

AUDITING CASH & CASH EQUIVALENTS

Because of the very nature of cash and cash equivalents, this area of credit union operations is usually considered a high-risk area that requires good internal controls and careful monitoring. Our article outlines the testing that Supervisory/ Audit Committees, Risk Management, and Internal Audit Departments may want to consider as part of their review of the internal controls in the area of cash and cash equivalents.

Cash usually includes cash on deposit in other depository institutions, cash on hand, and cash equivalents. Cash equivalents are short-term, highly liquid instruments that are both easily convertible to known amounts of cash. Types of cash and cash equivalents include, but are not limited to, cash, teller cash, vault cash, ATM cash, petty cash, traveler's checks, money orders, cashier's checks, investments, movie tickets, stamps, etc.

Risk is defined as the potential that events (expected or unanticipated) may have an adverse impact on a credit union's earnings, capital, or credibility. Existence of risk is not, by itself, a reason for concern. Rather, Management must consider whether the risks are warranted. Risks are warranted if they are understandable, controllable, and within the credit union's capacity to readily withstand adverse performance. The area of cash and cash equivalents historically is a low risk area compared to other areas of the credit union. However, continuous coverage in the area of cash and cash equivalents must be part of the internal control consideration due to the nature of cash.

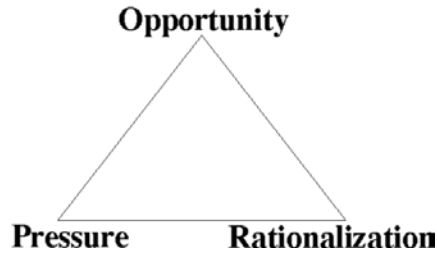
As can be seen in the "Fraud Triangle," three items are usually needed for an embezzlement of cash to occur; an Opportunity, Pressure, and the individual's Rationalization of a situation. The definitions of these terms are as follows:

Opportunity: Circumstances exist for example, the absence of controls, ineffective controls, or the ability of Management to override controls that provide an opportunity for fraud to be perpetrated.

Pressure: Management or other employees may have an incentive or be under pressure, which provides a motivation to commit fraud.

Rationalization: Those involved in a fraud are able to rationalize a fraudulent act as being consistent with their personal code of ethics. Some individuals possess an attitude, character, or set of ethical values that allow them to knowingly and intentionally commit a dishonest act.

The Fraud Triangle



	<i>Opportunity</i>	<i>Pressure</i>	<i>Rationalization</i>
1.	I have access to the vault.	I need the money.	The CU has excess cash.
2.	I have access to the vault.	I need the money.	I do not want to go to jail.
3.	I do not have access to the vault.	I need the money.	The CU has excess cash.
4.	I have access to the vault.	I do not need the money.	The CU has excess cash.

The above example relates to individuals who are tellers and how the three areas could effect a potential embezzlement. As can be seen in the matrix above, all three items (Opportunity, Pressure, and Rationalization) need to exist in order for a potential embezzlement to occur. The “colored” explanation in three of the rows provides an example where the likelihood of the probability of embezzlement would not occur. Therefore, in the matrix above, embezzlements would most likely occur when conditions in row 1 exist. This matrix could be developed for specific areas for virtually all conditions and/or situations where fraud could potentially exist.

Based on the numerous areas affecting cash and cash equivalents, the following recommendations should be considered at a minimum, to deter against fraud.

Conduct surprise cash and cash equivalent counts. These cash counts should be conducted through the year and should cover all branches and, if possible, all tellers. These cash counts could be on a “spot basis” and may cover all and/or a sample of tellers. In addition, other cash and cash equivalent areas should be covered in these counts.

- Bait money should be verified as part of the cash counts. It should also be periodically rotated to ensure the bait money does not give the appearance of being old.
- Check teller drawers to determine if tellers have any of the teller's own personal checks in his/her cash drawer. It is not uncommon for tellers to place their personal checks in their drawer without “dating” the check. The embezzlement of funds is accomplished by the teller taking money for long periods of time and in the event of a surprise cash count, the teller states that the check was placed into the drawer that day and that he/she forgot to date the check.

- Counts of cashier's checks and credit union checks should ensure that tellers are issuing checks in sequence and that missing check numbers are accounted for by voided checks.

Test dual custody or dual control procedures. Dual custody requires that a minimum of two people are required to physically access certain items or records and are equally accountable for their protection. For example, one employee has the key and a second employee has the combination to access the ATM machine. Dual control extends that concept by requiring that the work of one employee is verified or approved by a second employee. One employee counts and records the deposits obtained from the night deposit box, a second employee verifies that count. Dual custody and control procedures should be tested to ensure only collusion could bypass internal control procedures and possibly perpetrate a fraud. Examples include but are not limited to:

- Reserve cash, negotiable instruments, unissued traveler's checks, the night depository, the vault, ATM machines, the reserve supply of official checks are examples of items and areas that should be under dual custody. Walk through the steps to obtain these items or access these areas to ensure at least two people are required to obtain access.
- Night depository procedures should be done under dual control. For example; withdrawal of funds, opening of bags, recording of bag numbers, envelope numbers, and depositors' names, and counting and verifying the contents of the envelopes. Review a sample of daily work for dual control sign off.
- Deposits received by mail should be opened under dual control. Review a sample of daily work for dual control sign off.
- If the ATMs are replenished or serviced by external third parties, a credit union representative should be present. Verify with Management that this occurs.
- Logs should record entrance and exits to the vault, ATM machines, night depository, safe deposit boxes, etc. Review logs for completeness and appropriate access granted.
- Currency shipment procedures (sending and receiving) should be done under dual control. Verify procedures with appropriate personnel and review cash order receipts for appropriate signatures.

Review mandatory vacation policies. The credit union should have a written vacation policy that mandates employees be absent from their duties for an uninterrupted period of not less than one week. Someone else should assume the duties of the absent employee as a fraud prevention/detection tool. Review the written policy. To ensure the policy is enforced, select a sample of employees and verify the mandatory vacation was taken in the prior year.

Review teller cash overage/short accounts. There should be written procedures in place for prompt reporting and investigating of shortages when they become known. Cash overages/shortages should be properly recorded in a cash over/short account. Review account details for recurring patterns or any large or unusual items. Ensure shortages have been properly investigated and resolved.

Test key and combination assignments. The credit union should have a record of all keys and combinations issued to employees. Physically verify each employee has in his or her possession the keys assigned from this record. Keys should be retrieved and combinations changed when an employee terminates. Review the records to ensure this has occurred if an employee with possession of a key or combination has recently terminated. Unassigned keys should be kept under dual control. Walk through the steps to observe how access to these keys is obtained to ensure at least two people are required to gain access to the keys.

Review of other procedures and controls. Your credit union may have other controls in place for security of cash and the teller function. Does credit union policy and procedures require any of the following? If yes, verify practice is consistent with written policy.

- Pocketless uniforms or clothing for tellers. Several credit unions have required that tellers wear uniforms, which are pocketless. However, the implementation of this requirement would be based on a cost versus benefit basis depending on each credit union.
- Receipts for all transactions. Management should consider making it a requirement that tellers provide each member with a receipt reflecting the member's transaction. Each teller station should have a sign posted that states:

“All members must be provided with a printed receipt as part of your transaction. In the event that the member does not receive a receipt, please notify Management.”

- Installation of video cameras. Video cameras should be placed in strategic places where there are cash and cash equivalents. In addition, while most video cameras are installed to monitor member activity, consideration should be considered in areas behind the teller lines and in areas where there is continuous traffic. Also, if the tellers have an area where they store their personal belongings during the working hours, the installation of a video camera in this area should be considered.
- Lockers installed outside the cash area. The credit union may want to establish an area outside of the teller area where credit union employees can place their personal belongings away from the area where cash and cash equivalents are maintained. This procedure could prevent the transfer of unauthorized funds into the credit union employee's personal belongings.

Review of teller access and authentication mechanisms on the computer system. Access and authentication mechanisms on the computer system are important tools to ensure accountability and prevent unauthorized access to transactions and information. Review authentication and password policies for appropriateness. Select a sample of employees and review their access rights on the system. Compare system user ID lists to a current employee list from Human Resources to ensure terminated employees have been removed from the system.

- Most computer systems have the capability to require passwords to access the system. However, passwords need to be changed on a frequent basis. We recommend forced password changes every 45-60 days. In addition, the employee should not be allowed to use the same password.
- Password construction should mandate that passwords be a minimum of 6 alphanumeric characters and should not be easily guessed. Guidance should be provided about the importance of keeping the employee's password confidential to include not writing it down or sharing it with other employees.
- Also, the computer system should log out the teller when there has not been activity for a certain period of time (usually 10 minutes). If automatic log-off is not an option, consider screen savers that would activate after 10 minutes of inactivity and would require re-entering the teller's password when coming back to the application.
- Terminated employees should be removed from the system as soon as possible to prevent anyone from using that ID for unauthorized access to transactions and information.
- One last point is that tellers should not be permitted to make any transactions to their personal or relative's accounts. It has been noted that tellers who have embezzled in the past have used their relative's accounts for unauthorized activity (Sometimes with and without their relative's knowledge). In addition, teller access to the system should be based on the principle of "least privilege" - limited to those functions required for their job responsibilities.

Review hiring procedures. Appendix A of NCUA Regulation 748 recommends that credit unions consider background checks for any employees with responsibility for or access to member information. Depending on your credit union and the views of Management, the Board of Directors, and the Supervisory/ Audit Committee, full and/or limited background checks should be conducted on each teller. Also, these background checks should be considered for individuals in sensitive positions at the credit union. Review your credit union's written hiring procedures and select a sample of employees to ensure hiring procedures were followed. The following are some of the more common background checks and hiring procedures:

- Criminal background checks.
- Background check on the driving history of the potential employee. (This is also important when tellers travel from Branch to Branch during credit union hours.)
- Prior employment checks. Verifies the information the prospective employee has given on past employment. If possible, contact the former employer of the potential employee and request their last two evaluations. (This may not always be possible during the hiring stage due to the potential employee not wanting their current employer to know that they are seeking employment elsewhere. However, once the potential employee has given notice to his/her current employer that they are leaving their current position, this information could then be requested. This procedure can provide the credit union with valuable information on the potential employee and also confirm information provided during the interviewing process.)

- Credit bureau review. (Besides providing information on the potential employee's credit history, the credit bureau reports can also verify the potential employee's employment history, employee's address, social security number, etc.)
- Drug testing. (While this is a very sensitive area, would you as a potential employer want to know if there were pre-existing problems prior to this individual being employed by your credit union?)
- Finger printing of a potential employee. (Due to the sensitive area of cash, this may be a procedure that the credit union may want to consider. It has also been brought to our attention that several local police departments provide this service free of charge to financial institutions.)
- Signing an "annual disclosure form." (The annual disclosure form provides information on the credit union employees related to employee and family member accounts and must be filled out annually by the employees. An annual disclosure form was covered in a previous article and a sample of one can be obtained by going to our website.)
- Signing a confidentiality statement and/or an acknowledgment of the credit union's fraud policy.
- Bondability check. (Verify that potential employees are able to be bonded by your insurance company.)

Policies, procedures, and zero tolerance of fraud. Credit union employees should be informed of the policies and procedures covering the area in which they are working. The credit union's employees should also be informed that the credit union has zero tolerance for any fraud and they will prosecute any credit union representative who violates these policies. In addition, it should also be communicated to all employees that any credit union representative who is aware of a potential fraud has a duty to report this to the appropriate individuals at the credit union. Not reporting this to the appropriate individuals constitutes a violation of the credit union's policies and procedures and the employee will be subject to the same disciplinary actions, which will take place against the original abuser. Review the credit union's written policies related to fraud. Determine how these policies are communicated to the employee. If the employee is required to sign an acknowledgment of receiving the policy, select a sample of employees and verify an acknowledgment was signed.

Based on the information presented in this article and the potential for detecting fraudulent activity, we strongly recommend that credit unions consider the recommendations we have discussed. Most of the items are proactive measures and a psychological deterrent, which should aid the credit union in their monitoring of these sensitive areas.

*Cecil D. Maynard, CPA, MPA, CFE, Director
& Rachel E. Fisher, CISA, NCCO, Director
Nearman, Maynard, Vallez, CPAs & Consultants, P.A.*

Established in 1979, Nearman, Maynard, Vallez, CPAs & Consultants, P.A. is a full service CPA firm providing auditing and consulting services to credit unions nationwide. Services include financial statement audits, pension audits, fraud audits, internal audit outsourcing, compliance reviews, and information technology audits. For more information, contact us at 800-288-0293 or info@nearman.com, or visit our website at www.nearman.com.