CUsolutions GROUP

AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE

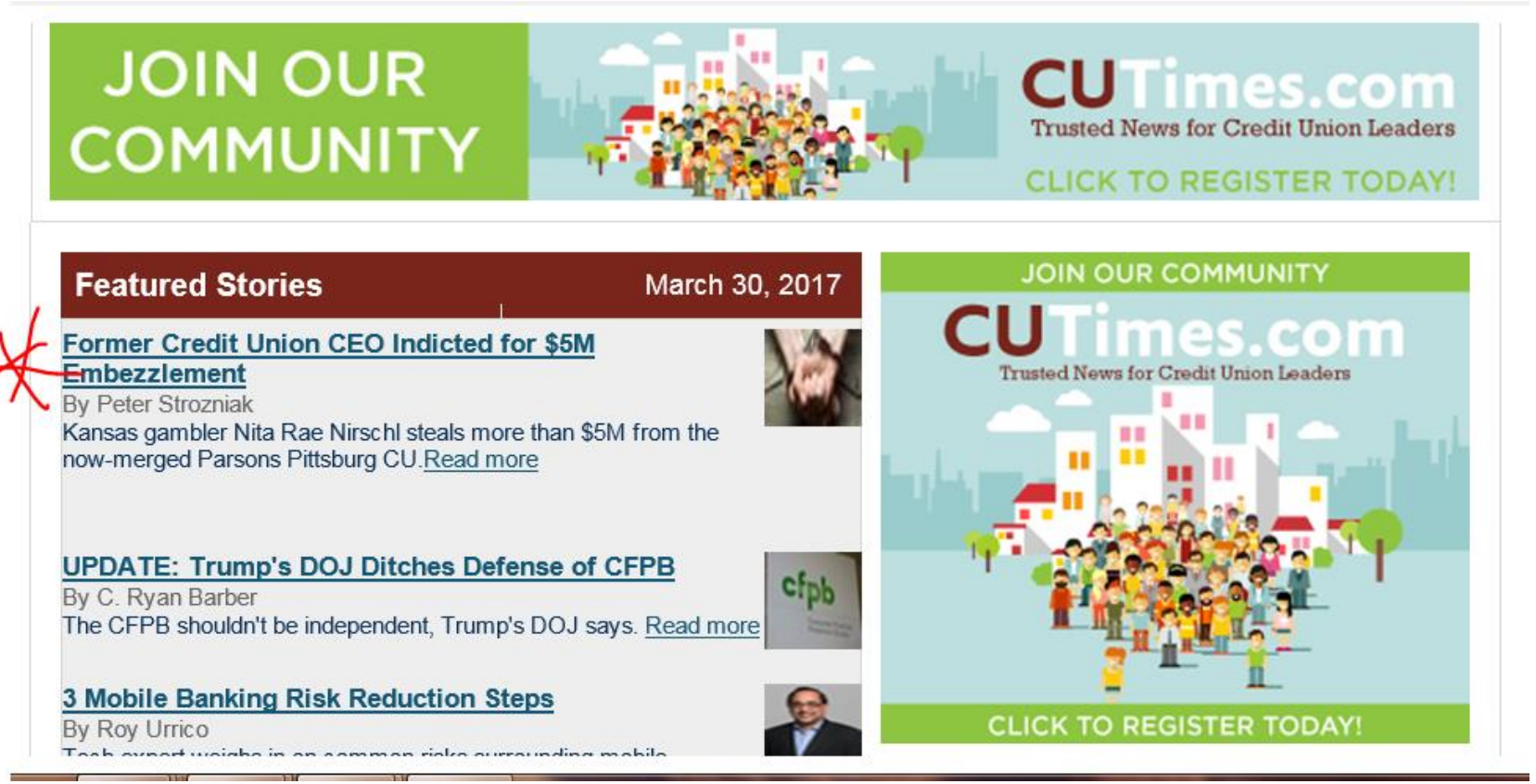
Good From The Inside Out

Saturday, April 8, 2017

What's New?

CUsolutions GROUP
AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE

Just last week…

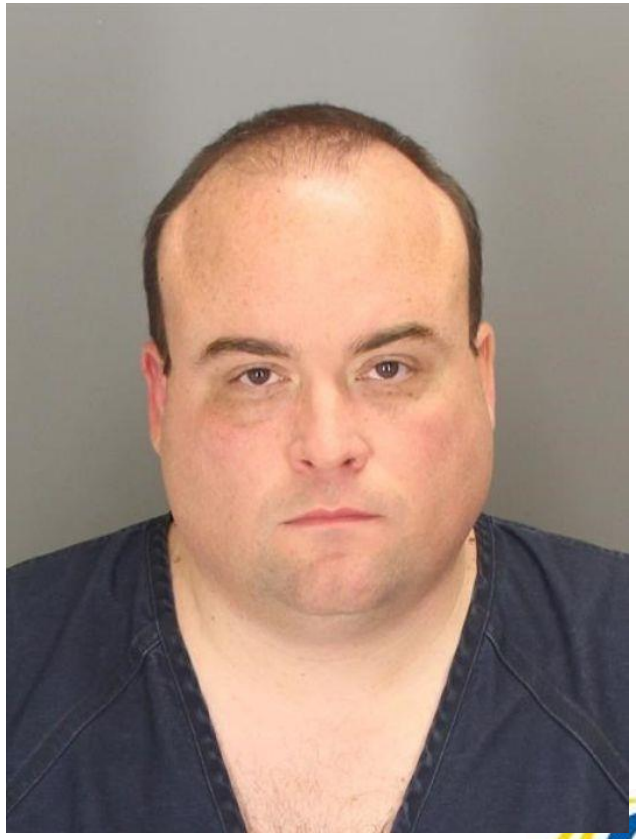


Headlines

- "Ex-CFO Accused of Embezzling $20M From Credit Union"

-Detroit Free Press

January 9, 2016



GROUP CUsolutions
AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE

Recent headlines

Engaged CU Employees Run Check Fraud Scheme for Drugs

- She worked as an accounting specialist for a $26.8M CU
- He worked as a teller at a $42.9M CU
- Allegedly responsible for 328 fraudulent checks that were deposited into 6 different accounts
- Allegedly responsible for 429 unauthorized ACH transactions deposited into 3 different accounts
- The check scheme ran from January 2015 through March 2016
- **Total loss $374,459**
- Couple faces up to 40 years each in prison and $100,000 fine

The Reality

- For every headline we read, there are a dozen cases of insider fraud that are kept quiet.
- The problem is bigger than we'd like to admit.
- **Everyone** is capable of committing fraud.

The Good, The Bad & The Ugly

Good News

- Most insider fraud is limited to thousands rather than millions
- Your bond may cover most losses associated with insider abuse
- Law enforcement is more willing to investigate than in the past

Bad News

- If news goes public, your reputation may take a hit
- Your credit union may become insolvent
- Clean up will be expensive
- Confidence will be undermined
- You can't trust anyone

Fighting Insider Abuse

CUsolutions GROUP
AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE

Why is fraud committed?

- Attitude is everything…it can happen to you!
- Motivation:
  - Pure intent at the outset
  - Greed
  - Operational failures that lead to opportunities
    - Weak policies
    - Weak procedures
    - Lack of supervision or review
- No dual control or file maintenance reviews

Types of fraud

- **Misappropriation**
  - Largest amount of fraud in this category
  - Least costly
  - Employee theft, exploitation of resources
- **Corruption**
  - Employees use the company for their own benefit
  - Bribery, extortion and conflict of interest
- **Financial Statement Fraud**
  - Least amount of fraud in this category
  - Employee omits or intentionally misstates information
  - Fictitious revenue, hidden liabilities or inflated assets

Recognize Your Risk

The first step to preventing internal fraud is to admit that it exists in the first place.

CUsolutions GROUP
AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE

Where Are We at Risk?

Liquid

- Cash/Coin
- Loans
- Corporate drafts
- Misc. negotiables (tickets, stamps, etc.)
- Equipment/Supplies

Static

- Identities
- Member account info
- User ID & Passwords
- Investments
- Credit reports

Who Poses A Threat?

- Board/Volunteers
- Staff
- Members
- Strangers

CUsolutions GROUP
AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE

Risks to your Credit Union

Trends

- Employee theft for financial or personal gain
  - Be aware of behavior or personality changes
- Insider espionage-targets internal data and trade secrets
  - Sold on the market for a higher rate of return

How Do We Manage The Risk?

- Knowledge of your tools
- Checks & balances
- Internal Controls
- Segregation of duties
- Reports that track risky behavior
- Review bond coverage annually
- Stay current on risky topics

CUsolutions GROUP
AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE

Types of internal controls

- Directive
- Preventive
- Detective
- Corrective

Directive Controls

Designed to establish desired outcomes

- Policy and Procedure
- Approval limits
- Laws and regulations
- Training
- Job description
- IT configurations

Preventive controls

Proactive in detecting

issues with an emphasis on quality

Preventative Controls require:

Authorization and approval

Supervision

Segregation of duties

Controls over access to resources and records

Examples of Preventive Controls

Segregation of duties to ensure the same person is not:

- Initiating and recording transactions
- Making purchases and approving payments
- Ordering and accepting inventory
- Approving vendors and making payments
- Receiving bills and approving payments
- Preparing, distributing, approving, writing and signing checks/posting payroll

Examples of Preventive controls

- Passwords for IT systems
- Supervisory approval of payroll before disbursement
- Dual authorization of payroll data by accounting and human resources departments
- Prior approval of credit customers, vendors and purchases
- Loan underwriting, approval, and disbursement
- Shredding sensitive information

Detective controls

Measures a company uses to identify issues that can be corrected

- Monitoring and oversight activities conducted on a regular basis
  - File maintenance reports
  - Employee and relative account monitoring
  - Reconciliation
  - Audits
  - Physical Inventories

Corrective controls

Response to errors or irregularities that have been detected

System backups

Quality Control

Corrective journal entries

Think Like A Criminal

Case Study #1: Zombie Accounts

CUsolutions GROUP
AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE

Profile: Credit Union X

- CU Asset Size: $440M
- Position: Head teller/BSA officer
- Method: Takeover of deceased member accounts
- Total money embezzled & laundered: **$738,000**
- Time period: 5 years

Who

- **Head Teller was responsible for:**
  - Her own cash drawer
  - The vault
  - BSA Officer
  - Scheduled and random cash audits
  - Managing deceased accounts
- **Profile:**
  - Employed for 18 years
  - Never sought advancement opportunities despite being qualified
  - Ultra reliable, rarely took any time off
  - Known for her exacting attention to detail and thorough work
  - No red flags of living beyond means, pricey purchases

How

- When the credit union would receive notice of death from SSI, the perpetrator would hide the notice so the account looked like it was still active
- Slowly, the perpetrator would siphon money out of the deceased's account by making cash withdrawals from her teller drawer and pocketing the cash, transferring money to other accounts under her control and using fraudulent ATM cards
- Coded the accounts not to generate statements
- Targeted dormant accounts with large balances, less likely to have relatives showing up looking for the funds

How Did It End?

- After 5 years and approximately 40 accounts, the crime was finally discovered by accident when another employee found a death certificate for one of the zombie accounts
- When confronted, the perpetrator immediately confessed, explained her system and admitted she used the funds to gamble with at a local casino
- CU terminated employment immediately, filed a SAR and a bond claim

Hindsight is 20/20

Prevention

- Should have had better checks & balances in place
- Although policy called for periodic audits, they were not being done
- As CU grew, analysis of duties should have been reviewed & reassigned
- Mandatory vacation policy

Aftermath

- CU just wanted to make the problem go away
- Should have done forensic audit to verify the depth of the fraud
- Did not seek criminal charges against perpetrator

Think Like A Criminal

Case Study #2: Fake It To Make It

CUsolutions GROUP
AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE

Profile: Credit Union Y

- CU Asset Size: $71M
- Position: Loan Officer
- Method: Fake Loans
- Total money embezzled & laundered: **$121,000**
- Time period: 9 months

Who

- **MSR was responsible for:**
  - Opening new accounts
  - Processing loan applications
  - Closing loans

- **Profile:**
  - Employed for 9 months
  - Quickly became most prolific loan processor
  - Previous employer was Ford Motor Credit
  - Married to Ford executive, upper class lifestyle

How

- MSR would open accounts with stolen identities, issue debit cards and then put in loan applications under those accounts
- Centralized lending gave loan approvals
- MSR would close loans on fake accounts and access funds via debit cards
- Made payments on fraudulent loans with proceeds from new fraudulent loans, so the fake loans never went delinquent

How Did It End?

- Also discovered by accident, another CU employee saw member's Lexus parked in driveway in a run down neighborhood. When asked about it, MSR seemed very flustered.
- Employee reported this to internal auditor, who then looked into activity and caught the fraudulent loans.
- Before HR could act, MSR quit and walked out.
- CU filed bond claim, had forensic audit performed and reported activity with SAR.

Hindsight is 20/20

Prevention

- CU had strong checks & balances in lending process, but were weak in account opening process
- CU didn't perform background check, which would have alerted them to similar activity that led to her termination from Ford

Aftermath

- CU contracted forensic audit to uncover full scope of fraud
- Sent notice to all affected consumers whose identities were used
- Deleted all fraudulent trade lines from credit reporting
- Did not seek criminal charges against perpetrator

How policies and procedures help

- Policy and Procedure give specific direction for employees to follow
- A measure of accountability by management
- Makes exceptions to policy and procedure more obvious to staff
- Should include oversight by management

Best practices

- **Know your employees!**
  - Thorough background checks
  - Follow up on references
  - Review accounts before hiring and after
- **Education**
  - Educate staff at a minimum of annually & new hires during orientation
    - Employee's responsibility to report suspicious behaviors
    - Fraud policies
    - Establish communication channels for whistleblowers

Best practices

- **Annual independent audit**
  - Independent 3rd party analyze all areas for risk
- **Utilize data analytics**
  - Software to identify trends, patterns and exceptions in data
  - Requires human judgment to determine if data is detecting fraud

Best practices

- **Rotation of duties**
  - Cross train employees to perform multiple jobs
  - Dual purpose-succession planning
- **Compulsory vacations**
  - Require employee relinquish duties for at least one week
  - Requires another employee to be fully trained to perform duties
  - Remote access must be blocked

Best Practices

- **NCUA Fraud Hotline-**

  800-827-9650

- **MCUL Anonymous Whistleblower Hotline-**

  800-262-6285 ext. 193

Questions?

Thank you for your time!

CUsolutions GROUP
AN AFFILIATE OF THE MICHIGAN CREDIT UNION LEAGUE