Employee Dishonesty and Embezzlements

2015 Spring Leadership Development Conference

Presented by: Ken Otsuka
Credit Union Protection Risk Management
CUNA Mutual Group
14% of the claims filed under the Bond are for Employee Dishonesty; however, they represent 46% of the claim dollars paid.

Source: CUMIS Insurance Society, Inc.
It Could Happen at Your Credit Union

71% of the claims for losses caused by dishonest employees were submitted by credit unions that did not have any employee dishonesty claims during the prior 3 years.

Source: CUMIS Insurance Society, Inc., 2013
Financial Services Industry
The Top Victimized Industry According to ACFE

- Highest number of cases - 244
- Highest percentage – 17.8%
- Median Loss - $200,000

Source: 2014 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiner, Inc.
Sound Familiar?

• 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
Duration and Severity of Embezzlement

Early Detection is Critical

Source: 2014 Report to the Nation on Occupational Fraud and Abuse
Association of Certified Fraud Examiner, Inc.
A Fraud Hotline Helps in the Detection Process

Sources of tips:
- Employees (49%)
- Customer (21.6%)
- Anonymous (14.6%)
- Vendor (9.6%)
- Other (6.5%)
- Shareholder/owner (4.3%)
- Competitor (1.5%)

Source: 2014 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiner, Inc.
Who Commits Fraud?

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 – 43.8%
- Experiencing financial difficulties – 33%
- Unusually close association with vendors or customers – 21.8%
- Control issues (i.e., unwillingness to share duties, seldom leaves desk, or hoards data) – 21.1%

Source: 2014 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

<table>
<thead>
<tr>
<th>Perpetrator:</th>
<th>Vault Teller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount:</td>
<td>$120,000 Over Two Years</td>
</tr>
<tr>
<td>Action:</td>
<td>Theft of vault and teller cash</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Perpetrator:</th>
<th>AVP/Vault Teller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amount:</td>
<td>$826,000 Over Ten Years</td>
</tr>
<tr>
<td>Action:</td>
<td>Theft of vault cash</td>
</tr>
</tbody>
</table>

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.
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)

• Prohibit tellers 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
Fraud Case Study 4: 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 5: 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
• 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

• “Do not mail” controls
  – Require a supervisory override to add this flag
  – Generate report of accounts flagged as “do not mail”
  – Confirm “do not mail” 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 6: Visa Payments

Perpetrator: Three employees
Amount: $750,000 Over Two Years
Action: Visa payments

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.

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
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
Lack of Internal Controls is the Main Cause

Source: 2014 Report to the Nation on Occupational Fraud and Abuse
Association of Certified Fraud Examiner, Inc.
Males Embezzle More than Females

Figure 57: Gender of Perpetrator — Frequency

Figure 59: Gender of Perpetrator — Median Loss

Source: 2014 Report to the Nation on Occupational Fraud and Abuse, Association of Certified Fraud Examiner, Inc.
What can Credit Unions do?

- Implement dual control over vault cash, verifying currency shipments and replenishing ATMs/teller cash dispensers/teller cash recyclers
- Control access to data, information, checks, and cash
- Maintain an active Supervisory Committee
- Conduct frequent surprise cash audits (at least quarterly – monthly is better)
- Establish sound controls over expenses
- File maintenance report reviews
- Mandate employee time-off
- Management/internal audit review of internal controls
- Maintain complete and comprehensive fraud policy
- Provide fraud training for employees and volunteers
- Emphasize fraud prevention and maintain a comfortable whistleblower policy
- Perform Bondability verification and background checks
IT Department can Help

• Strong password standards

• Periodic review of employee access levels
  – Ensure access levels are appropriate for each job description
  – Review annually

• Employee and family member accounts
  – Annual disclosure to capture family member accounts
  – Lock-out feature
    • Financial and nonfinancial transactions

Review employee and family member account activity semiannually:
• Kiting indicators
• Overdrafts
• Fees
• Loans
IT Department can Help

- File maintenance transactions
  - Limit employees who are authorized to initiate critical loan file maintenance changes on existing loans

- "Do not mail" account flags
  - Limit employees who can flag accounts as “do not mail”

- Device control on workstation computers
  - To help prevent employee theft of member confidential data
  - Lock down USB ports and CD/DVD ROM drives
  - Data loss prevention solution
Tight job markets 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 through third-party service provider
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
• Access additional resources in the Protection Resource Center @ www.cunamutual.com
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, 2015 All Rights Reserved
Common Purpose. Uncommon Commitment.