Employee Dishonesty
Lessons Learned: Internal Controls

Presented by: Doug Roossien, CRM, CFE
Business Protection Risk Management
CUNA Mutual Group

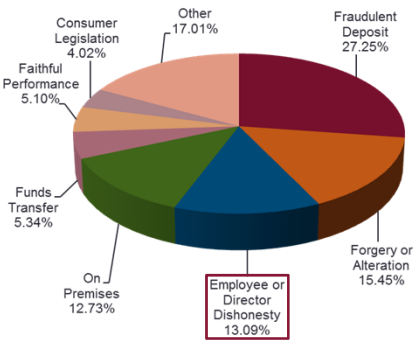
CUNA MUTUAL GROUP

Common Purpose. Uncommon Commitment.

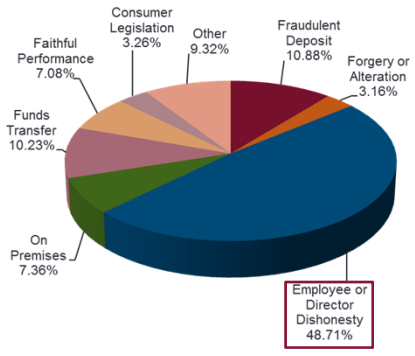
Bond Claim Trends: Incurred Losses

Embezzlement schemes are longer in length resulting in bigger losses

Bond Claim Count
(frequency)



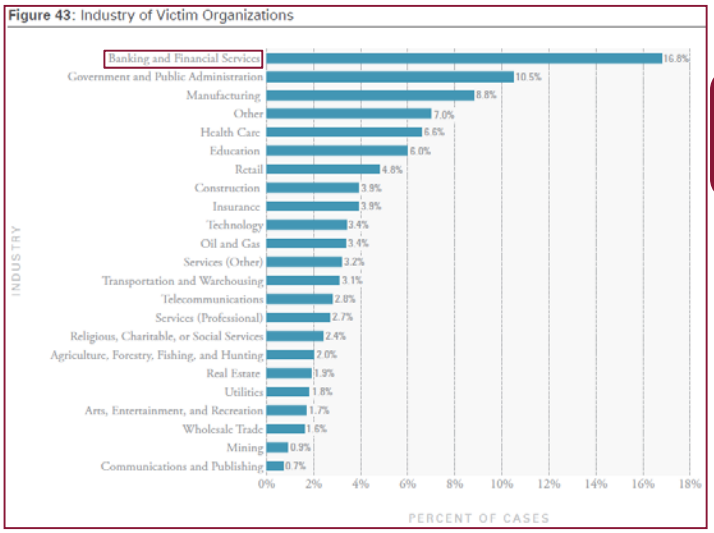
Bond Claim Dollars
(severity)



Point of Emphasis: Always consider both frequency and severity

Source: 2011-2015 CUNA Mutual Group internal claims data

Financial Services Industry
The Top Victimized Industry According to ACFE



Financial Service Industry
- Highest # of cases (368)
- Highest percentage of cases (16.8%)
- Median loss $192,000

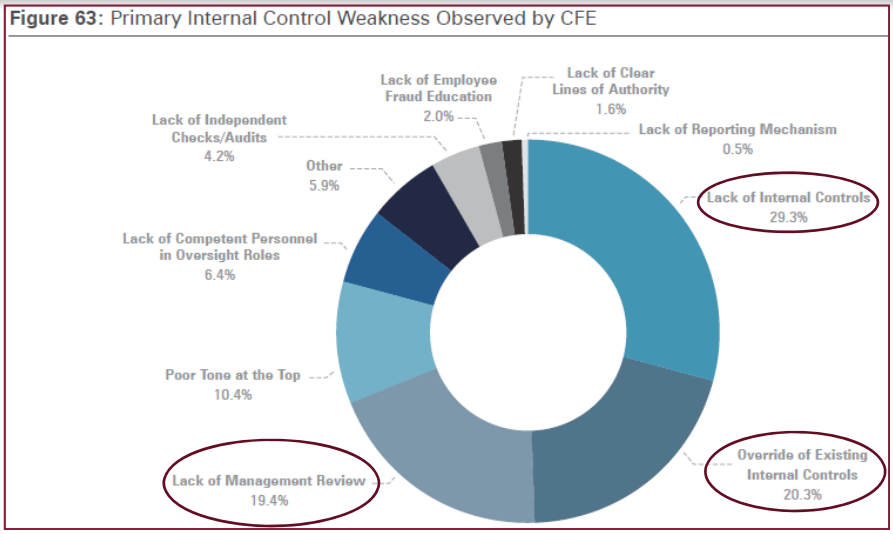
Source: 2016 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiner, Inc.

Famous Last Words

- *It could never happen to us*
- *We trust our employees*
- *All of our employees are long-term*
- *Our controls can't be circumvented*
- *We don't employ thieves*
- *We live in a smaller community and don't see that type of activity*
- *We are a small credit union*

Lack of Internal Controls is the Main Cause

Figure 63: Primary Internal Control Weakness Observed by CFE

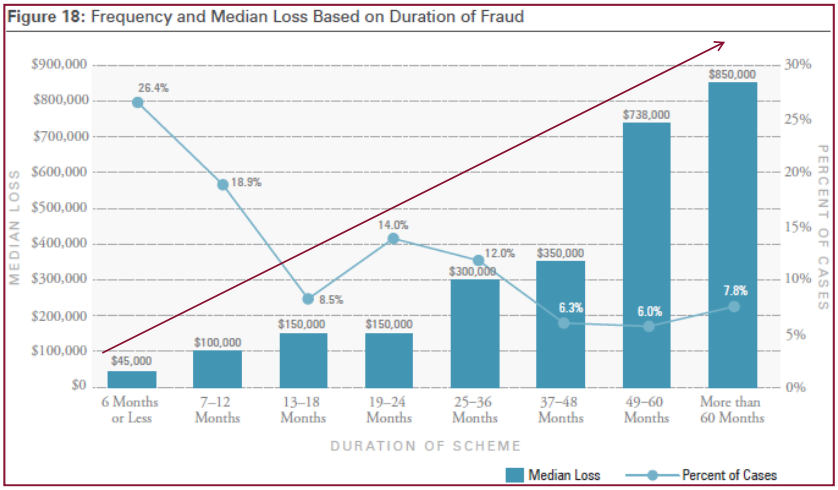


Source: 2016 Report to the Nation on Occupational Fraud and Abuse Association of Certified Fraud Examiner, Inc.

Duration and Severity of Embezzlement

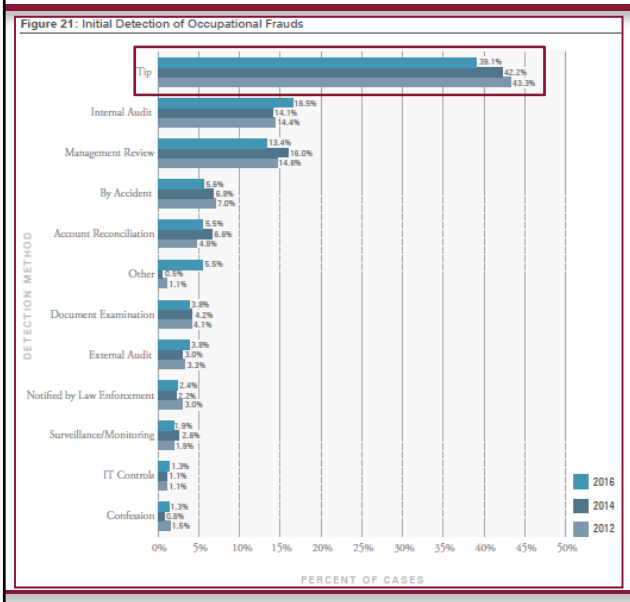
Early Detection is Critical

Figure 18: Frequency and Median Loss Based on Duration of Fraud



Source: 2016 Report to the Nation on Occupational Fraud and Abuse Association of Certified Fraud Examiner, Inc.

A Fraud Hotline Helps in the Detection Process



- Tips were the most common detection method by a wide margin, accounting for 39.1% of the cases
- Organizations that had fraud reporting hotlines were much more likely to detect fraud through tips than organizations without hotlines – 47.3% compared to 28.2%, respectively

Source: 2016 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiner, Inc.

Recipe for an Embezzlement

Traits that create a powerful temptation:

Need
(perceived financial need)

Opportunity
(weak or non-existent controls)

Rationalization
("just this once" is a way of life)

Behavioral Risk Characteristics

- Overly nervous or defensive during audits and questions – common ACFE finding
- Lives beyond their means – 45.8%
- Experiencing financial difficulties – 30%
- Unusually close association with vendors or customers – 20.1%
- Control issues (i.e., unwillingness to share duties, seldom leaves desk, or hoards data) – 15.3%

Source: 2016 Report to the Nation on Occupational Fraud and Abuse Association of Certified Fraud Examiner, Inc.

Fraud Case Study 1: Theft of Teller & Vault Cash

Perpetrator: Vault Teller
Amount: $80,000 over two years
Action: Theft of vault and teller cash

Vault teller stole $60,000 from vault cash and $20,000 from her cash drawer.
Theft discovered in January 2014 during a surprise cash count.
The last surprise cash count was in Q1 2012.

Fraud Case Study 2: Theft of Teller & Vault Cash

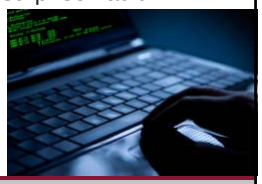
Perpetrator: Vault Teller
Amount: $120,000 over two years
Action: Theft of vault and teller cash

Stole $100,000 from her cash drawer.

She evaded detection during surprise cash counts on her drawer by making entries to sell cash to other tellers. Entries were reversed afterwards.

Stole $20,000 in vault cash by taking bait money.

Vault bait money was never included in surprise vault cash counts.

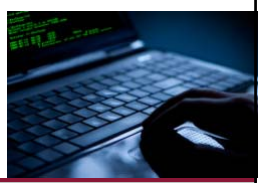


Fraud Case Study 3: Theft of Vault Cash

Perpetrator: AVP/Vault Teller
Amount: $826,000 over ten years
Action: Theft of vault cash

She evaded detection during surprise cash counts on the vault cash by making entries to sell cash to other tellers and moving funds to the ATM general ledger account.

Entries were reversed afterwards.



Fraud Case Study 4: Theft of Vault Cash

Perpetrator: Manager
Amount: $2 million over 13 years
Action: Theft of vault cash

As manager, she knew when surprise cash counts were going to take place.

She evaded detection during surprise cash counts on the vault cash by making entries to sell cash to a non-existent cash drawer.

She reversed the entries to the non-existent cash drawer after the surprise cash counts were completed transferring the balance to a suspense account.

She was responsible for reconciling GL accounts, including suspense accounts.

Relevant Internal Controls - Cash

Cash controls that could have prevented the theft or lessened the severity

- Frequent surprise cash counts
  - At least quarterly (monthly is better)
  - Random days and times (avoid patterns)
  - Include bait money
  - Reconcile count to system totals (not a manually prepared record)
- Tellers should be prohibited from:
  - Selling/buying cash to/from each other
  - Making general ledger entries reflecting buying/selling cash from/to vault
  - Block these transactions on system
- Review transactions initiated by teller or vault teller shortly before start of surprise cash audit
  - Selling cash to other tellers or the vault (if not blocked on system)
  - Transferring funds to the ATM/teller cash dispenser/teller cash recycler
  - Cash withdrawals from member accounts
- GL suspense/clearing accounts should be reconciled monthly by someone *without* GL posting authority

Fraud Case Study 5: Fictitious Loans

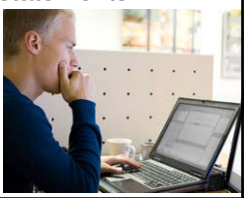
Perpetrator: VP of Lending
Amount: $250,000 over three years
Action: Fictitious loans

VP of Lending created 3 fictitious loans.
She opened the fraudulent accounts on the system.
She disbursed the loan proceeds.
She advanced due dates to prevent the loans from appearing on the delinquency report.

Fraud Case Study 6: Unauthorized Loans

Perpetrator: Loan Officer
Amount: $250,000 over two years
Action: Unauthorized loans

Unauthorized shared secured loans created on a dormant account.
Account was flagged as “Do Not Mail.”
Activities were uncovered several months later when the member called to see why statements were not being mailed.



Relevant Internal Controls - Lending

Controls that could have prevented the loan officers from embezzling or lessened the severity

- Segregation of duties in the loan department
  - Segregate loan approval from disbursement
  - Block loan officers from opening new accounts on the system
- Review file maintenance reports daily
  - Changing payment due dates
- Periodic confirmation of member loans by telephone
- Protect/monitor dormant accounts
  - Supervisory override
  - Review transactions on dormant accounts report
- "Do not mail" & "bad address" controls
  - Require a supervisory override to add these flags
  - Generate report of accounts flagged as "do not mail" and "bad address"
    - Confirm legitimacy of flag
      - Bankrupt accounts
      - Bad addresses
  - Audit transactions occurring on these accounts
- Statements mailed to branch offices
  - Generate report of accounts with statements mailed to branch offices
  - Why mailed to branch?
  - Audit transactions

Fraud Case Study 7: Visa Payments

The Den of Thieves

Perpetrator: Three employees
Amount: $750,000 over two years
Action: Visa payments

This was part of a $1 million plus claim. The employees also –
- Approved loans to themselves and family members
- Exceeded policy limits
- Some didn't even qualify
- Advanced due dates on the loans 280 times

Used credit card terminal to enter Visa payments on their credit union-issued credit cards reducing their balances.

Payments were never made.

Created out-of-balance situation for Visa loans outstanding between general ledger and card processor's records.

One of the employees was responsible for reconciling the monthly report from the card processor showing the total credit card balance outstanding.

Relevant Internal Controls – Card Department

Card department controls that could have prevented the theft or lessened the severity

- Deploy lockout feature on credit card terminal to block card department employees from processing transactions on their own credit card account and accounts belonging to their family members
- Review monthly report of employees and their family members with credit union-issued credit cards
- Audit card department employees' and their family members' credit card accounts
  - Credit limit agrees with approved limit
  - Waiving fees (e.g., late, over-limit and cash advance fees)
  - Unauthorized account reaging (advancing due dates)
- Monthly credit card report showing the total balance outstanding should be reconciled to the general ledger by someone not involved with card operations and who does not have access to the credit card terminal

Fraud Case Study 8: Theft of Equipment Purchased

Perpetrator: VP of IT
Amount: $2 million
Action: Theft of technology equipment

VP of IT purchased technology equipment (PCs, laptops, mobile devices, etc.) with credit union funds.

He performed all steps in the equipment purchase process.

He sold the equipment and pocketed the proceeds.

Relevant Internal Controls – Equipment Purchases

Controls over purchasing that could have prevented the theft or lessened the severity

- Segregation of duties
  - Purchase requisitions for equipment should be approved by a higher level of authority than the employee requesting the purchase
  - Employee requesting the purchase should not issue purchase orders to vendors
  - Employee requesting the purchase should not approve the invoice or issue payment
  - Employee requesting the purchase should not accept the shipment
- Perform periodic inventories of equipment

What can Credit Unions do?

- ❑ Implement dual control over vault cash, verifying currency shipments and replenishing ATMs/teller cash dispensers/teller cash recyclers
- ❑ Conduct frequent surprise cash audits (at least quarterly – monthly is better)
  - ❑ Don't forget about ATMs/teller cash dispensers/teller cash recyclers
- ❑ Establish controls over expenses
- ❑ File maintenance report reviews
- ❑ Audit dormant accounts
- ❑ Maintain an active Supervisory Committee
- ❑ Management/internal audit/supervisory committee review of internal controls
- ❑ Mandate employee time-off
- ❑ Maintain complete and comprehensive fraud policy
- ❑ Emphasize fraud prevention and maintain a comfortable whistleblower policy
- ❑ Perform Bondability verification and background checks

Discovery of Employee Dishonest Act

Report employee wrongdoing to CUNA Mutual Group Bondability Underwriting regardless of any loss

- The Fidelity Bond, underwritten by CUMIS Insurance Society, Inc. contains a provision (Condition 9, Subsection 1) that stipulates coverage for an employee terminates automatically when any officer, director, or supervisory staff of the credit union becomes aware of any dishonest or fraudulent acts committed by the employee, or any intentional violations of established and enforced share, deposit, or lending policies by the employee
- Problems arise when a credit union fails to notify CUNA Mutual Group and elects to retain an employee who committed a dishonest or fraudulent act
- If the employee subsequently causes a loss and it is discovered during the investigation that the employee committed a prior act, the claim may be denied

Bondability Verification & Background Checks

Today's job market can require quick hiring decisions. Bondability and background checks can help ensure job candidates will be an ideal employee or volunteer.

- CUNA Mutual Group's Bondability Verification database is only accessible to Bond Policyholders (must have username and password to access online services)
  - Contains over 40,000 individuals who lost their bondability under CUNA Mutual's Bond
- Also, conduct background checks

Session Summary

- Powerful temptation for some
- It just doesn't happen to others
- Credit unions of all asset sizes are exposed
- Simple controls and audits can be implemented
- Maintaining a good internal control environment will help prevent (but not eliminate) employee fraud

Questions & Answers

Ken Otsuka, CPA
Senior Consultant - Risk Management
CUNA Mutual Group
Email: kenneth.otsuka@cunamutual.com

Disclaimer

This presentation was created by the CUNA Mutual Group based on our experience in the credit union and insurance market. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value and implementing loss prevention techniques. No coverage is provided by this publication, nor does it replace any provisions of any insurance policy or bond.

Credit Union Loss Scenarios – Case Studies

The credit union loss scenario claim study examples do not make any representations that coverage does or does not exist for any particular claim or loss, or type of claim or loss, under any policy. Whether or not coverage exists for any particular claim or loss under any policy depends on the facts and circumstances involved in the claim or loss and all applicable policy language.

CUNA Mutual Group is the marketing name for CUNA Mutual Holding Company, a mutual insurance holding company, its subsidiaries and affiliates. Insurance products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company, members of the CUNA Mutual Group. Some coverages may not be available in all states. If a coverage is not available from one of our member companies, CUNA Mutual Insurance Agency, Inc., our insurance producer affiliate, may assist us in placing coverage with other insurance carriers in order to serve our customers' needs. For example, the Workers' Compensation Policy is underwritten by non-affiliated admitted carriers. CUMIS Specialty Insurance Company, our excess and surplus lines carrier, underwrites coverages that are not available in the admitted market. Data breach services are offered by Kroll, a member of the Altegrity family of businesses. Cyber liability may be underwritten by Beazley Insurance Group.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.

CUNA MUTUAL GROUP

Common Purpose. Uncommon Commitment.