

BLOCK LIST FUNCTIONALITY EXPANSION

THE NEXT OF MANY INVESTMENTS TO MITIGATE FRAUD

Jim Vilker, NCCO, CAMS
VP of Professional Services

Marvin Johnson, NCCO, CAMS, CFE
Manager AuditLink

AuditLink

LEADING UP TO THIS POINT 2016 LEADERSHIP PROMISE TO DRIVE DOWN YOUR COST OF COMPLIANCE

Tool #	Title
Go! 984	Work Daily BSA/CTR Activity
Go! 633	Print BSA/SAR Activity Report
Go! 985	Work Dormant Members
Go! 778	Scan a Single Name Through OFAC
Go! 559	OFAC Non-Member Scan History
Go! 532	Misc Advance Monthly Analysis Report
Go! 480	Loans w/ Interest Due Above Payment Amt
Go! 592	Portfolio Analysis - Concentration Risk
Go! 533	Misc Receipt Monthly Analysis Report
Go! 460	Loan Concentration Risk Report by Member
Go! 145	ATM/Dbt/Crdt: Audit Card Status Changes
Go! 774	Sample Checking Account Activity

Tool #	Title
Go! 775	Sample Transactions by Delivery Channel
Go! 980	Wire Transfer Activity Report
Go! 981	Wire Transfer Tracking
Go! 159	Audit CU File Maintenance (CUFMAINT)
Go! 247	Configure Due Diligence Codes
Go! 160	Audit Data Center Employee Activity
Go! 162	Audit Insider/Employee Activity (SECAUD)
Go! 664	Print Member Trackers
Go! 402	Insider Audit/Due Diligence Report
Go! 750	Red Flag Controls
Go! 272	Configure Privacy Controls
Go! 381	General Transaction Register

BIG PICTURE (APRIL 2019)

A NEW BUSINESS AND NEW RICH FUNCTIONALITY

- Leverage what we have learned from standalone system projects
- Expand AuditLink services to include shared execution
 - Work Abnormal Activity Monitoring dashboards and alerts created
 - Currently 20 credit unions using the AuditLink service
- Become the network experts in all fraud and ALM systems and consult relative to the purchase and use of those systems including CU*BASE, Verafin, and Global Vision. To date AuditLink has consulted with multiple credit unions and have quarterly focus groups with Verafin clients.
- Create new CU*BASE features that compete with standalone systems to detect potentially fraudulent activity
- **Proactively stop transactions vs. reviewing losses after the fact**

WHAT WE WILL DO (APRIL 2019)

- Identify places, actions, members, and people who are problematic
- Create a database for blocking services and transactions and encourage credit unions to use the new fraud database (released in 19.05)
- Translate known cases into actual pattern recognition programs
- Review those identified instances (alerts)
- Update member Tracker and alert credit union for them to respond
- Automate responses to problematic situations
 - Push notifications
 - Text
 - Email
 - Deny

PLAN (APRIL 2019)

1. Build a business on working the alerts and consulting for those who decide to go it on their own
2. Using what we learned from Fortress and other vendors, create a configuration scheme and develop the first batch of rules
3. Build the engine to run the rules and create alerts
4. Create a fraud log management system to work the resulting alerts (similar to BSA monitoring)
5. Finish the fraud database and blocked lists and use what is entered as a basis for rules moving forward
6. Use what we have learned and put the most effective rules into the payment and posting streams of CU*BASE (stop fraud before it happens)
7. Use what we have learned to reduce the duplicity and drive down the log management; transfer similar logic into the BSA log file

WHAT WE OWN: INVESTMENT ONE

Tool #101 Abnormal Activity Monitoring Config

Origins	Origin Codes	Risk Level	Transaction Count		Combined Transaction Amount	
			From	To	From	To
ACH	1 selected	NORMAL	0	32	0	20,000
		ABNORMAL	33	100	20,001	50,000
		HIGH RISK	101	9,999,999	50,001	999,999,999
ATM	1 selected	NORMAL	0	60	0	8,000
		ABNORMAL	61	110	8,001	30,000
		HIGH RISK	111	9,999,999	30,001	999,999,999
AUDIO RESP	1 selected	NORMAL	0	50	0	10,000
		ABNORMAL	51	150	10,001	50,000
		HIGH RISK	151	9,999,999	50,001	999,999,999
CREDIT CRD	1 selected	NORMAL	0	50	0	10,000
		ABNORMAL	51	100	10,001	20,000
		HIGH RISK	101	9,999,999	20,001	999,999,999
DEBIT	1 selected	NORMAL	0	75	0	5,000
		ABNORMAL	76	125	5,001	12,500
		HIGH RISK	126	9,999,999	12,501	999,999,999

WHAT IT DOES

Tool #537 Monitor Abnormal Transaction Activity

File Edit Tools Help

Monitor Abnormal Activity View All Risk Levels

Member group to monitor: INDIVIDUAL

Monitoring settings are based on a date range of 1 month of activity

Monitor transactions from:

Include all activity for members with Due Diligence flag

Flag if member age is below or above

* Highlighted name = Employee

Age *	Origin	# Trans	Trans Dollars	Trans Dollars	Risk Level	Last AT Tkr	By
75	ACH NETW	11	106,475	9,679	HIGH RISK	OP 11/24/18	99
62	AUDIO RE	16	83,700	5,231	HIGH RISK	OP 11/24/18	99
63	AUDIO RE	18	77,808	4,322	HIGH RISK	OP 11/24/18	99
56	AUDIO RE	4	56,000	14,000	HIGH RISK	OP 11/24/18	99
26	CREDIT C	124	1,840	14	HIGH RISK	OP 11/24/18	99
26	AUDIO RE	158	19,180	121	HIGH RISK	OP 11/24/18	99
72	ATM NETW	5	80,900	16,180	HIGH RISK	OP 11/24/18	99
53	ACH NETW	8	99,719	12,464	HIGH RISK	OP 11/24/18	99
53	AUDIO RE	4	181,978	45,494	HIGH RISK	OP 11/24/18	99
52	AUDIO RE	4	86,200	21,550	HIGH RISK	OP 11/24/18	99
36	AUDIO RE	12	81,502	6,791	HIGH RISK	OP 11/24/18	99
47	AUDIO RE	52	59,400	1,142	HIGH RISK	OP 11/24/18	99
41	AUDIO RE	26	225,604	8,677	HIGH RISK	OP 11/24/18	99
60	ATM NETW	128	3,938	30	HIGH RISK	OP 11/24/18	99
27	ATM NETW	112	5,789	51	HIGH RISK	OP 11/24/18	99
21	ATM NETW	126	4,420	35	HIGH RISK	OP 11/24/18	99

WHAT WE ARE DOING

- Learn from findings
 - Use to build new pattern recognition
- Build a share execution business to drive down the cost of the regulatory burden
 - Become practitioners and experts in the field of fraud mitigation and management
 - Answer the question on exam checklist “ongoing monitoring”
 - Reduce pressures to buy ancillary systems

INVESTMENT TWO: FRAUD DATABASE

Tool #1710 Fraud Incident Dashboard

Fraud Incidents								VIEW
# Fraud types		7						
Fraud Type	Last Fraud Date	# Events	Fraud Amount	Pct	Provisional Credit Amount	Pct	Recovery Amount	Pct
WIRE FRAUD	09/28/20	1	15,000.00	52.5	.00	.0	15,000.00	97.8
DEBIT CARD FRAUD-CONSUMER	10/19/20	75	5,187.48	18.2	.00	.0	.00	.0
CREDIT CARD FRAUD-LOW RAT	10/14/20	14	3,067.23	10.7	.00	.0	.00	.0
UNEMPLOYMENT FRAUD RETUR	09/29/20	2	2,438.00	8.5	.00	.0	.00	.0
CREDIT CARD FRAUD-REWARDS	10/01/20	9	1,332.60	4.7	.00	.0	344.08	2.2
REMOTE DEPOSIT CAPTURE FR	08/31/20	1	950.00	3.3	.00	.0	.00	.0
DEBIT CARD FRAUD-BUSINESS	09/26/20	2	592.29	2.1	.00	.0	.00	.0

- Designed to shine a light on the types and amounts of fraud
 - Member level
 - Credit union level
- Give C-level and fraud managers an overview of losses with a push of a button
- Build a community of practitioners to create a broad database to build new and effective functionality – guaranteeing wise future investments

INVESTMENT THREE: BLOCK LISTS

Tool #892/#1892 Update Fraud Alert/Blocked Persons Lists

- 9 new Block Lists (released 20.11)
- Primarily designed to mitigate fraud for fringe memberships but also incorporated existing “no future membership” list
- Designed to STOP – CHECK – NO – GO
- Two types:
 - Denial of Service (DOS)
 - Denial of Transaction (DOT) based on specific attributes

DENIAL OF SERVICE (DOS) BLOCKS

- Opening a new membership, adding non-member record, or opening a pre membership loan
- Enrolling in bill pay
- P2P
- Online/mobile banking
- Plastics ordering
- Incoming wires
- Outgoing wires

PRACTICAL APPLICATIONS

MEMBERSHIP DENIAL

- What's changed? Nothing just a different location
- Generally used when a member has caused the credit union a loss or had extreme high-risk activity that warrants the closing of the account
- Scans are completed when:
 - 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 via Tool #53 Process Member Applications (or Tool #2 Work/View Loan Application Status)
 - 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

PRACTICAL APPLICATIONS

DOS - P2P & BILL PAY

- Generally used when member credentials have been compromised, either through social engineering or malicious attack on a PC or other personal device and caused the credit union a loss
- Prevents them from re-enrolling after you have taken away access, or from granting access if opening a new membership
- Scans are completed when:
 - Trying to enroll member in Tool #14 Member Personal Banker
 - During account opening process if in workflow configuration
 - Member tries to enroll in online or mobile banking
- Hard stop – credit union must remove from list in order to allow enrollment

PRACTICAL APPLICATIONS

DOS - HOME BANKING

- Generally would be used when a member's account is taken over and credit union is fearful that non-public information will be exposed
- This is completed after you remove access from the Update Online Banking Access screen (PIN)
- Scans are completed when:
 - Employee attempts to enroll member in online banking via Tool #14 Member Personal Banker or directly using the PIN shortcut
 - Employee tries to reset password
- Remember to also disable See and Jump so others cannot get to the account

PRACTICAL APPLICATIONS

DOS – CARD ORDERING

- Used when members constantly lose cards, give up credentials, have been a victim of exploitation and/or caused the credit union a loss
- Scans are completed when:
 - Adding or recording a card via Tool # 11 ATM/Debit Maintenance
 - Adding a new card, adding a new emboss order, or reordering same pattern via Tool #12 Update/Order Online Credit Cards
 - Adding a plastics record via Phone Operator > OTB/Cards feature
 - Card expiration processing (Tool #147) makes card expiration non-input capable

PRACTICAL APPLICATIONS

DOS – MEMBER LOAN APPS

- Used when member has ongoing collection issues but does not cause the credit union a loss, or is deemed internally to be high risk due to deposit and other transactional activity
 - **Be careful with ECOA**
- Scans are completed when:
 - Processing member and pre-membership applications through Tool #53 or Tool #2 Work/View Loan Application Status
 - If the loan is already in the queue, staff will not be able to create loan
 - Does not prevent a member from applying online or loan going through indirect channels

PRACTICAL APPLICATIONS

WIRES IN OR OUT

- This one is geared more towards fraud management and money laundering, and members who have displayed activity deemed potentially illegal
- Scans are completed when:
 - Posting an incoming or outgoing wire through Tool #73
 - Phone operator wire nav

DENIAL OF TRANSACTION (DOT) BLOCKS

- Generally these blocks will prevent a member from sending money to someone you have already deemed belonging to an organization or individual that has defrauded other members through exploitation, account takeover, or social engineering
- Pay to name:
 - Accounts Payable quick checks (Tool #1961)
 - Miscellaneous Checks (Tool #667)
 - Checks via Teller Line Posting (Tool #1) Process code C or M
 - Phone Operator
 - Loan Disbursements (Tool #50)
 - Outgoing Wire Transfers (Tool #73)
- Country – Financial Actions Task Force (FATF) list of countries
 - Wire Transfers (Tool #73)

WHAT SHOULD YOU DO NOW

- Distribute the following to those who will be using the system
 - <https://www.cuanswers.com/wp-content/uploads/FraudBlockListsSupplementalGuide.pdf>
 - https://help.cubase.org/cubase/cubase.htm#Overview_Fraud_Block_Lists.htm
- Review whatever documentation you have been using to keep track of fringe members, including:
 - Comments in member inquiry and collections
 - Due diligence codes
 - Spreadsheets
- Make recommendations for the next set of lists to AuditLink

INVESTMENT FOUR: NEW ABNORMAL ACTIVITY MONITORING – PATTERN RECOGNITION

Project #53105 Coming in the 21.05 Release

- Learn from activities entered in the new fraud database
- Learn from activities uncovered through the use of the existing Abnormal Activity Monitoring service
- Apply what we know to real-time intervention and new log management features and business
- Develop 30 preconfigured rules out of the box
- On-the-fly run of patterns with dashboard-like queue management

THE RULES

Thinking like an auditor, rules might be categorized as follows:

- **Velocity** – transaction occurs x number of times over y period and is greater than \$z dollar amount
- **Product** – transaction on a specific product is greater than x or has occurred after x number of days of inactivity
- **Out of the ordinary** – transactions are x% greater than what is normal for the member over the past x number of days
- **Idle activity** – Member has not had a transaction on the specific product for x number of days and then has a flurry of activity
- **Cross channel** – transactions that occur and then followed by another via a different channel

THE RULES

Thinking like a software designer, rules might be categorized as follows:

- Cover as many different velocity, product, out-of-the-ordinary, and idle activity audit rule concepts as possible with flexible configuration(s)

The screenshot shows a web-based configuration interface for a rule. It includes several input fields and checkboxes. At the top, there is a 'Product(s) to watch' section with checkboxes for SH, SD, CD, IR, TX, LN, and OC. Below this, there are two rows of conditions: 'For [] or more transactions - OR - [] % increase in volume of transactions' and 'With total amount of [] or more - OR - [] % increase in trans amounts (???)'. There is an 'Include these transactions:' section with three 'Select' buttons for 'Origin code(s)', 'Tran code(s)', and 'Tran type(s)'. At the bottom, there are two more conditions: 'Compared to similar activity over the past [] days' and 'If following a period of inactivity of [] days'.

- Check for a specific sequence of transactions based on channel
 - May be more complex and therefore fewer similarities between different rules
 - Fewer config options; CU may just choose whether they want to use the rule or not
- Check against a blocked list
 - Config would likely be a simple list of choices to verify against or not

FOR EXAMPLE, TRIGGER AN ALERT IF...

Velocity and Similar		Cross-Channel
<ul style="list-style-type: none"> Member has more than 5 shared branching transactions over 3 days totaling more than \$800 Member has more than 4 ATM withdrawals over 1 day totaling more than \$600 Member has more than 5 wire transfers totaling more than \$10,000 over 30 days Member had more than 30 ACH withdrawals over a 4-day period totaling more than \$7,500 5 transactions occur totaling more than \$1,500 on a credit card after 180 days of inactivity 	<ul style="list-style-type: none"> Member has 70% more shared branch activity over the last 5 days compared to the last three-month daily average Member has 90% more teller line cash activity over the last 30 days compared to the last three-month daily average Member has 50% increase in ACH activity over the last 30 days compared to the last three-month average A transaction occurs via online banking on a HELOC totaling more than \$7,500 	<ul style="list-style-type: none"> Member had an ATM deposit totaling \$1,000 or more followed by a teller or draft withdrawal of an equal to or greater amount within three days Member had ACH deposits totaling more than \$5,000 followed by a teller withdrawal of equivalent or greater amount Member had transfers via online banking followed by an email address change followed by passthrough to bill pay Member had a credit or debit card transaction for under \$2.00 with a 'card not present' code at an out-of-state business RDC deposit matching a prior teller deposit (or vice versa)

INVESTMENT FIVE (FOR 2023): REAL-TIME INSPECTION OF ACTIVITY

- Use what we have learned and invested in over a decade to STOP-CHECK-NO-GO in a real time environment
- Create member and staff alert systems to manage and monitor high risk or fraudulent activity
- Create case management dashboard to work activity stopped or ready to be approved or denied activity
- Become the data processor to use our collective knowledge and investments to **stop losses before they happen** in a real-time environment

VISIT US AT

[HTTPS://AUDITLINKSUITE.COM/](https://auditlinksuite.com/)

AuditLink

[Why AuditLink](#)

[Who We Are](#)

[News](#)

[AuditLink Suite](#)