Fraud Discovery Checklist for Credit Union Board of Directors

Fraud can be committed in any department of the credit union and by anyone from a teller to a board member, or even collusion between a group of employees or board members. Officials should keep this in mind as they begin to act on a suspicion of fraud. The following checklist will assist officials upon discovery of a fraud. This checklist is provided for guidance only and should not be construed as all-encompassing for actions needed on the part of Credit Union Officials upon fraud discovery. Prior to beginning the outlined tasks read the entire checklist.

Tasks	Initials	Date	Comments
1. Contact the credit union's legal counsel for advice on how to proceed.			
2. Contact the credit union's NCUA examiner and state regulator, if applicable.			
3. Control access of the involved personnel:[1]			
a. Obtain keys and passwords from the individual(s). Request Fed tokens, security codes, user names and passwords, and vendor contact information. If the individual(s) is not cooperative, void authorization access.[2]			
b. Revoke remote access to credit union systems.			
c. Re-key locks on doors, disable electronic badge access, and change alarm and camera codes. If the building is leased, notify the			

[1] Access restriction should occur prior to placing the individual on administrative leave.
[2] Obtain user names and passwords for all systems such as web-based applications, third party services, and credit union email.

building management of re-keyed door locks.			
d. Change computer system passwords.			
e. Change signatories and wire authority on bank, Federal Reserve, investment, safekeeping documents, custodian accounts and corporate credit union accounts, etc.[3]			
f. Obtain total control of any post office or mailboxes, night drops, ATMs, vault, teller drawers, etc.[4]			
g. Notify third party vendors of the change in personnel. Vendors to include initially: ACH service provider, online banking provider, CUSO to support any electronic payment activity, post office box, security system provider, core system provider, and ATM network.			
h. Ensure any saved footage from security cameras is secured and not subject to being overwritten.			
i. Secure credit union owned assets (for example, cell phone, laptop, vehicle) from the individual including items maintained offsite.			
4. After consulting with the credit union's legal counsel, restrict access to involved			

[3] Financial institutions normally require identification of new signatories. This process will be facilitated if current signers assist in the change. As different institutions will have varying procedures to make this change, the Board should contact the individual institution for further guidance on how to make the change as soon as possible.
[4] This includes collecting all keys (such as cash drawers, mailboxes, desk drawers) from the individual and changing combinations where applicable (for example, vault, ATM, night deposit).

personnel's credit union accounts including:			
a. Freezing accounts (primary and joint).			
b. Closing charge cards (personal and corporate).			
c. Restricting access to safe deposit boxes.			
5. Perform review procedures to determine cash differences:			
a. Perform cash, vault, and ATM cash counts, under dual control.			
b. Account for teller/cashier checks, money orders, and negotiable instruments.			
6. Contact involved personnel:			
a. Interview the individual(s) to determine the information they will share. You may want to have legal counsel present for the interview. Be vague on the information found. Do not give a possible dollar loss to involved personnel.[5]			
b. Suspend the personnel involved with pay until an investigation can be completed. Determine if other employees should be suspended during the investigation.[6]			
c. Escort involved individual(s) out the door. Do not leave involved personnel alone. Advise them their personal possessions will be			

[5] At least two officials should be present during the interview.
[6] Credit union officials should consult with their human resources department and attorney during this step.

inventoried and boxed up, and they will be contacted for pick up.[7]			
7. Isolate and preserve all hard copy evidence. Ensure originals are in "as-is" condition (do not write on or alter originals).			
8. Depending on the individual's involvement in the credit union's operations, fill the operational void caused by the suspension.			
9. Contract a third party to complete a mirror image of affected computers and computer systems.[8]			
10. Review bond contract to determine notification deadlines and notify bonding company of potential fraud.[9]			
11. Contact law enforcement.			
12. Determine if a forensic audit is needed.			
13. Assign a media contact person and develop a message to address media questions.			
14. Inform staff. Messaging to staff should include, at minimum, an emphasis on business as usual, how to respond to member questions, maintaining confidentiality and no comments on social media.			
15. If member accounts are involved in the fraud, a verification of member accounts should be performed.			

[7] This step does not include maintaining car keys, wallet, etc. If the individual(s) leaves with a briefcase or bag, officials should check contents for credit union possessions or evidence of the fraud prior to the individual(s) exiting the credit union.

[8] Mirroring makes an exact copy of the storage media on the computer that is precisely the same as the original both physically and logically. The purpose of mirroring is evidence preservation.

[9] The credit union officials should consider consulting with an attorney to ensure notifications deadlines are met.

16. File a bond claim after all facts are known and per the bond contract deadlines. (The forensic CPA may be able to assist you in filing the bond claim.)			
17. Once the fraud is confirmed, consult with attorney to formally notify the individual(s) of termination and to determine pay due to involved individual(s). The acceptance of a resignation letter containing a "Hold Harmless" clause will be detrimental in pursuing any restitution. You should consult with your attorney before accepting any resignation letter and ensure any termination letters does NOT contain a "Hold Harmless" clause.			
18. Complete a Suspicious Activity Report (SAR) per regulatory requirements.			