AuditLink
CU*ANSWERS Management Services

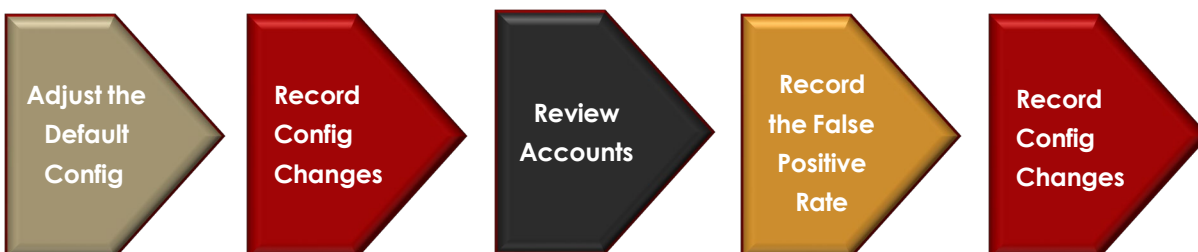# Abnormal Activity Monitoring – Transaction Pattern Change Management

Purpose

The Transaction Pattern option within the Abnormal Activity Monitoring CU*BASE tool was developed to arm credit unions with a means to identify anomalous account activity daily. This feature allows you to run three different series of patterns to flag member transaction activity that meets your configured abnormal parameters.

This booklet describes the change management and data governance methodology developed by AuditLink for use by our credit union partners.

A well-tuned configuration is vital for achieving an efficient and effective abnormal activity identification and review process for credit unions. It is also imperative to have a method for ensuring the integrity of the data being reviewed; something to record the before-and-after of what a configuration was prior to it being changed.

When adjusting, an important question to keep in mind is: "By changing this pattern, will high-risk accounts that were previously flagged no longer be identified?"

The booklet covers the following process:

Adjust the Default Config → Record Config Changes → Review Accounts → Record the False Positive Rate → Record Config Changes

CU*ANSWERS
A CREDIT UNION SERVICE ORGANIZATION

Contents

Pattern Types

Discovering How Different Pattern Types Work

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.

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.

Pattern Configuration

When configuring a transaction pattern, input a descriptive pattern name that will be easily identifiable when reviewing the dashboard of triggered patterns. You must select which savings/loan product(s) to watch.

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 also 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***.)

You are presented 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.)

Default Configuration Adjustments

## Tailoring the Configuration to Fit Your Credit Union

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.

*Sample Transactions by Delivery Channel (**Tool #775**)*
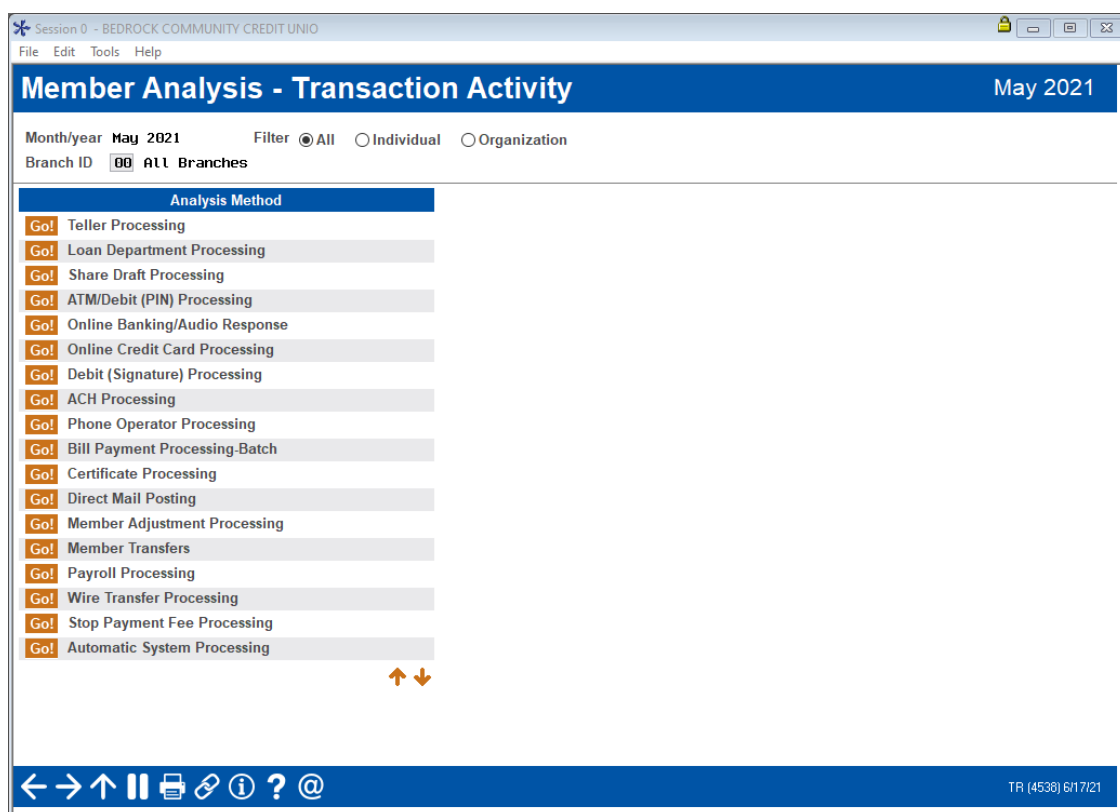
For example, the graphic on the next page shows the highest number of debit card transactions for any member was 255 during the month of May. That breaks down to about 8.2 debit card transactions per day.

Transaction Activity Inquiry

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.

Transaction Activity Inquiry

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.

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.

Abnormal Activity Monitoring Config **(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 that you have a reasonable review population for each pattern.

Configuration Tracking Template
Documenting the Existing Config and Subsequent Changes

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.)

Transaction Pattern Monitoring

Reviewing Flagged Accounts for Abnormal Activity

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).

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.

Review of 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 Inquiry 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

	Activity Date	Review Date	Pattern	Account	Trigger	Configuration	Review Notes	Worthy of Review	False Positive
ABC Credit Union									
#									
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 templates mentioned in this booklet, 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

	Pattern	Type	Description	Activity Date 5/17/2021	Activity Date 5/18/2021	Activity Date 5/19/2021	Activity Date 5/20/2021	Activity Date 5/21/2021		5/17 - 5/21 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 templates mentioned in this booklet, place a FREE store order.)

Pattern Adjustments for False Positives

Revising Configurations for Accurate Abnormal Representation

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

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

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

5/17 - 5/21

> **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 CU*BASE to "show your work" and provide proof the accounts are being reviewed.