AuditLink
CU*ANSWERS Management Services

Abnormal Activity Monitoring – Transaction Pattern Change Management
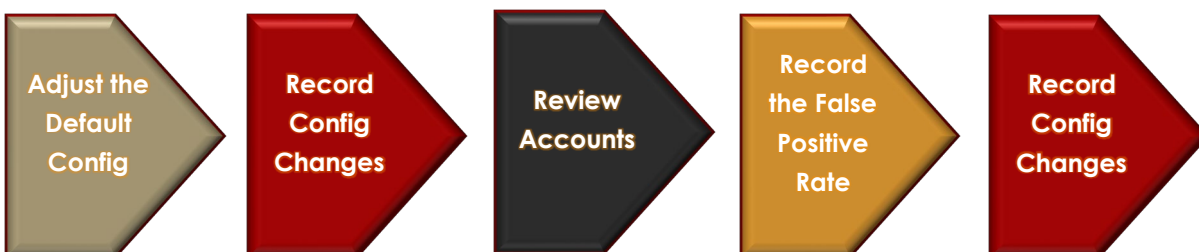
Purpose

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 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

Adjusting the Default Configurations
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.

Determine a 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 to work from.

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.

Member Analysis - Transaction Activity   Debit (Signature) Processing

Month/year May 2021   # Records   5,918   Filter Individual
Branch ID   00   All Branches

Account #	Orig	Name	# of Transactions
			255
			249
			225
			216
			178
			177
			171
			165
			163
			163
			163
			161
			161
			161
			160
			156
			154
			151

■ Select   ↑ ↓

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.

Velocity Trigger Pattern Configuration Screen (Tool #101)

Session 0 CU*BASE GOLD -
File   Edit   Tools   Help

Configure Abnormal Activity Monitoring Settings   CHANGE

Set Up Transaction Patterns to Monitor

Pattern name   V5 DBT DLY   Last maintained   06/10/2021   by   /0   MARVIN JOHNSON (MGR)   AUDIT
Description   Uncover high velocity debit card activity

Velocity Triggers

For individual memberships
    Watch for   10   or more transactions during a period of   1   day(s)
    Watch for a total daily transaction amount of   2,000   or more (whole dollars) during a period of   1   day(s)
For organizational memberships
    Watch for   10   or more transactions during a period of   1   day(s)
    Watch for a total daily transaction amount of   3,000   or more (whole dollars) during a period of   1   day(s)

i   If both counts and $ amounts are configured, the period must be the same for both.
     In order to be shown in the monitoring queue, an account would need to match all criteria for that membership type.

Save/Update

← → ↑ ❚❚ 🖨 🔗 ⓘ ? @

Run a Test on a Pattern Configuration

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.

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

Review Your Results for Needed Adjustments

Then run **Tool #537 – Monitor Abnormal Transaction Activity** and review resulting accounts for at least 2-5 days.

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.

How to Use the Configuration Tracking Template

Documenting the Existing Config and Subsequent Changes

Track Before Making Configuration 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 subsequent changes.

Configuration Tracking Template

How to Use the Review Tracking Template
Documenting the Account Review

Document Your Accounts Reviewed

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

Use the Review 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	

How to Use the Hit Tracking Template

Documenting the False Positive Rate

Determining the False Positive Rate

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

	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

ABC Credit Union

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.

9

Adjusting Your Pattern Based on False Positive Rate
An Example

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 6 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. 75% of the accounts (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 dollar threshold should be raised to capture fewer false positives.

False Positive Ratios

Pattern	Type	Description		Total	WOR	FP	FP Ratio	Raise / Lower / Remain
							5/17 - 5/21	
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.**

Best Practice Use of Due Diligence Codes

Applying due diligence codes to accounts that have been reviewed for abnormal activity is highly recommended. This enables you to track which accounts have already been reviewed and what conclusion was reached. An example is using one code to identify accounts that have been reviewed and the activity deemed not suspicious, and another code used to identify accounts that required continued monitoring.