MACPAGE™

Accessible
Approachable
Accountable

# Fraud in Credit Unions

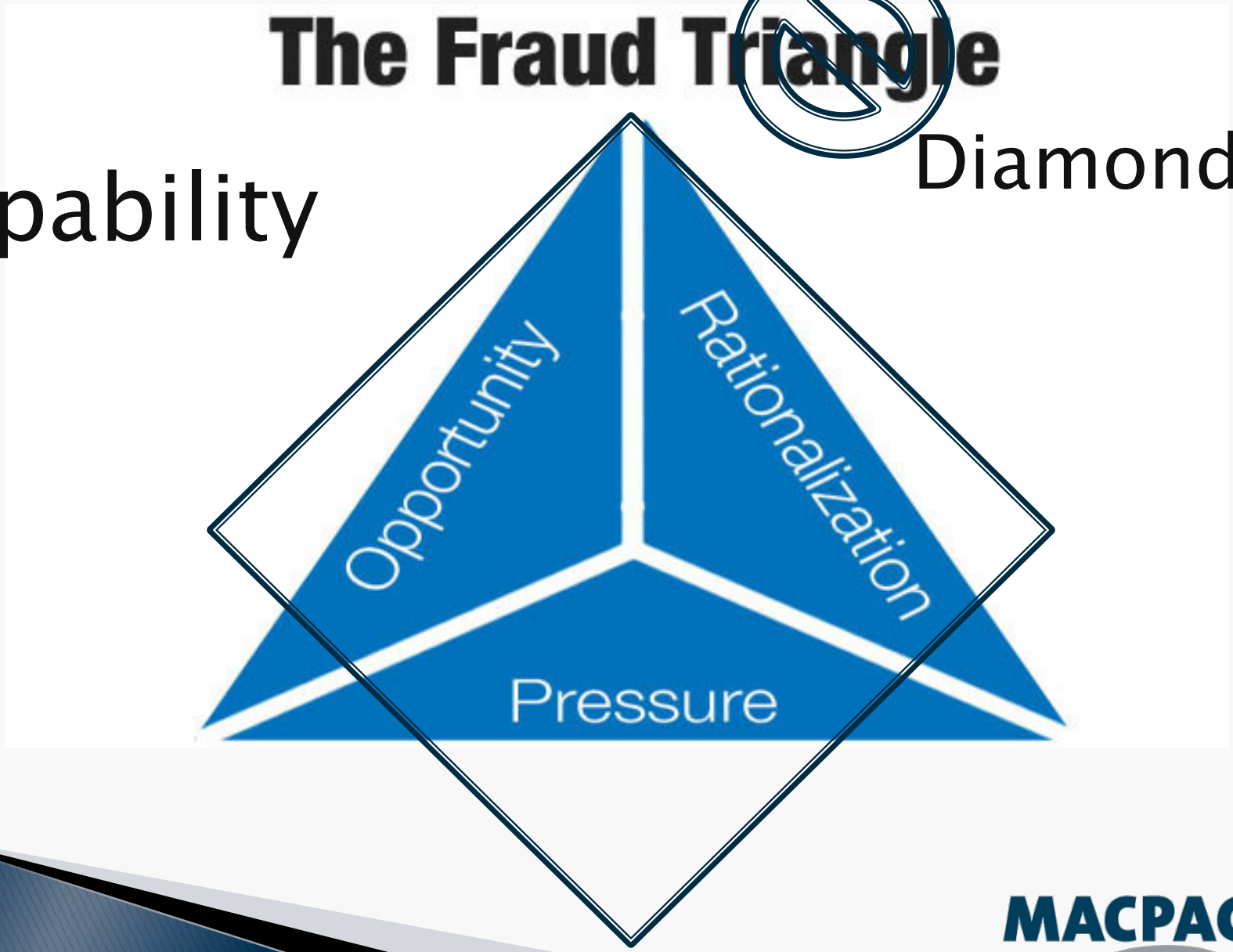
Presented by:

Michael Moreau, CFE, CIA, CFSA
Manager, Credit Union Group
Macpage LLC
mpm@macpage.com
978-760-0195

# The Fraud Triangle


MACPAGE™

# The Fraud Triangle




Capability

Diamond

MACPAGE™

- Capability – can they do it?
  - Necessary position and authority
  - Sufficient understanding of systems and processing?
  - Able to handle the stress of deceit?
  - Is it in their nature?

# Recent Frauds and Fraud Trends

- Fraudulent Loans

- Ohio man, California woman.  She works at a CU, as a business loan processor.
- Ultimately, she opened 30 lines of credit for him, totaling almost $3 million in lines, and ending up with more than $1.2 million in losses.

The two were involved in a long-distance romantic relationship, carried out through text messages (  ) and other communications.

He would send her gifts and checks, and suggest he would take her on trips, in exchange for bypassing the necessary approvals at the CU to open unsecured lines of credit.

On text read ““I just got everything omg…..Why is there a check with my name on it???? I love the card by the way…. Going down to the branch let me see what I can get done for you…$200 in your personal account, right?”

To which he replied ““Thanks my baby. The cashiers check is my show of appreciation and love for u…..”.

- He provided her with information about business and persons, including names and Social Security Numbers, without their knowledge or consent”.
- At one point, she texted him “I have too much access here :) “
- She used her access to increase the credit lines to $100,000 , double the CU’s limit.
- He never made one payment on any line.

- She omitted the loans from reports and task lists.
- She didn’t forward the underwriting documents to her supervisors.
- She would email underwriting information to her home, so she could work without supervision.

- Unable to determine how the scheme was ultimately discovered.

- However, could have been one of several ways:

- 30 loans appear on a delinquency report.
- Analytics – 30 first-payment defaults, processed by the same loan processor.

- Control breakdowns (or lack of controls):
  - No one looking at a new loan report?
  - QC was not performed, or was performed only on loans provided by the processors?
  - No one looking at a file maintenance report to identify the changes made to the credit lines?
  - No one reviewing an excessive line report?
  - No system control or review to identify/prevent large outgoing email attachments?
  - Excessive access – able to underwrite, approve, set up, and disburse loans, and also perform file maintenance?

# Another Loan Scheme

- Man opened an account at one CU, as the sole owner of an auto dealership. He provided a false document from the IRS, including his (fraudulent) tax ID number.
- Recruited a dozen people to apply for auto loans (in their own names) at other CUs, providing them with fraudulent documents for addresses, employment, and paystubs. Also provided fraudulent paperwork showing autos purchased at auctions.

- Any independent verification of the applicant's identification (eFunds, etc.) may have reported mismatches in addresses.
- If ID address did not match given address, secondary verification of address (utility bill, etc.)?

# Teller Fraud

- Teller identified accounts that had infrequent transactions.  Teller performed unauthorized cash withdrawals, issued official checks, then cashed the checks out of his teller drawer.
- Posted fictitious deposits to member accounts.
- Changed addresses to keep members from receiving statements.
- Allegedly stole $527,000 over 4 years.
- Authorities did not release how the alleged crimes were discovered.

- Could have been detected by:
  - File maintenance review of address changes, and/or address change verifications (sent to the old address).

# CEO Embezzles $718,000

- CU had $231 million in assets.
- Forged a vendor's service contract and special purchase authorization for an "employment incentive". Also altered CU records to disguise the payments. A check was issued for more than $30,000 , to pay for his wife's birthday party.
- Forged a service contract for a fake vendor, then forged a reimbursement form, to pay his credit card bills, for more than $34,000 .

- Altered Board of Director meeting minutes, forged bank statements, and forged a letter to disguise a payment as a donation to a soup kitchen.  Payment was actually to fund a $25,000 golf sponsorship.
- Forged the signature of a Board member on a payment approval form, to funnel $18,650 to pay his tuition at Temple University.

- Possible ways to detect:
  - Compare budget to actual
  - Independent set up/review of new vendors
  - Independent review of all CU checks over $X.

# It Gets Worse!

- CEO rigged elections, electing and then impersonating fictitious members of the Board and Supervisory Committee.

# CEO Fraud

- CEO of a $12 million credit union:
  - Embezzled more than $1.6 million to buy real estate and pay credit card bills that resulted from a shopping obsession.

- Raided teller cash, created fake loans, processed unauthorized financial transactions, and posted false entries in the CU's accounting records.
- Created fictitious transactions in the general ledger, then corrected the entries my making miscellaneous journal entries, where the offset was her personal account.
- To secure $248,000 in loan advances, she used, without authorization, the shares IN HER MOM'S ACCOUNT.

# Possible Detection

- Regularly review the accounts of insiders and relatives.
- Mandatory vacation policy – someone else must do the job – work can't pile up to be completed by the vacationing employee when they return.
- If volunteers are performing the account reviews, ensure they are knowledgeable about what to look for.

# Abandoned Checks

- VP of Accounting and IT manipulated controls to embezzle more than $1.2 million.
- Identified unclaimed checks, cancelled them, and reissued new checks to pay her personal bills.
- Lack of segregation of duties let to VP controlling the entire process.

- Need to track aged checks (starting at approximately 6 months of age). Checks clearing after this time should be reviewed for propriety.
- Consider transferring outstanding check amounts to an accounts payable account, to reduce the number of employees able to manipulate these checks.
- System access controls – limit who is able to cancel and reissue checks.

# Loan Fraud

- Business relationship manager, commercial loans, embezzled funds, created fraudulent loans, paid loans through the misapplication of funds from other loans, increased credit lines on unapproved loans, issued undocumented business loans, issued undocumented letters of credit.

- Direct criminal losses to the CU were more than $13.7 million.

- Employee presented CU executives with Excel spreadsheets, not supported by, or instead of, system loan reports.

- Non-system reports should be supported by system reports.  If not, ask for them.  If not accurate or available, this should be investigated.
- Review new loan reports for propriety.
- Review new loans on a sample basis for propriety of loan documentation.
- Review and test increases in credit limits.
- Review reports of new letters of credit.

# Fraud by CFO

- In 13 years, CFO embezzled $18.6 million from his $68 million credit union.
- Stole more than $2.5 million by issuing cashier's checks without authorization, and depositing them into his personal accounts at other financial institutions.
- Stole more than $16.1 million by conducting ACH withdrawals from the CU's accounts, to his personal accounts. Set up ACH withdrawals to withdraw funds from the CU's Investment accounts (which he was responsible for reconciling).

# Concealment

- CFO created fictitious investments (certificates, bonds) at another institution.

# How Could It Have Been Prevented/Detected?

- Independent verification/confirmation of investments/deposits.
- Independent reconciliation of CU's accounts.
- Segregation of duties for issuing CU checks.

# Manager Embezzles Nearly $2 Million

- Manager embezzled nearly $2 million from a $17 million CU over 17 years.
- Needed money to pay bills, so took $2,000 from the cash vault, under her control.
- Gave cash to tellers to deposit to family members' accounts.

# Detection

- Finally detected by an independent auditor performing an annual audit.

# Preventing/Detecting

- Periodic, independent cash counts (balanced to system reports/balances).
- Independent review of insider/related party accounts.
- Possible dual control over main cash supply.

# Construction Mortgage Fraud

- Borrower building $1.6 million house. Bank provided a $1.6 million construction loan, and used $1.15 million to pay off the previous construction loan.
- Remaining $450,000 was to be used to complete the house. Invoices and lien waivers were to be submitted prior to disbursement.

- Twelve false invoices and lien waivers were submitted, and disbursements made to the borrower's bank account.
- Borrower ultimately stopped building efforts.
- Bank took a $782, 349 loss after the sale of the partially completed project. This included payments of $103,257 to settle mechanic liens placed by contractors who were not paid.

# Controls to Detect/Prevent?

- Site inspections to verify work has been completed.
- Disbursement checks made payable to the borrower AND the contractor.
- Construction loan to 100% LTV??

# Fraud by Bank Branch Manager

- Branch Manager was able to identify both inactive accounts and accounts where activity was not being monitored  by the owners.
- Was able to embezzle $967,573 from these accounts.

- Would have been identified by a review of reactivated accounts/review of subsequent activity on recently reactivated accounts.

# Fraud by Loan Officer

- Loan officer had loan approval authority, and, when authorized by members, authority to
  - Make withdrawals from their accounts
  - Transfer funds among their accounts
  - Increase the amount of their loan accounts
  - Open new loans in their name

  Without the members' knowledge, the employee added to loan amounts and opened new loans in their names, and used the proceeds to pay her personal debts and partial payment for the purchase of a home.

- Loan Officer was able to conceal her fraudulent activity by moving funds among members' accounts, to make it appear as if loans had been repaid, or funds replaced.

# Prevention/Detection?

- Appears to be a lack of segregation of duties. It appears the Loan Officer was able to “take an application” for a new loan or a loan increase, underwrite, approve, and disburse.

# Lack of Segregation of Duties

- Loss to the credit union of $300,000+.
- Small CU, individuals with multiple, conflicting duties.
- Employee had system access to:
  - Open accounts
  - Open new member loans
  - Perform monetary transfers between member accounts
  - Issue cashier's checks, including access to check stock

- Originate ACH transactions
- Post to G/L accounts
- File maintenance, including names, addresses, account statement codes, and Social Security Numbers.

- And the kitchen sink.

Yikes!

- Employee had committed a small original fraud due to a financial hardship, of course with the intention of paying it back. However, since the first fraud was easy, AND was never detected, she committed fraudulent acts for years, undetected, until the CU began investigating a stale-dated $20,000 reconciling item in the G/L.

# How Did She Do It?

- Opened a fake account in the name of a CU member with health issues.  She knew the member would not identify unusual activity in the member's account.
- Changed the last name on the account by a single letter.
- Changed the Social Security Number by two digits.
- Changed the mailing address to a PO box.

- All above info would be changed just before the statement cutoff date, then change it back immediately after statement date.
- Opened a number of fraudulent loans, depositing the proceeds to the controlled account.
- Set up ACH transfers to transfer funds to her personal accounts at other financial institutions.

- Identified and took over dormant accounts, and created fictitious loans for these members, again transferring the proceeds to herself via ACH, or with fraudulent checks.
- Used a system module to process changes, move money between accounts, and generate ACHs, that did not track transactions by teller number, so the transactions were difficult to track back to the employee.

- Used G/l suspense accounts to purchase cashier's checks payable to other banks.  Her account information was handwritten on the checks, so the system did not include her account information.  These items eventually showed up as stale dated items on reconcilements.
- Items were researched, BUT

- You guessed it, our perpetrator was charged with researching the reconciling items. Items were cleared using funds from the various fictitious accounts she controlled.
- The CU eventually made some changes to the systems, including limiting the access to open new loan accounts. Since this was the primary source of new funds, these changes ultimately led to the discovery of the fraud.

# Preventative/Detective Controls?

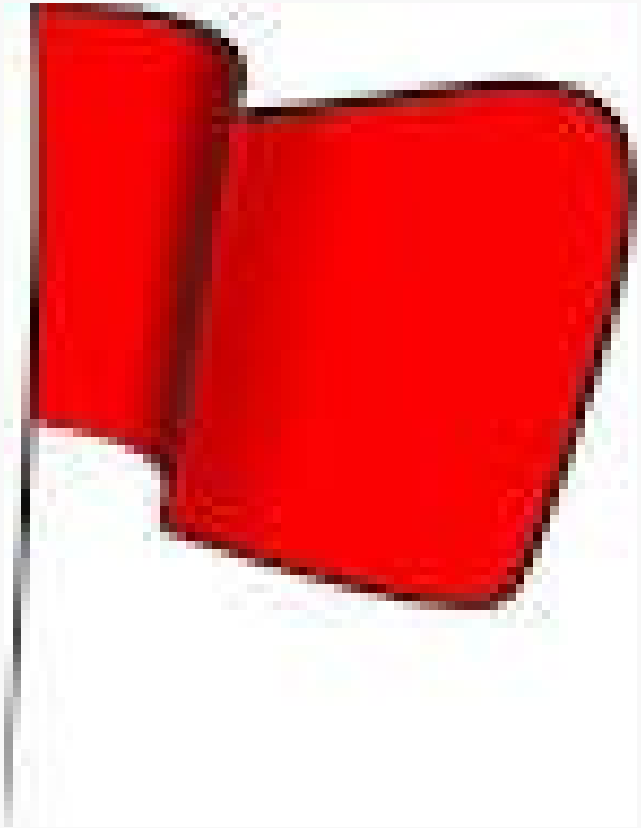
- Obviously, limit access and implement segregation of duties as much as possible.
- Independent review of the new loan report.
- Independent review of file maintenance. Recall that maintenance was happening right before and after the statement cutoff date.

# Loan Fraud

- A couple, who managed a credit union, embezzled $2 million from the credit union, to support three successful business ventures.  Mr. was the president, and Mrs. Was the CU manager.

- Submitted false loan applications, using fictitious names, along with falsified personal, employment, and income information.
- In their capacities at the credit union, approved the loans despite knowing the information in the loan applications were false.

- In 2011, an NCUA examiner questioned management about the loans. Rather than answering the questions, management forced the examiner to leave the credit union, and resisted subsequent attempts by the NCUA to re-enter the credit union



- When NCUA finally got back in to the credit union, management indicated that some of the critical documents had inadvertently been shredded.

- Collusion – can be very difficult to detect.
- Segregation of duties – too much control concentrated in too few positions.

- Anyone have any good fraud stories we can learn from?

Michael Moreau, CFE, CIA, CFSA
Manager, Credit Union Group
Macpage LLC
mpm@macpage.com
978-760-0195