



# FRAUD TRENDS TO WATCH FOR IN 2018

Presented by:  
Daniel J. Mahalak

# Session Overview

In recent years, fraud has seemingly been increasing in credit unions. Some of this fraud is related to the technology in use today and the lack of member awareness of the activity in their accounts. Some of it is done the old-fashioned way, through internal theft or misstatement of financial statements.

However it happens, the risk has increased in credit unions. We will discuss what you can look for to attempt to prevent or at least detect it when it happens.

Your credit union will never be fully protected, but awareness of what has happened in other organizations can help in your reviews. Keeping your eyes open can always help

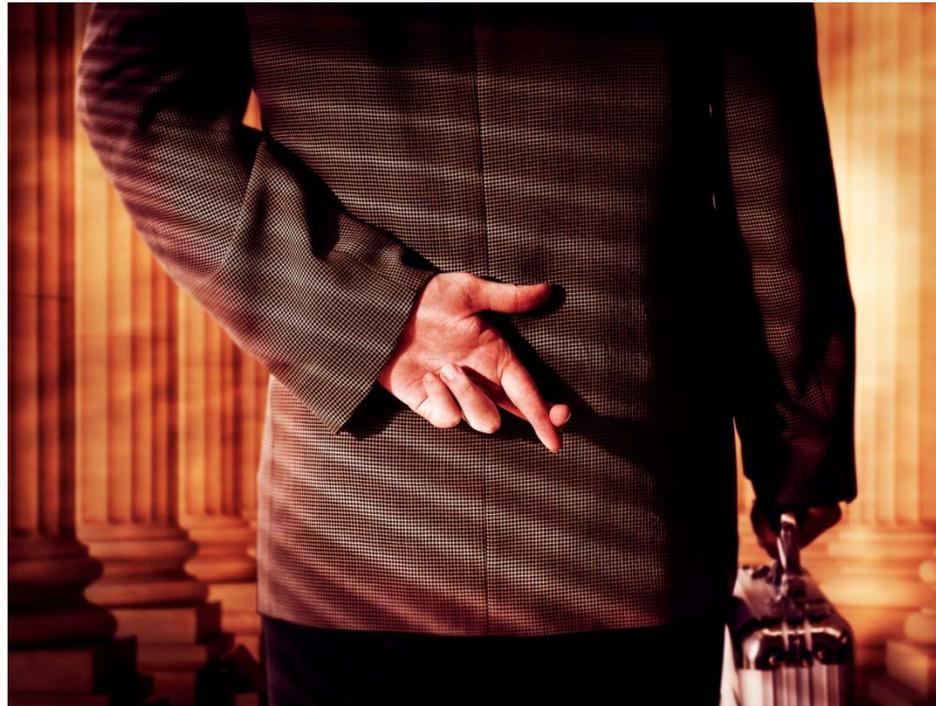
# Agenda

- Revisiting fraud definition
- Types of fraud
- Fraud statistics and trends
- Where is the risk?
- Prevention, detection, deterrence
- Types of fraud occurring at credit unions
- Questions

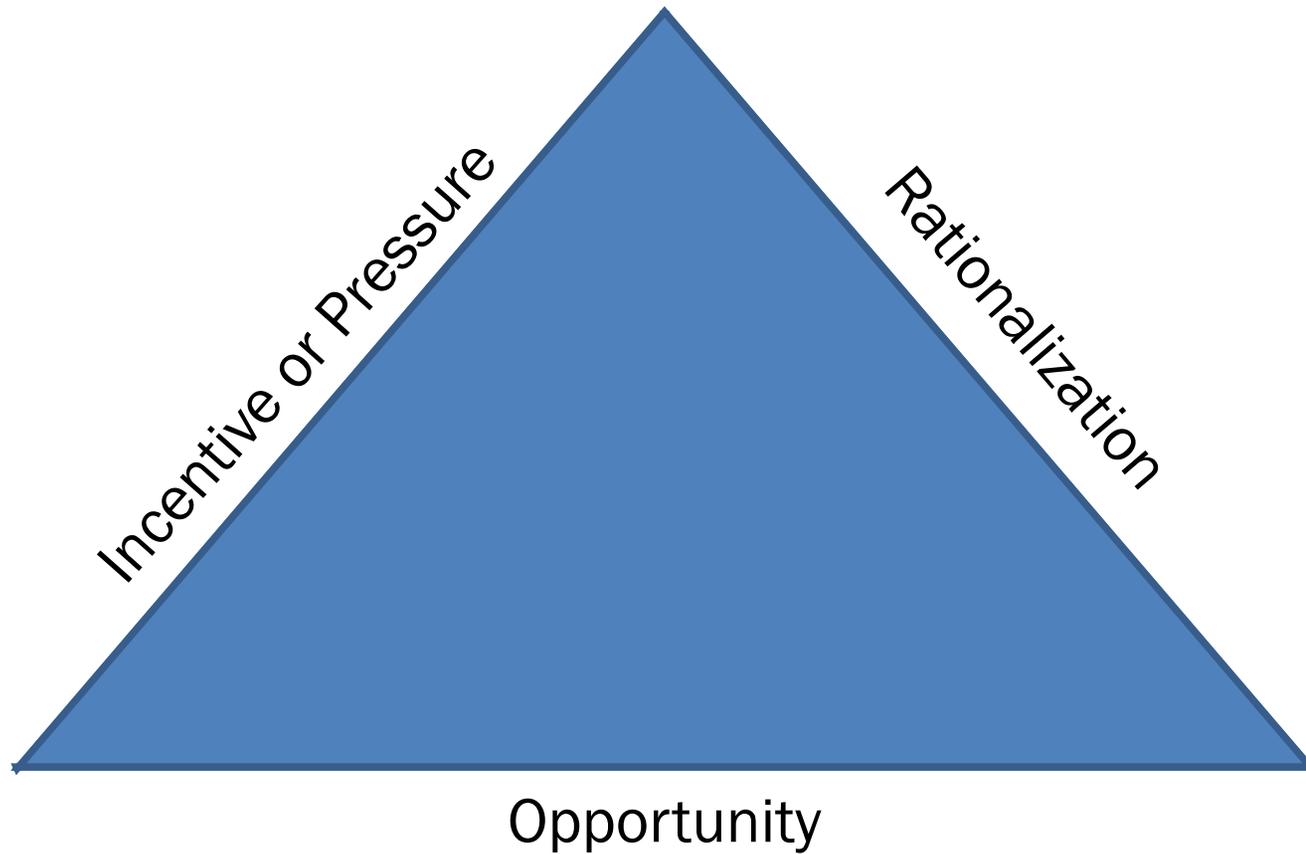


# Fraud Defined

- Act or course of deception, an intentional concealment, omission, or perversion of truth, to gain unlawful or unfair advantage, induce another to part with some valuable item or surrender a legal right, or inflict injury in some manner.



# The Fraud Triangle



# NCUA Concerns

- Regulators are continuing to evaluate the adequacy of internal controls and efforts to prevent and control fraud
- This is the result of recent frauds in CU industry
- CUs with limited staff more susceptible to internal fraud
  - *Inherent risk due to size*
  - *Lack of segregation of duties*

# Types of Fraud

- Fraudulent financial reporting
  - *Internal*
- Misappropriation of assets
  - *Theft or embezzlement*
    - Internal or external
  - *Insider dishonesty*
    - Internal
  - *Identity fraud*
    - Internal or external

# How is Fraud Detected

- Tip 39.1%
- Internal audit 16.5%
- Management review 13.4%
- By accident 5.6%
- Account reconciliation 5.5%
- Other 5.5%
- Document examination 3.8%
- External audit 3.8%
- Notified by law enforcement 2.4%
- Surveillance or monitoring 1.9%
- IT controls 1.3%
- Confession 1.3%

# Statistics

- 10% of instances are fraudulent financial reporting
  - *But account for 80 – 90% of dollars*
- 90% of instances are misappropriation of assets
  - *But account for 10 – 20% of dollars*
- 60% of frauds occur in the revenue cycle in most businesses
  - *This is different in financial institutions*
- Biggest risk is with most experienced staff
- Biggest losses are in frauds that run the longest

# Synthetic Identity Fraud

- Fraudsters open DDA account
  - *Establish consumer profile*
  - *Process small transactions*
  - *Apply for credit later, sometimes much later*
- Pick random social security numbers and use them for other purposes such as cell phone contracts
- Open multiple accounts using same address or adjacent addresses at multiple institutions

# Payment Fraud

- Losses increasing
  - *Signature based debit cards*
  - *PIN based debit cards*
  - *Credit cards*
- Losses also higher in paper checks, wire transfers, and prepaid cards
- 65% of respondents to a recent survey said they outsource debit card fraud management
  - *Thus they have no internal expertise on this topic*

# Fraudulent Financial Reporting

- Manipulation, falsification, or alteration of accounting records or supporting documents from which financial statements are prepared
- Misrepresentation in or intentional omission from the financial statements of events, transactions, or other significant information
- Intentional misapplication of accounting principles related to amounts, classification, manner of presentation, or disclosure

# Recent Credit Union Frauds

- Over \$1 million in auto loans and \$1.5 million in home equity lines taken by 3 people from 15 credit unions and 3 banks
  - *Fake online loan applications using 30 people they recruited for this purpose*
  - *Fraudulently repaired their credit reports*
  - *Fake employment and income information*
  - *Bogus information about cars to be purchased*
  - *Created auto dealerships as a front, including websites, bank accounts, purchase orders, etc.*
  - *When loans defaulted, borrowers claimed identity theft*

# Recent Credit Union Frauds

- Theft of CU assets (member money)
  - *Cash*
  - *Loans*
  - *Equipment*
- Overstatement of expenses and/or assets
- Understatement of expenses and/or liabilities
- Overstatement of income

# Theft of Assets

- Cash taken from teller drawers, vault, dispensers, ATM
- Funds taken via ACH, wire transfer, check
- Fictitious loans
- Modified loans
- Loans outside of policy, good business judgement
- Theft of computer equipment, furniture, etc.
- Corporate credit card abuse

# Where is the Risk?

- Changes in personal lives of employees
- Wage increases lower than anticipated
- Benefit programs reduced
- Access to areas of operation outside of their responsibility

# Fraudulent Financial Reporting

- Lower than expected profitability
- Higher loan losses & delinquency
- Declining collateral values
- Tighter interest margins
- Declining net worth
- Incentive plans
- Regulatory pressure

# Where is the Risk?

- Lack of segregation of duties
- Dominant senior management
- High turnover in management staff
- Weak or ineffective management
- Weak accounting controls
- Inadequate monitoring of controls
- Significant unsupported transactions
- Override of internal controls

# Where is the Risk?

- Incentive plan tied to operating results
- Dramatic change in profit/net worth
- Actual results far less than budget
- Board pressure for unrealistic results or improvement
- Regulatory pressure

# Prevent - Detect - Deter

- Internal controls should be designed to prevent, detect, and deter fraud
  - *Prevention is not always possible*
  - *You can deter honest folks from crossing the line*
  - *Detection is necessary*



# How to Fight Fraud

- Strengthen internal controls
- Control objectives
  - *Existence*
  - *Occurrence*
  - *Completeness*
  - *Valuation*
  - *Rights and obligations*
  - *Presentation and disclosure*
  - *Reasonableness*

# How to Fight Fraud

- Key control elements
  - *Segregation of duties*
  - *Dual control*
  - *Authorization of transactions*
  - *Retention of records*
  - *Supervision or monitoring of operations*
  - *Physical safeguards*
  - *Analysis of results*
  - *Information technology security*

# How to Fight Fraud

- IT security
  - *Password controls*
  - *Restricted access*
  - *Physical security*
  - *Independent of other departments*
  - *Effective monitoring systems*

# How to Fight Fraud

- Organizational “tone at the top”
- Code of conduct
- Internal audit
- Effective board of directors and audit committee
- Respond to internal/external audit reports
- Respond to regulatory exam reports

# What Can You Do

- Effectively oversee management
- Understand the credit union business
- Realistically assess risk
- Maintain skepticism
- Presume dishonesty
- Ask questions

# Where is Biggest Risk of Fraud

- Weak or non-existent internal controls
- Employees feel they are not compensated fairly
- Many electronic transactions
- “Tone at the top” is not one of integrity

# Security as a Differentiator

- Financial institutions that implement effective fraud solutions that mitigate risk in real time will be ahead of the competition
- Members must be educated as they are a part of the process, but that will give them peace of mind
- As risk evolves, the technology to detect must also
- What is normal activity for each member?
- Knowing this will help in prevention and detection.

# Real Life Stories

- Fictitious loans
- Diversion of member funds
- Fictitious investments
- False entries on bank reconciliation
- Unauthorized activity using CU funds
- Fictitious invoices
- Misstatement of financial results
- Unauthorized corporate credit card activity
- Missing cash

# Something to Remember

- Fraud risk areas are different today
  - *More electronic transactions*
  - *Better and more technology*
  - *Less loyalty*
  - *Lower morals and ethics in society*
- Members are a big part of the control system
  - *Their online access and monitoring is critical*



Thank You

# My Contact Information.....

**Daniel J. Mahalak**

[dmahalak@cm-co.com](mailto:dmahalak@cm-co.com)

Office: 586-296-1155 ext 231

Mobile: 586-899-8029