially blank) are those for whom abnormal/high risk activity is associated with more than one transaction type.

> *Keep in mind that you will only see the transaction types (origins) that were configured for this member group (e.g., ACH, ATM, debit card, credit card, etc.).*

Monitoring Options Available to Member Groups Only

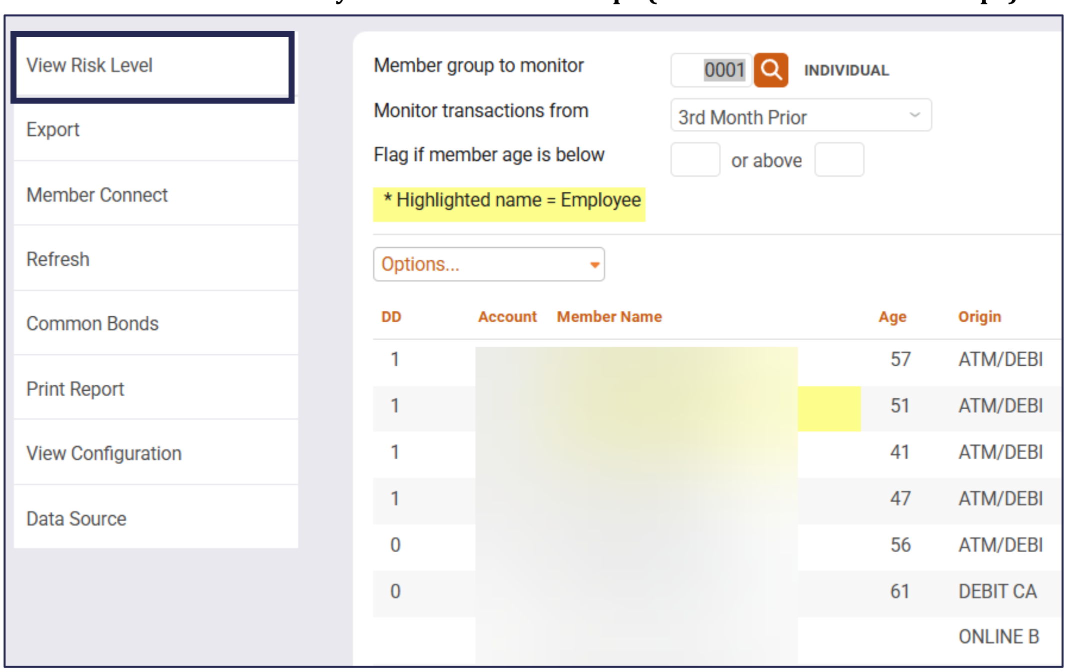
After accessing the abnormal activity monitoring dashboard for member groups, you’ll be able to monitor member groups using the options below, in addition to the monitoring options discussed in the *Monitoring Options Available to Both Member Groups and Transaction Patterns* section on page 22.

Filter by Risk Level

You can filter the Risk Level column to display only accounts showing “high risk” or only accounts showing “abnormal”.

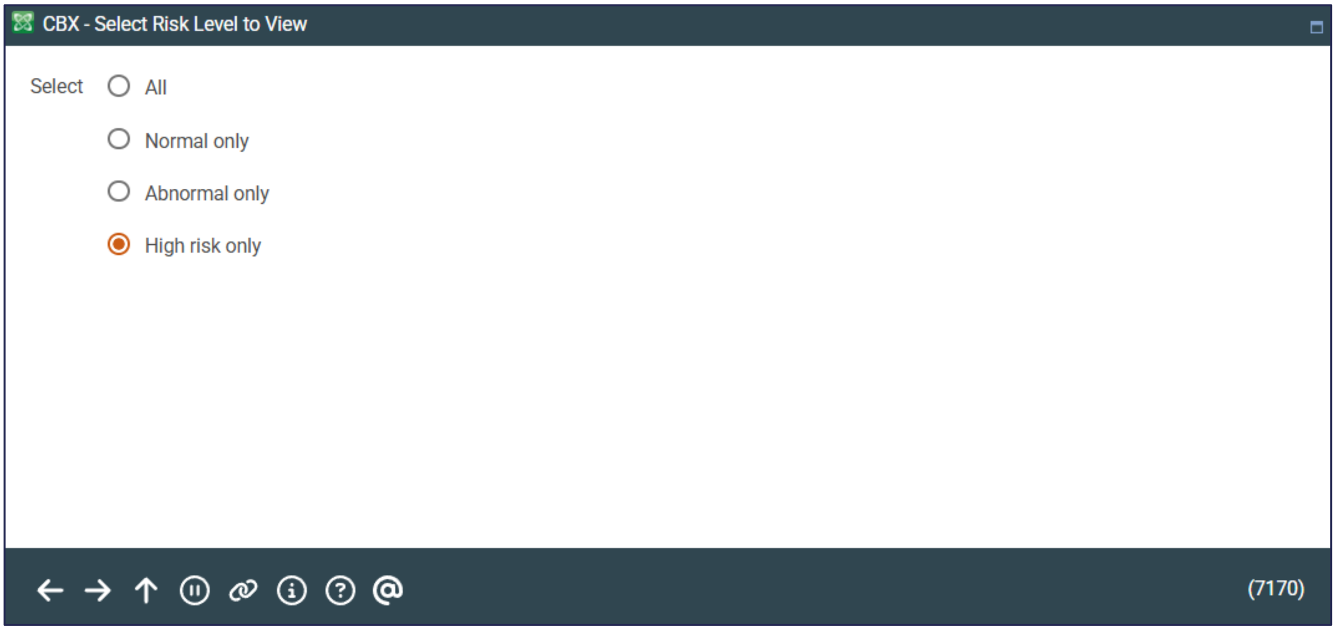
1. Select **View Risk Level**.

Monitor Abnormal Activity Across Member Groups (Tool #537 > Member Groups)



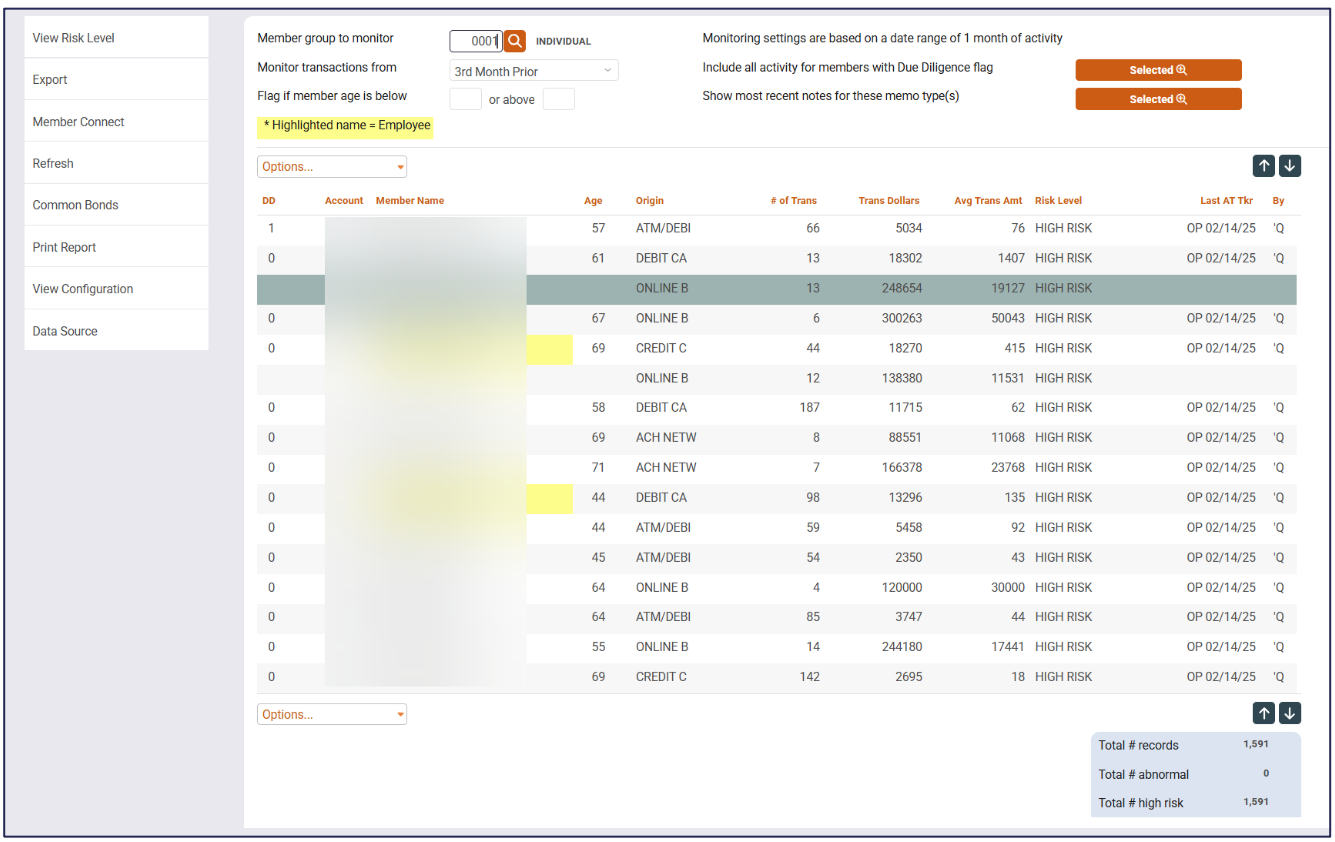
2. Select the desired risk level option.

Select Risk Level to View (Tool #537 > Member Groups > View Risk Level)



3. Use Enter.

Monitor Abnormal Activity Across Member Groups (Tool #537 > Member Groups)



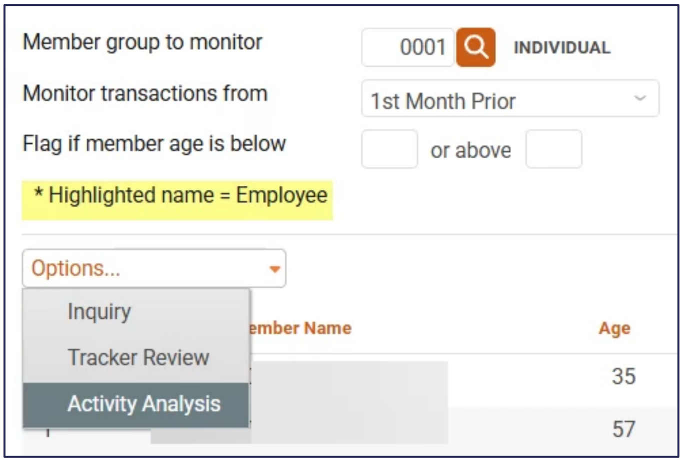
DD	Account	Member Name	Age	Origin	# of Trans	Trans Dollars	Avg Trans Amt	Risk Level	Last AT Tkr	By
1			57	ATM/DEBI	66	5034	76	HIGH RISK	OP 02/14/25	'Q
0			61	DEBIT CA	13	18302	1407	HIGH RISK	OP 02/14/25	'Q
				ONLINE B	13	248654	19127	HIGH RISK		
0			67	ONLINE B	6	300263	50043	HIGH RISK	OP 02/14/25	'Q
0			69	CREDIT C	44	18270	415	HIGH RISK	OP 02/14/25	'Q
				ONLINE B	12	138380	11531	HIGH RISK		
0			58	DEBIT CA	187	11715	62	HIGH RISK	OP 02/14/25	'Q
0			69	ACH NETW	8	88551	11068	HIGH RISK	OP 02/14/25	'Q
0			71	ACH NETW	7	166378	23768	HIGH RISK	OP 02/14/25	'Q
0			44	DEBIT CA	98	13296	135	HIGH RISK	OP 02/14/25	'Q
0			44	ATM/DEBI	59	5458	92	HIGH RISK	OP 02/14/25	'Q
0			45	ATM/DEBI	54	2350	43	HIGH RISK	OP 02/14/25	'Q
0			64	ONLINE B	4	120000	30000	HIGH RISK	OP 02/14/25	'Q
0			64	ATM/DEBI	85	3747	44	HIGH RISK	OP 02/14/25	'Q
0			55	ONLINE B	14	244180	17441	HIGH RISK	OP 02/14/25	'Q
0			69	CREDIT C	142	2695	18	HIGH RISK	OP 02/14/25	'Q

Take note that the number of records shown in the lower right-hand corner of the dashboard will adjust to reflect only the number of accounts with the chosen risk level.

View Transaction Information for a Specific Member on List

By selecting the *Activity Analysis* option, you can view a summary of the transaction activity for the member you selected broken down by origin. Keep in mind that the transaction activity you will be able to view will be for all transaction types (origins) you had configured when setting up your group.

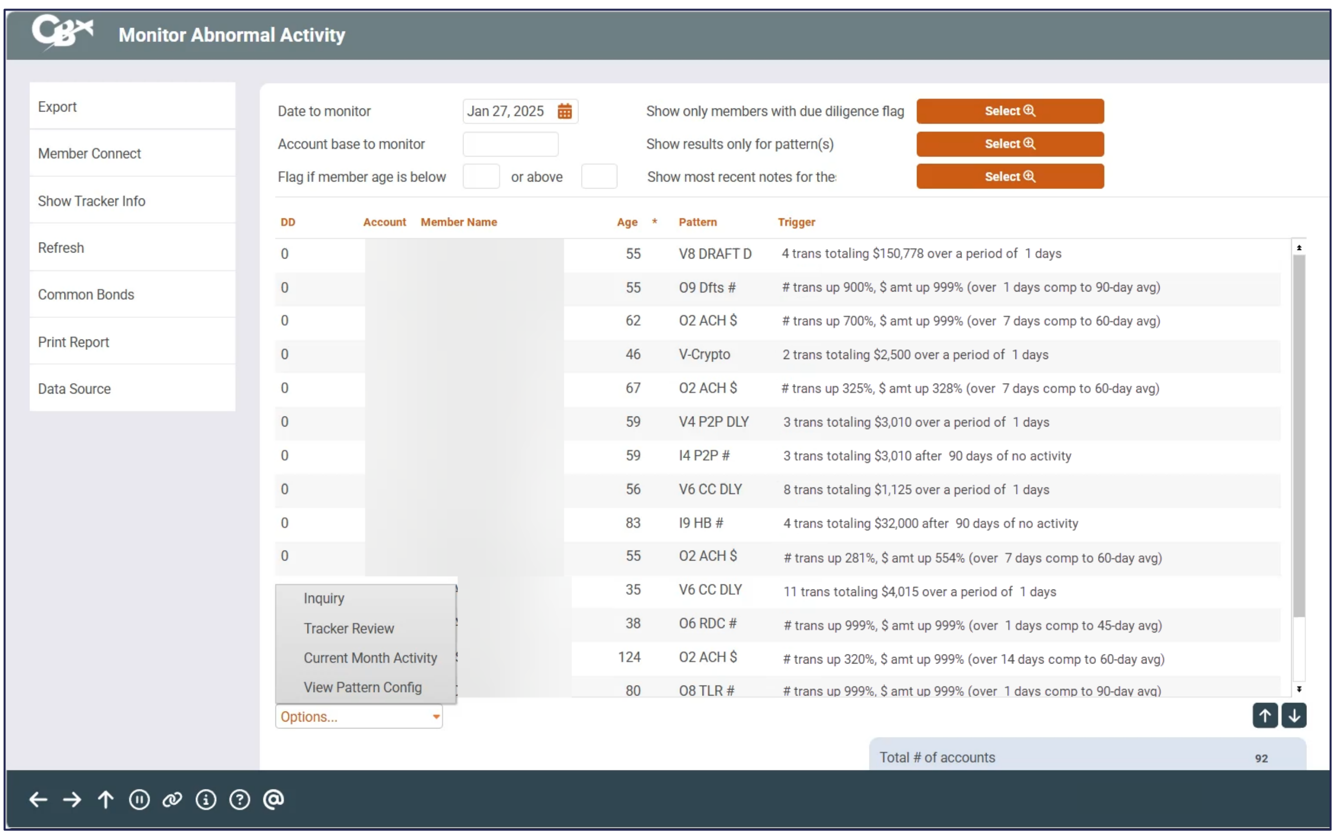
Monitor Abnormal Activity Across Member Groups (Tool #537 > Member Groups)



Monitoring Activity for Transaction Patterns

After setting up your transaction patterns, you can monitor flagged accounts via **Tool #537 *Monitor Abnormal Transaction Activity***. Review the resulting accounts daily.

Monitor Abnormal Activity – Transaction Patterns (Tool #537)



There may be instances where less time is needed to assess whether a pattern needs to be adjusted. For example, you may want to adjust your pattern if your test run yields a large number of accounts with normal activity (false positives). See page 34 to learn more about *Transaction Pattern Adjustments for False Positives*.

While you are monitoring abnormal transaction activity, we recommend you document the accounts you've reviewed and track the false positive ratio for the pattern. You may do so by using the *Review Tracking Template* and using the *Hit Tracking Template*.

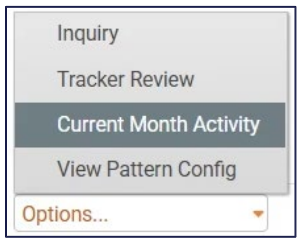
Monitoring Options Available to Transaction Patterns Only

After accessing the abnormal activity monitoring dashboard for transaction patterns, you'll be able to monitor transaction patterns using the options below, in addition to the monitoring options discussed in the *Monitoring Options Available to Both Member Groups and Transaction Patterns* section on page 22.

View Current Month Activity

To view an account's activity for the current month, select the account on the dashboard, then select the *Current Month Activity* option.

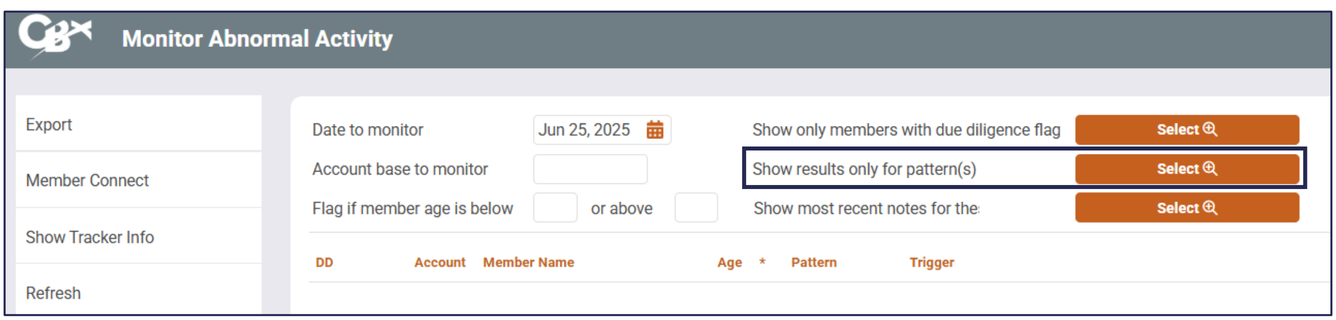
Monitor Abnormal Activity (Tool #537)



View Members Who Triggered a Certain Pattern

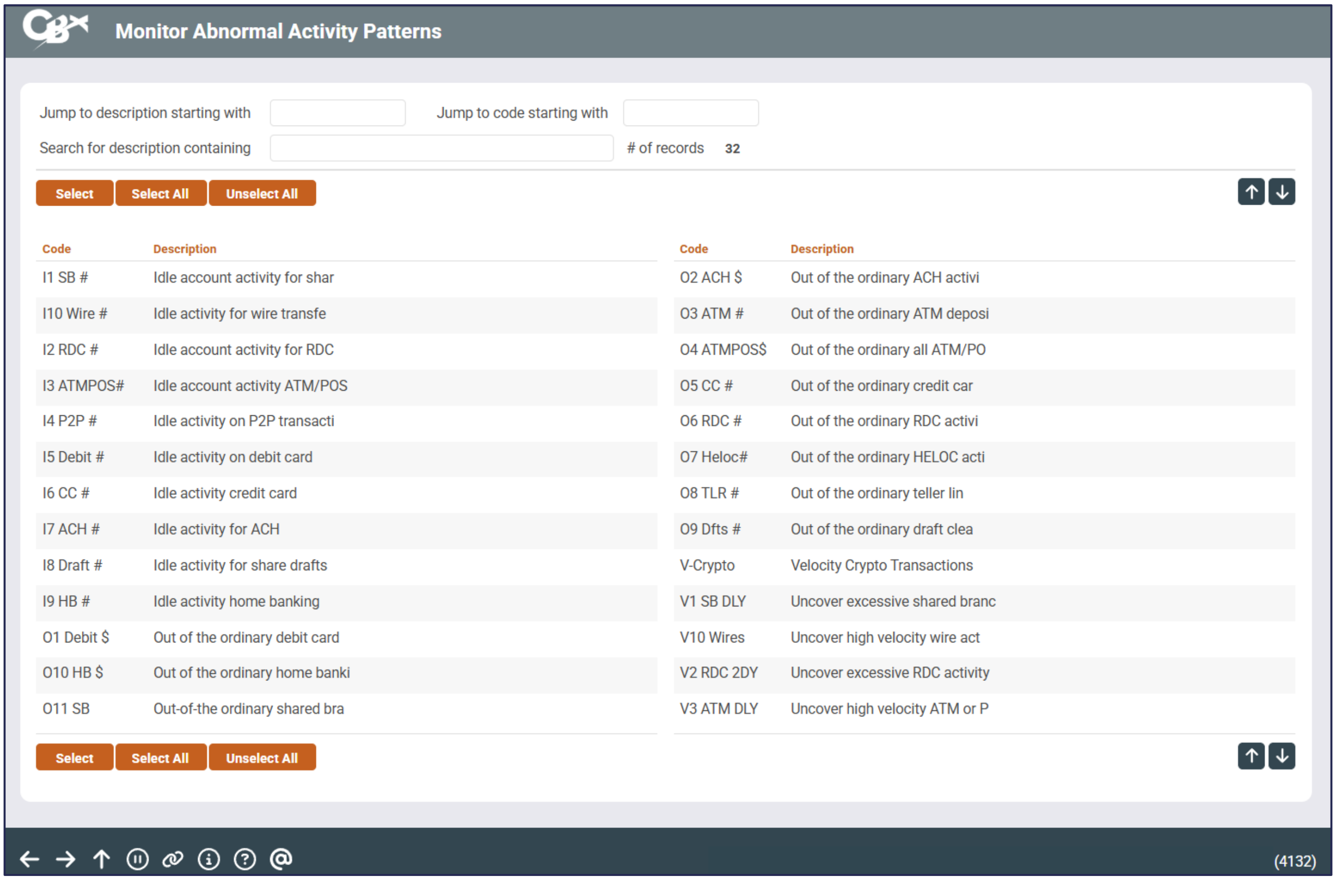
To view only those accounts who've triggered a certain pattern, select Show results only for pattern(s).

Monitor Abnormal Activity (Tool #537)



You'll be able to select multiple patterns to limit the dashboard results by.

Monitor Abnormal Activity Patterns (Tool #537 > Show results only for pattern(s))



Review Transaction Pattern Flagged Accounts

The dashboard for **Tool #537** displays the flagged accounts, patterns triggered, and transaction activity that triggered the pattern. Remember: just because an account surpasses the trigger threshold does not mean the activity is abnormal for the member.

To take a deeper look at the account's transaction activity, select the flagged account and the *Inquiry* option to jump into member inquiry. Viewing the transaction history allows you to ascertain whether or not the activity is actually abnormal for that member.

There are several things you should be looking for when reviewing the accounts within the dashboard.

- What is the nature and purpose of the account? (Do they have a regular ACH payroll deposit? Does the member have a loan with the credit union? How long have they been a member? Etc.)
- If transactions are incoming, does it look like potential layering activity? Are the funds still in the account? Were payment applications used to move funds out of the account? Did the member purchase cryptocurrency?
- If transactions were outgoing, what were they funded by (wire transfers, payment applications, etc.)?
- How old is the member? Were they the individual who conducted the transaction, or was it a joint owner?

Review Tracking Template

An actual review of account transactions is the best way to distinguish false positives from those that have potentially fraudulent activity.

Use the Review Tracking Template to document the results of your review of accounts that appear in **Tool #537 *Monitor Abnormal Transaction Activity***.

Review Tracking Template

ABC Credit Union									
#	Activity Date	Review Date	Pattern	Account	Trigger	Configuration	Review Notes	Worthy of Review	False Positive
1	4/22/2021	4/23/2021	V7 ACH DLY	XXXXX	10 trans totaling $8279 over 1 day	10 or more trans during a period of 1 day and $7500 or more during 1 day			X
2	4/22/2021	4/23/2021	I7 ACH #	XXXXX	2 trans totaling $5531 after 90 days inactivity	1 or more trans after 90 days of inactivty and $5000 or more after 90 days			X
3	4/22/2021	4/23/2021	V5 DBT DLY	XXXXX	14 trans totaling $68911 over 3 days	8 or more trans during a period of 3 days and $10000 or more during 3 days		X	
4	4/22/2021	4/23/2021	V9 HB DLY	XXXXX	5 trans totaling $150000 over 1 day	5 or more trans during a period of 1 day and $10000 or more during 1 day		X	
5	4/22/2021	4/23/2021	V5 DBT DLY	XXXXX	11 trans totaling $10196 over 3 days	8 or more trans during a period of 3 days and $10000 or more during 3 days			X
6	4/22/2021	4/23/2021	V9 HB DLY	XXXXX	6 trans totaling $80000 over 1 day	5 or more trans during a period of 1 day and $10000 or more during 1 day		X	
7	4/22/2021	4/23/2021	I7 ACH #	XXXXX	1 trans totaling $6583 after 90 days inactivity	1 or more trans after 90 days of inactivty and $5000 or more after 90 days			X
8									
9									
10									
11									
12									
							Worthy of Review	3	43%
							False Positive	4	57%
							Total	7	

(To access the template, *place a FREE store order*.)

Hit Tracking Template

To determine the false positive rate, it is important to review an adequate sample of accounts within the origin under consideration and over an ample amount of time.

Use the **Hit Tracking Template** to determine the ratio of false positives vs. accounts with potentially fraudulent activity (i.e., accounts worthy of review).

Hit Tracking Template

ABC Credit Union				Activity Date	Activity Date	Activity Date	Activity Date	Activity Date	5/17 - 5/21				
	Pattern	Type	Description	5/17/2021	5/18/2021	5/19/2021	5/20/2021	5/21/2021	Total	WOR	FP	FP Ratio	Raise / Lower / Remain
1	I1 SB#	Idle	Idle activity for shared branching	NH	NH	1	1	NH	2	1	1	50%	Remain
2	I2 RDC#	Idle	Idle activity for RDC	NH	NH	NH	NH	NH	0	0		0%	Lower
3	I3 ATMPOS#	Idle	Idle activity for ATM/POS	1	1	2	2	1	7	2	5	71%	Raise
4	I4 P2P#	Idle	Idle activity for P2P	NH	NH	NH	NH	NH	0	0		0%	Lower
5	I5 Debit#	Idle	Idle activity for debit card	NH	NH	NH	1	1	2	1	1	50%	Remain
6	I6 CC#	Idle	Idle activity for credit card	NH	NH	NH	NH	NH	0	0		0%	Lower
7	I7 ACH#	Idle	Idle activity for ACH	2	NH	NH	NH	NH	2	1	1	50%	Remain
8	I8 Draft#	Idle	Idle activity for share drafts	NH	NH	NH	NH	NH	0	0		0%	Lower
9	I9 HB#	Idle	Idle activity for home banking transfers	NH	NH	NH	NH	1	1	0	1	100%	Remain
10	I10 Wire#	Idle	Idle activity for wire transfers	NH	NH	NH	NH	NH	0	0		0%	Lower
11	01 Debit$	Out-of Ord	Out of the ordinary debit card activity	2	1	1	2	3	9	4	5	56%	Remain
12	02 ACH$	Out-of Ord	Out of the ordinary ACH activity	1	NH	NH	NH	1	2	0	2	100%	Remain
13	03 ATM#	Out-of Ord	Out of the ordinary ATM activity	NH	2	3	4	5	14	4	10	71%	Raise
14	04 ATMPOS$	Out-of Ord	Out of the ordinary ATMPOS activity	2	5	4	4	9	24	6	18	75%	Raise
15	05 CC#	Out-of Ord	Out of the ordinary credit card activity	NH	NH	NH	NH	NH	0	0		0%	Lower
16	06 RDC#	Out-of Ord	Out of the ordinary RDC activity	NH	NH	NH	NH	NH	0	0		0%	Lower
17	07 HELOC#	Out-of Ord	Out of the ordinary HELOC activity	NH	NH	NH	NH	NH	0	0		0%	Lower
18	08 TLR#	Out-of Ord	Out of the ordinary teller line activity	NH	NH	NH	NH	NH	0	0		0%	Lower
19	09 Dfts#	Out-of Ord	Out of the ordinary draft clearings	1	3	7	8	9	28	5	23	82%	Raise
20	010 HB$	Out-of Ord	Out of the ordinary home banking transfers	NH	1	1	1	1	4	1	3	75%	Remain
21	V1 SB DLY	Velocity	Excessive shared branch activity	NH	1	2	2	3	8	2	6	75%	Raise
22	V2 RDC 2DY	Velocity	Excessive RDC activity	NH	NH	NH	NH	NH	0	0		0%	Lower
23	V3 ATM DLY	Velocity	Excessive ATM or POS activity	2	1	NH	2	2	7	3	4	57%	Remain
24	V4 P2P DLY	Velocity	Excessive P2P activity	1	2	2	2	2	9	5	4	44%	Remain
25	V5 DBT DLY	Velocity	Excessive DBT activity	NH	NH	2	NH	NH	2	1	1	50%	Remain
26	V6 CC DLY	Velocity	Excessive CC activity	NH	NH	NH	NH	NH	0	0		0%	Lower

For each applicable pattern, record the number of accounts reviewed and the date of the review. Enter "NH" (i.e., "no hits") if the pattern returned no results.

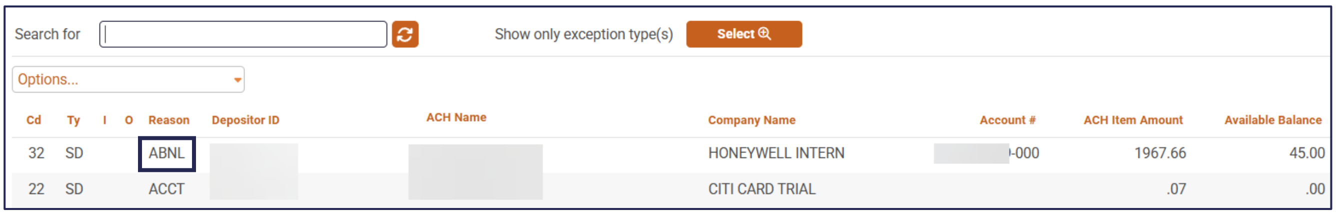
(To access the template, *place a FREE store order*.)

Monitoring Stop-No-Go Patterns

For the ACHDEPOSIT stop-no-go pattern, once a member's ACH deposit reaches the configured thresholds for the stop-no-go pattern, the deposit that triggered the pattern (along with any additional ACH deposits that day for that member) will be sent to your ACH exceptions.

You can view and work your stop-no-go ACH exceptions within **Tool #1875 *Work ACH Exceptions***. These exceptions will be listed with a reason code of ABNL. You can use the **Select** button next to *Show only exception type(s)* to filter the results by only those with the ABNL code.

Work with Daily ACH Exceptions (Tool #1875)



Review these exceptions daily and determine whether to post or return the item.

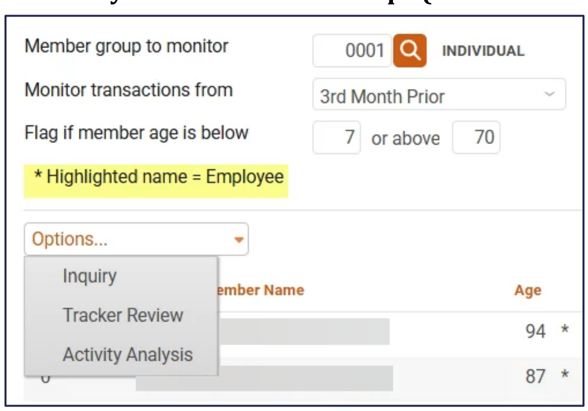
Adjust your pattern settings based on the actions taken with these exceptions.

Documenting Your Member Group Activity Review

Once you have completed your review of account activity, it is important to record your conclusions. This will not only serve as evidence of your review but will also create a history of notes for any future reviews.

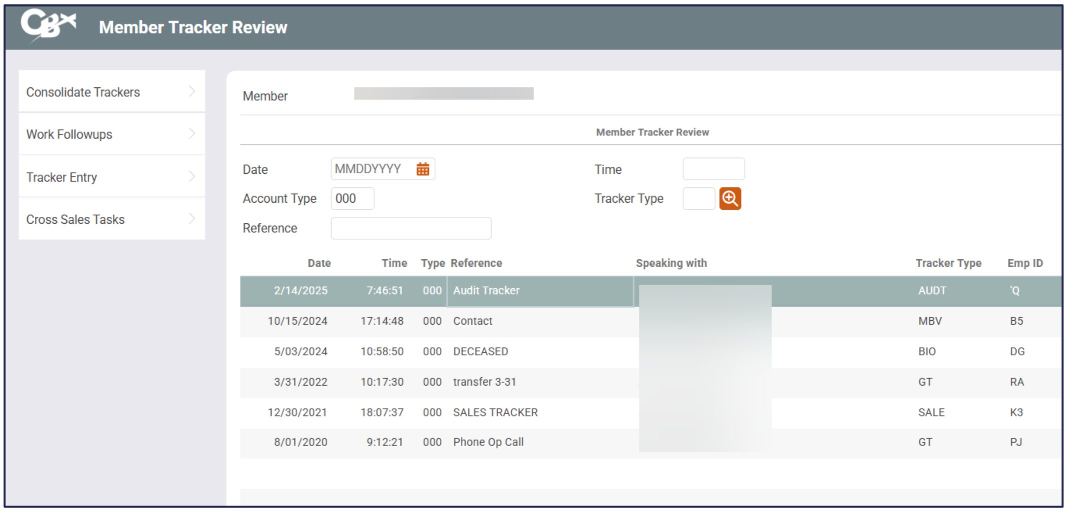
1. Highlight the account and select the *Tracker Review* option from the Abnormal Activity Monitoring dashboard.

Monitor Abnormal Activity Across Member Groups (Tool #537 > Member Groups)



2. From the Member Tracker Review screen, select the existing Audit Tracker entry and choose the option to *Update*.

Member Tracker Review (Tool #537 > Member Groups > Tracker Review)



CU*TIP: It is recommended to create a specific Memo Type under the Audit Tracker Type in order to distinguish abnormal activity monitoring trackers from other trackers.

Transaction Pattern Adjustments for False Positives

Adjust the applicable pattern configurations based on the resulting ratios. The pattern criteria (days and/or dollar amounts) should be raised, lowered, or remain the same depending on the composition of false positives vs. accounts worthy of review. Conduct this analysis periodically—at least annually—in order to determine false positive rates and make necessary configuration adjustments.

> ***IMPORTANT NOTE:*** *The configuration change should not impact the accounts that were worthy of review. Those accounts should still appear in results just as they did prior to the configuration change.*

An Example

As an example, over the course of 5-days (5/17 – 5/21), 24 accounts were reviewed for out-of-the-ordinary ATM/POS activity. Of the accounts, 75% (18) were false positives. This is an indication that the number of transactions and/or dollar threshold is set too low. Consequently, the number of transactions and/or dollar threshold should be raised to capture fewer false positives.

False Positive Ratios on the Hit Tracking Template

			5/17 - 5/21				
Pattern	**Type**	**Description**	**Total**	**WOR**	**FP**	**FP Ratio**	**Raise / Lower / Remain**
I10 Wire#	Idle	Idle activity for wire transfers	0	0		0%	Lower
01 Debit$	Out-of Ord	Out of the ordinary debit card activity	9	4	5	56%	Remain
02 ACH$	Out-of Ord	Out of the ordinary ACH activity	2	0	2	100%	Remain
03 ATM#	Out-of Ord	Out of the ordinary ATM activity	14	4	10	71%	Raise
04 ATMPOS$	Out-of Ord	Out of the ordinary ATMPOS activity	24	6	18	75%	Raise
05 CC#	Out-of Ord	Out of the ordinary credit card activity	0	0		0%	Lower
06 RDC#	Out-of Ord	Out of the ordinary RDC activity	0	0		0%	Lower
07 HELOC#	Out-of Ord	Out of the ordinary HELOC activity	0	0		0%	Lower
08 TLR#	Out-of Ord	Out of the ordinary teller line activity	0	0		0%	Lower
09 Dfts#	Out-of Ord	Out of the ordinary draft clearings	28	5	23	82%	Raise

> ***IMPORTANT NOTE:*** *Sometimes changing patterns impacts previously flagged accounts deemed worthy of review.* ***If this is unavoidable, use due diligence codes and follow-up trackers to mitigate the risk of a previously***

identified account slipping through the cracks after a configuration change.

Average Calculation Method

With out-of-the-ordinary patterns, you have the option to calculate the average daily transaction amount by dividing by the number of days or the number of transactions within the period. The calculation method you choose may affect the false positive rate.

If you choose to calculate by dividing by the number of days, you may experience a higher false positive rate. For example, some members may perform only a few, high-value transactions during the period, which would calculate a low average daily transaction amount when dividing by the number of days. Since the transaction amount would be a large percentage higher than the calculated average, those members' usual high-value transactions could trigger the pattern to flag their account for abnormal activity, despite the behavior being consistent for the member.

As an attempt to reduce the false positive rate, you may switch the calculation method from # of days to # of transactions in the period. When switching calculation methods, be sure to *Run a test* on the pattern to view how the change affects the accounts that populate the dashboard. You will likely have to edit the pattern's thresholds to populate the dashboard with the expected results.

Due Diligence Codes/Trackers

Applying due diligence codes to accounts that have been reviewed for abnormal activity is highly recommended. This enables you to flag accounts with the appropriate risk rating to easily review accounts. Apply a DD code to accounts you consider abnormal for enhanced due diligence. Also, apply an audit tracker to these accounts and utilize the "AB" memo type. If you do not have memo type "AB" configured for your credit union, please contact AuditLink.

You should also apply an audit tracker with memo type "AB" to accounts that are deemed unsuspicious to explain that the activity was normal for that member and clarify no further enhanced due diligence is necessary. The tracker proves you reviewed the account and made your determination.

Utilizing **Tool #664 *Print Member Trackers***, you can pull this information out of CBX to "show your work" and provide proof the accounts are being reviewed.