Resource Document

March 2023

Best Practices to Prevent Employee Fraud

Employee fraud can cost a financial institution thousands or millions of dollars, along with damaged brand reputation.

Cross check your current processes with these best practices to prevent employee fraud from happening in the first place.

Table of Contents

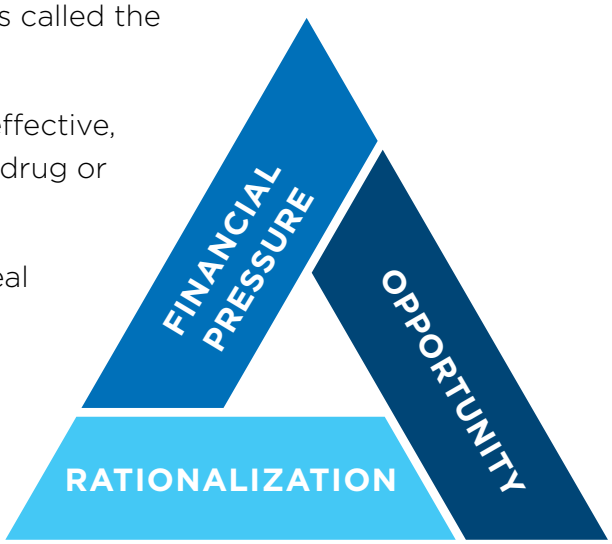
Employee Fraud Explained

Financial institutions can be vulnerable to internal theft if the proper controls are not implemented and followed. Unfortunately, the institutions at the highest risk of exposure tend to have far fewer fraud prevention mechanisms in place.

A strong internal control system reduces the *opportunity* to commit fraud, making it harder for employees to steal or engage in dishonest business practices. While there's no single deterrent to prevent internal fraud, adopting the controls outlined in this document will help your institution more effectively detect and prevent exposure to these crimes.

EMPLOYEE FRAUD MOTIVATIONS

Certain situations drive some people to steal. It's sometimes called the "Fraud Triangle" and it generally contains three elements:



Financial Pressure: This is often financial stress seeing no effective, legal way out. It may be combined with job dissatisfaction, drug or alcohol abuse, or failure to meet family pressures.

Opportunity: If employees perceive there is a chance to steal and they are under pressure, they may try it, particularly if they think they can get away with it.

Rationalization: These employees believe stealing isn't really wrong. Excuses range from: "I will pay it back" to "I'm not taking anything that will be missed," or "They should pay me more."

EMPLOYEE FRAUD WARNING SIGNS

While warning signs may not always be present, employers should be mindful that these situations can lead to employee-conducted theft:

- Addiction
- Sudden expensive purchases
- Working after hours
- Reluctance to delegate tasks
- Prolonged or frequent absences

THE IMPACT OF EMPLOYEE FRAUD

The cost of employee fraud can be devastating for a financial institution. Many reported attacks in recent years have resulted in hundreds of thousands or even millions of dollars in stolen funds.

Damage to your reputation can be significant. It is a high cost to your brand to have negative stories repeated or associated with your financial institution's name. Even minor image problems can damage accountholder confidence. Reputation risk is too important to overlook.

Damage to employee morale can poison the whole spirit of the entire working environment. The act of embezzlement takes a toll on honest and open working relationships.

Resources are diverted away from other projects and plans. The organization may be thrown into turmoil and may have to make adjustments just to keep abreast of basic operations.

Controls to Prevent Employee Fraud

CASH CONTROLS

Currency Shipments

Currency Order

The employee who is responsible for placing the currency replenishment order should not have the ability to perform the currency order general ledger entry. This separation of duties will circumvent the manipulation of the vault cash order.

Currency Shipment

The currency shipment should be locked and stored in your currency vault or money safe under forced dual control.

Verification of Currency Shipment

Currency Shipments should be verified under "forced" dual control. The bundles received in the shipment should be unstrapped and individual bills should be counted either by counting machine or manually. Both employees should remain present throughout the entire verification and re-strapping process until the re-strapped bundles are secured in the vault or money safe. Both employees should initial and date the original straps of each bundle.

Surveillance Camera

A surveillance camera is helpful to monitor the activities in the bulk cash handling area. Strategically placing surveillance cameras can assist in helping deter theft of cash by employees. Consult with your legal counsel for issues related to company privacy.

Vault Cash

Using Vault Cash

The strapped bundles in the vault cash should be used on a FIFO (First In First Out) basis so that the oldest strapped bundles are the first to be distributed.

Vault Cash Access

The vault cash should be under "forced" dual control. There are several ways to achieve "forced" dual control. An effective method is to store the vault cash in a cash box with dual locks. The key (or combination) to one lock can be given to one or two employees and the key (or combination) to the other lock can be given to one or two other employees. Under no circumstances should one employee have access to both keys (or combinations).

Another option is to split the combination to the money safe between employees in a way so that no one employee has the full combination. If dual control is not practical, the vault cash should be stored in a locked container under the exclusive control of one employee. If this is a hardship due to vacations, breaks, and other absences, a second fund should be set up and retained in a locked container under the exclusive control of one employee.

Do not rely on a camera as the only means of cash control. A camera can be disabled and rendered useless by a dishonest employee.

Vault Cash Custodian Change

The vault cash in its entirety should be verified under dual control when there is a change in the custodian.

Currency Transfers

Documenting Currency Transfers

A dated receipt should be completed whenever there is a transfer of currency between the vault cash and tellers.

The receipt should be signed by both parties involved in the transaction after they have verified the currency under dual control (strapped bills should be broken down and verified).

Do not rely on a camera as the only means of cash control. A camera can be disabled and rendered useless by a dishonest employee.

Vault Cash Transfer Entries

Tellers should not have the ability to perform a system entry to reflect currency transferred to their cash drawers from the vault cash.

The ability to make an entry could be used by a dishonest teller to conceal the theft of a cash shortage. If a teller knew of an impending surprise cash count he/she could quickly perform a bogus transaction to force balance and reverse the transaction after the surprise cash count.

Currency Transfers Between Tellers

Tellers should not have the ability on the system to buy or sell cash to each other. Teller replenishments should only be made from the vault cash.

The ability to perform this entry could be used by a dishonest teller to conceal the theft of a cash shortage. If a teller knew of an impending surprise cash count he/she could quickly perform a bogus transaction buying cash from another teller and reverse the transaction after the surprise cash count.

Teller Cash Drawers

Spare Cash Drawers

When a teller drawer is used by more than one employee due to part-time tellers or as a floater drawer, dual control of the drawer's contents should be exercised during the exchange.

Keys to Spare Cash Drawers

When spare cash drawers are not in use the keys to the tray tops should be secured under dual control (a dual locking key box).

Locking Teller Cash Drawers

Tellers should always lock their cash drawers and take the key with them when they leave their teller station, even for a brief moment.

Teller Cash Storage - During Nonbusiness Hours

Tellers should lock the tray tops on their cash trays when securing them in the currency vault/money safe and retain possession of the key. The key should not be left in the building overnight.

Spare Keys

The use of lockable containers requires the need to control access to the spare keys. In the event of a loss, lack of proper spare key control subjects every employee who had access to the spare keys to accusations of misappropriation. The ease of spare key access could lead to employee theft without the ability to determine the responsible party.

Spare keys to all lockable cash containers should be stored in a dual locking key box. The key to one lock should be given to one or two employees and the key to the other lock should be given to one or two other employees. No one employee should have access to both keys.

Surprise Cash Counts

Surprise cash counts are an excellent deterrent to "borrowing" from teller funds. They serve as an excellent detection tool for unreported cash shortages.

Surprise cash counts should be performed on a monthly or at least quarterly basis, but follow no predictable pattern. Surprise cash counts should be performed by an individual that does not have access to that cash supply.

The person performing the surprise cash count should be the counter of the cash in the presence of the person responsible for the cash supply. The cash count should include a review of cash replenishment transactions conducted by the teller for that day prior to the cash count. Surprise cash counts should be performed for all cash items (teller funds, vault cash, postage stamps, petty cash, bus tickets, amusement park tickets, etc.).

Teller Cash Dispensers/Teller Cash Recyclers

Replenishment

This should be performed under dual control. Lack of dual control could subject an employee to accusations of misappropriation of funds in the event of a shortage.

ATM Procedures

ATM Replenishment and Balancing

ATMs should be replenished and balanced under dual control. Lack of dual control could subject an employee to accusations of misappropriation of funds in the event of a shortage.

ATM Cassettes

ATM cassettes containing cash should be locked and stored in the currency vault/money safe until they are taken to the ATM for replenishment. The filled cassettes should have a numbered plastic or wire adhesive security seal while stored in the currency vault/safe. The number of the security seal should be recorded and confirmation that the seal was not tampered with should be made before being taken to the ATM for replenishment.

ATM Surprise Cash Counts

Surprise cash counts should be performed at least quarterly.

ATM General Ledger Account

The employee balancing the ATM(s) should not have the ability to perform system entries to the ATM general ledger accounts. The duties should be segregated.

ATM Deposits

All ATM deposits should be verified under dual control.

Night Depository

The night depository should be accessed under "forced" dual control. No one person should have the ability to open the night depository. A key and combination or a split combination method should be implemented.

The contents of the night depository should be verified by two employees acting jointly. All contents should be logged and both employees should sign the entries.

IMMEDIATE ISSUE PLASTIC CARD CONTROLS

Blank Card Stock

Storage

All blank card stock (credit, debit, ATM, prepaid) should be secured under dual control in your currency vault/money safe. Lack of adequate control increases your risk of unauthorized issuance.

Verification of Inventory

Inventory of the blank card stock should be performed quarterly by someone without access to the card stock.

PIN Encryption

All employees authorized to issue or re-encode plastic cards using the PIN encryption device should have their own individual confidential password. Passwords should be changed at least quarterly or sooner if there is an indication of a compromise.

PIN Encryption Log

A log should be maintained that includes new cards issued and PIN changes made using the PIN encryption device. The log should include the date, cardholder name, the identification used to verify the cardholder's identity and the employee's signature.

SAFE DEPOSIT BOX CONTROLS

Safe Deposit Box Guard and Gate Keys

In order to prevent unauthorized access to the currency vault, the guard and gate key should be stored in a secure location accessible to authorized employees only.

Spare Guard Keys

All spare guard keys should be stored under dual control, but not in a safe deposit box since you would not be able to open any safe deposit box if the guard key were lost.

Unrented Safe Deposit Box Keys

All unrented safe deposit box keys should be stored under dual control in an unrented safe deposit box.

Drilling of a Safe Deposit Box

If a safe deposit box must be drilled in the absence of the leaseholder, at least two employees as witnesses should be present during the entire process. After the box is opened, the contents should be documented and stored under dual control.

COMPUTER SYSTEM CONTROLS

Employee Password Standards

Complex Passwords

The system should require only complex passwords. At a minimum, passwords should be at least eight characters long, alphanumeric, case sensitive, and require the use of special characters (!, @, #, $, %, etc.).

Multi-Factor Authentication

Enable multi-factor authentication (also known as 2-step verification) for systems access. Biometrics can also be integrated into MFA for an additional layer of security.

Password Confidentiality

Passwords should never be shared or disclosed to another employee.

Password Changes

Passwords should be set up to force password changes at least every 90 days. The system should not allow a change to a recent password that was used within a recent period of time.

Incorrect Password Attempts

Your system should be designed to automatically lock user IDs after three incorrect password attempts. A report should be generated and reviewed of failed login attempts.

Terminal Sign-Off

Employees should always sign off of their terminals when they leave their workstations. In addition, the system should automatically log off after five minutes of inactivity.

Supervisory Overrides

Dormant Accounts

Dormant accounts should require a supervisory override to post a transaction (deposit, withdrawal, loan activity). Dormant accounts are often the target of dishonest employees.

Supervisory Override Report

The Supervisory Override report should be reviewed on a regular basis by an employee without override authority. Transactions in dormant accounts, waiving fees, accounts changed to “do not mail”, etc., should be reviewed for legitimacy.

Activity on Dormant Accounts

You may want to generate a separate report of activity in dormant accounts to be reviewed by internal audit.

"Do Not Mail" Account Review

Periodically a separate report of accounts flagged as "do not mail" should be generated and reviewed by internal audit. These types of transactions can be used by a dishonest employee to control an account.

File Maintenance/Non-Financial Transaction Report

An individual that does not have the ability to perform a file maintenance transaction should review this report on a regular basis. The types of transactions that should be reviewed for legitimacy include:

- Advancing a loan next payment due date
- Changing the payment amount for a loan
- Changing the payment frequency for a loan
- Changing the collateral code
- Changing interest rates for any account
- Several address changes to a single address

The file maintenance report should be reviewed for credit card transactions by someone not authorized to perform these types of transactions.

Employee and Family Member Accounts

Employee Annual Disclosure of Accounts

Procedures should be in place requiring employees to annually disclose their accounts and those of family members and other individuals living in their household.

Employee and Family Member Account Activity

Employees should not have the ability to perform transactions in their own or family member accounts. In addition to a written policy, the computer system should be programmed to enforce this policy by restricting access.

Your plastic card processor should be contacted to determine if a lockout feature is available to block card department employees from their own and family member accounts.

Employee and Family Member Account Review

Procedures should be in place to review employee and family member accounts and others living in their household periodically.

A monthly report should be received from your plastic card processor of insider credit card accounts (employees and family members). Someone outside of the card department should review this report to detect unauthorized changes (i.e., limit increases).

At a minimum, a review should consist of at least the following:

- Courtesy Pay usage
- Not-Sufficient Fund activity
- Balances extending beyond credit limit
- Loan advances
- Credit limit increases
- Delinquent loan payments
- Overdrawn accounts
- Suspected check kiting
- Transfers from other accounts
- Large deposits

LENDING CONTROLS

Separation of Duties

To deter unauthorized/fictitious loans, no one employee should have the ability to approve a loan, process the loan, and disburse the proceeds. Separation of duties in the loan process can be accomplished by segregating the loan approval and disbursement.

Opening New Accounts

Loan officers should not have the ability to open new accounts on the system. Lack of this separation increases the chance of a fictitious loan.

Confirmation of Accountholder Loans

Someone not active in the lending department should perform a confirmation of new loans and loan advances, including new credit cards and limit increases.

Collection Activity

Collection staff should not have lending authority or the ability to post collection payments to delinquent accounts. All payments for collection accounts should be sent to the teller staff for posting. Collection staff should not have transaction authority. Lack of separation of duties could allow fictitious loans and/or theft of collection proceeds.

Someone not involved in the approval or collection of delinquent accounts should periodically review the entire collection process including:

- Documentation of progressive collection efforts at each stage of delinquency
- Reporting of delinquencies to the Board of Directors
- Separation of duties of collection staff
- Invoices of repairs of repossessed collateral
- Condition reports on collateral
- Physical inspection of repossessed collateral
- Bids for sales of collateral

EMPLOYEE AND DIRECTORS EXPENSE CONTROLS

Expense Reimbursement Policy and Procedures

Approved Expenses

A policy should be in place that clearly specifies approved use of assigned corporate credit cards and out-of-pocket expenses for both volunteers and employees. At a minimum, the policy should include the following:

- Cell phone/internet
- Supplies
- Transportation (auto mileage, rental cars, airline, etc.)
- Hotel (internet, movie rentals, etc.)
- Incidental travel expenses (taxi, tips, etc.)
- Use of the corporate credit card (acceptable and unacceptable use)
- Policy exceptions

Expense Reporting

Employees and Directors should be required to complete an expense report for business related expenses. Both out-of-pocket and expenses charged to their corporate credit card should be included. Receipts should be required that would include the reason for the expense, business purpose and individuals involved in the expense (i.e., if others were present at a meal).

Expense reports should be turned in within a reasonable period of time.

Conference Summary

If attending a conference, at the conclusion, each employee and/or official should complete a conference summary. This ensures the maximum benefit of the travel expenses incurred, as well as documents the attendance.

A policy should be in place that clearly specifies approved use of assigned corporate credit cards and out-of-pocket expenses for both volunteers and employees.

Expense Approval

- Expense reports should not be approved by a subordinate. The following is a next higher level of authority approval listing:
- The CEO and all volunteers except for the Chairperson of the Board – Chairperson of the Board approves
- The Chairperson of the Board – Board Treasurer approves
- All employees except for the CEO – CEO approves

Segregation of Duties

The person who approves expenses should not post them to the general ledger. This violates sound internal control procedures and could allow fictitious or unauthorized expenses to go undetected.

ACCOUNTING CONTROLS

Corporate Checking Account Reconciliation

Segregation of Duties

The corporate check account should be reconciled by an employee who does not have the authority to sign checks or post deposits. The reconciliation should be performed every month.

Unresolved differences should be brought to management's attention immediately. Differences not resolved within 90 days should be reviewed by internal audit or the supervisory committee.

Voided Checks

A report of voided cashier's checks and official checks should be generated monthly. The review should be performed by an employee who does not have the authority to issue checks to verify the checks were voided and reissued for legitimate reasons.

To increase the effectiveness of this audit procedure, the employee who reviews voided checks should not have the authority to issue them.

Accounts Payable System Access

Accounts payable system access should be limited to only Accounts Payable employees.

An audit should be performed quarterly to include verification of new vendors. To reduce the risk of fraudulent vendors/payments a sampling of payments made should be reviewed for supporting invoices and proper approval authority.

General Ledger Suspense and Clearing Accounts

All general ledger suspense and clearing accounts should be reviewed monthly by an employee who does not have posting authority. These types of general ledger accounts are often used by a dishonest employee to force balance an embezzlement scheme.

Employee Payroll

Payroll functions of creating the payroll file, authorizing the payroll and issuing the payroll/submitting the file to an outside payroll service should be segregated.

A manager not involved in the payroll process can be assigned to authorize the payroll prior to being issued for payment/submitted to the outside payroll service. Or, the employee creating the file is not the same employee submitting the file.

Funds Transfer System Controls

Dual verification for funds transferred through Fedline or the corporate electronic funds transfer system should be used. Frequency and monetary limits should be in place. Implementation of internal processes will reduce your exposure to employee dishonesty.

Equipment Purchases

Approvals

Requests for equipment purchases should be approved by the requester's superior. Lack of approval from the next higher level of authority could allow unauthorized or fictitious purchases.

Competitive Bids

A policy should be established for obtaining competitive bids for equipment purchases. Sound business practices consider price, vendor, quality, and support. Not only will this prevent overpaying, but also the temptation of an employee receiving kickbacks.

Physical Inventory of Equipment

When new equipment is ordered it should be inventoried to determine it is on-site. In addition, a semi-annual inventory of equipment should be performed. This practice will deter employee theft of equipment.

ADDITIONAL INTERNAL CONTROLS

Know Who You Are Hiring

Consider the use of a reputable third party to perform a criminal background check, a credit check, work, education verification, and possibly a drug test prior to making a job offer to any applicant.

Consider Enforcing Mandatory Vacations

It is essential to enforce a mandatory one week of consecutive vacation. If an employee is committing internal fraud, a week of consecutive days off potentially removes the opportunity for an employee to cover their tracks.

The intent of the mandatory vacation policy and enforcement of the policy is to allow for the discovery of fraudulent activity.

Whistleblower Process

Employees should be provided a resource for reporting fraud or theft that they become aware of. Using a third party for fraud and theft reporting may increase employee usage, by providing anonymity and reducing the fear that information will be traced back to the reporting employee.

Implement a Formal Complaint Handling Process for your Accountholders

Several employee dishonesty schemes have been uncovered while investigating accountholder complaints.

If an acccountholder reports suspicious transactions or questions their account activity, it should be taken seriously, even if it seems trivial at first. All accountholder complaints should be investigated in a timely manner.

Anti-Fraud Policy

A written anti-fraud policy should be developed together with legal counsel, approved by the Board of Directors, and included in the board minutes. Every employee should be required to read and acknowledge the policy by signing and dating it when hired and annually thereafter.

Fraud Training for All Employees

Employees, management, and board members should receive annual fraud awareness training. This sets the tone that fraud will not be tolerated and ensures procedures are reviewed on a regular basis. This training should include fraud ramifications and reporting procedures.

Rotation of Duties

Limited staff may make cross-training employees more challenging, but implementing these internal controls can greatly reduce exposure to fraud. Many embezzlement cases have been detected when the employee goes on vacation and another employee steps in to perform his or her duties.

Board Oversight

The Board of Directors should have oversight of the institution's anti-fraud program. The Board should also meet with internal and external auditors on a regular basis. Internal controls should be implemented at the Board level and established throughout the credit union. It is the responsibility of the Board to set the tone from the top that fraud will not be tolerated.

Proper controls require time and consistency to implement and follow. However, these preventative measures can go a long way in reducing a financial institution's vulnerability to embezzlement and misuse of organizational data.

Subscribe to receive more fraud prevention and education: alliedsolutions.net/enews.

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

Learn More

Visit our website: alliedsolutions.net

Follow Allied on Twitter: twitter.com/alliedsolutions

Visit Allied on LinkedIn: https://www.linkedin.com/company/allied-solutions-llc/

Like Allied on Facebook: www.facebook.com/AlliedSolutionsLLC/

Visit Allied Insights: alliedsolutions.net/allied-insights

Subscribe to our Newsletters: alliedsolutions.net/enews