

# Suspicious Activity Monitoring

## Vilker's Dirty Dozen

*Detecting the Normal, the Irregular, and the Risky*

### 1. Excessive Abnormal Activity

#### "UNDERCOVER BUSINESS ACCOUNTS"

**Activity** – Member has excessive ACH activity on the account. Generally these come from ATM providers, sometimes who in fact, are members who have purchased an ATM machine to operate their own network. As consistently larger cash withdrawals are made, it's discovered that the member is using the credit union for cash inventory.

Another symptom of an "undercover business account" is excessive Pay Pal transactions which reveals a small business operation. We have, through our review of ACH activity, uncovered instances of pyramiding pay-day loans.

In many cases credit unions have no clue that excessive abnormal activity is occurring on a member account. These could be commercial accounts which fly under the radar and are used purposely to avoid the scrutiny and due diligence requirements placed on a financial institution for accounts of this type. When large withdrawals and corresponding deposits occur, flag these accounts as high risk because they are invitations for money laundering and potential for money store accounts.

**Solution** – Through system configuration, broaden the scope of reporting available. Encompass an array of account types and transactions within a specified time period.

In a configuration screen build tracking factors based on number of ACH transactions, total dollar amounts, specify timeframe (day, week, or month)

- ◇ Wire transfers in excess of X number and/or total dollars of Y during time period Z
- ◇ Deposits and withdrawals in excess of X number and/or total dollars of Y during time period Z
- ◇ Any activity at shared branches and ATMs where more than X number of shared branches and ATMs were used, totaling at least Y number of transactions over Z amount of time
- ◇ Merchant review of ACH where tracking is based on a specific merchant code, such as casinos.
- ◇ Debit Card Activity

- ◇ ACH in excess of X number and/or total dollars of Y during a time period of Z

### 2. Identity theft

**Activity** – Member has not had any activity on their line of credit (primarily Visa). A sudden onslaught of transactions in extraordinarily large amounts are one clue that this is identity theft.

This activity has the potential for both loss of the card and card information. With the stolen identity, the perpetrators often purchase gift cards from retailers which they re-sell at a discount; or they take copious cash advances which are then used to purchase high-demand, easily liquidated goods such as electronics and jewelry.

**Solution** – Track the transaction history on LOCs and create a system configuration that allows tracking of a specified number of months since last transaction. If transactions process after that time period, report any accounts having in excess of X number of transactions per day, which total at least X percentage of the specified limit or dollar amount. Flag accounts where small transactions are followed by those of sizable dollar amounts.

### 3. Check Kiting

**Activity** – Members who make deposits at one institution using funds drawn from another financial institution when that account has no balance, are guilty of Check Kiting. These members are 'playing the float'.

Viewed as suspicious in most cases, tellers are encouraged and even warranted to place extended holds on these accounts.

**Solution** – Review deposit and withdrawal activity on a checking account. When a pattern emerges where a deposit is made followed by a corresponding withdrawal within a short period of time, report these accounts as suspect. One metric to follow is when the withdrawal and deposit are within X percent (5%) of each other over an X (5) day period of time.

Check kiting can also be traced to excessive use of home banking. Another indicator is the frequent return of deposited items. Tying indicators together requires strong analysis, but is worth the investment. Whether manual or using software solutions you will apply the same investigative logic. Look backward to find how often this account

would have gone negative if the deposit had not been made within 24 hours.

#### 4. OFAC Scan: Corporate Drafts & A/P Vendor Names

**Activity** – Credit Unions are required by regulators to run a scan against the SDN list on anyone they do business with.

**Solution** – Add the OFAC Scan operation to corporate check printing and A/P Vendor Files.

#### 5. Detecting debit/credit card fraud

**Activity** – Member(s) card(s) are compromised

**Solution** – Create a flexible system configuration for the credit union to specify conditions to monitor as noted in the following situations.

- ◇ Excessive PIN failure (not sure how we would know this)
- ◇ Distance between transactions on any given day exceeds X number of miles
- ◇ Accounts that have had no activity for X number of days or months suddenly have Y number of transactions
- ◇ Excessive cash withdrawals or cash advances
- ◇ Members over the age of X have more than Y transactions. (e.g. Elder or minor abuse)

#### 6. BSA—ATM Activity

**Activity** – Member makes all deposits and withdrawals at the ATM to avoid the scrutiny of the BSA tracking system.

**Solution** – Change the system to monitor for ATM cash activity in the BSA file.

Similar to the manner in which we added shared branching activity we should also include ATM activity in the BSA file.

#### 7. BSA—Joint Owner Activity

**Activity** – Member avoids currency transaction monitoring by depositing cash into multiple accounts, some on which the member is the primary owner, others listed only as joint owner.

**Solution** – Enhance the BSA monitoring feature to include the ability to track every account, connected to the social security number of every member, regardless of classification: Primary Owner or Joint Owner.

#### 8. BSA—Layering

**Activity** – Member gets a line of credit, uses it for a cash advance, then wires the money out of the credit union; or they purchase gift cards through the miscellaneous receipts process.

Member then makes large payments on the loan and each time the available limit grows, another wire transfer is made. Many times it is a foreign wire. If the member receives the disbursement via cash, our

BSA monitoring system picks it up and there's a record of the transaction. Consequently the activity is the transfer to the wire G/L.

**Solution** – Review transactions on member LOCs against the wire transfer log and miscellaneous receipts log.

#### 9. Accounts with wrong address

**Activity** – A member account, even though flagged as having a wrong address, is still processing transactions against the account. However, the member is not receiving a statement that shows transactions are being performed.

**Solution** – Generate a daily report or set up a screen similar to the dormancy monitoring screen which would allow the credit union to review these high risk transactions.

#### 10. Critical field monitoring

**Activity** – Currently credit unions must review the file maintenance logs to determine if the changes made to member accounts were completed correctly and with the proper authority.

**Solution** – Create a screen where the credit union could chose up to 15 different critical system fields which currently show on the file maintenance log. At the end of the day, populate a screen similar to the one used for BSA daily monitoring where the credit union would work these changes in real time.

#### 11. New Notice Events: Compliance Related

**Activity** – Members do not know when they go dormant and they become aware of it only when they are charged a dormancy fee.

**Solution** – Create a configurable notice that would be generated and sent to the member alerting them that their account has gone dormant. The credit union could potentially use this notice instead of sending out notices by hand.

**Activity** – When a member has a new address we do not send a notice to both the new and old address.

**Solution** – At time the address is changed send the notice to both the old and the new address.

#### 12. FinCen

**Activity** – Credit unions are required to extract the FinCen report and **visually** compare the reported list of names to see if any members are on the list.

**Solution** – Pull the file into CU\*BASE and automate a scan similar to the manner in which the credit union performs the OFAC check.

#### Jim Vilker, NCCO

VP of Professional Services  
CU\*Answers / Xtend  
Audit Link

advisor.cuanswers.com  
ms.cuanswers.com  
cuasterisk.com

