LSC

Legal Services Corporation
Office of Inspector General

Inspector General
Kirt West

MEMORANDUM

TO: Executive Directors
LSC Grantees

FROM: Kirt West Kirt West
Inspector General
Legal Services Corporation

SUBJ: Advisory Bulletin on how to Protect Your Organization from Internal Thefts

DATE: September 15, 2005

I am issuing this guidance to provide information to all Executive Directors of LSC grantees on possible steps that can be taken to reduce your organization's vulnerability to internal theft. Many of you probably feel confident that, because the person who handles petty cash, credit card purchases, travel vouchers, etc., is a trusted, long-time, valued employee, you are not vulnerable to theft. Until very recently, those were the exact sentiments of the senior management team of an LSC grantee.

Early this year, the Office of Inspector General (OIG) chief investigator received a phone call from an LSC grantee after managers started to notice some financial irregularities. The grantee reported that an employee, using the grantee's corporate account, had purchased a $2,000 computer from a local vendor for personal use, and had embezzled $3,600 from petty cash funds. Understandably, the Executive Director was worried and upset. Within a few days, the OIG had staff on site at the grantee's headquarters. The OIG and the grantee worked very closely to identify the actual loss and to strengthen management practices to reduce the program's vulnerability to fraud. Recently, I spoke with the Executive Director who expressed his deep appreciation for the highly professional manner in which the OIG approached the problem and the assistance the OIG provided to the program.

3333 K Street, NW 3rd Floor
Washington, DC 20007-3522
Phone 202.295.1500 Fax 202.337.6616
www.oig.lsc.gov

Grantee staff provided the OIG with evidence that a long-time, trusted employee, who served as the office manager, embezzled funds though the filing of false travel vouchers and petty cash reimbursement vouchers. As the petty cash custodian, the employee was able to circumvent the internal controls and obtain funds through the filing of fraudulent reimbursement claims. This individual was also responsible for ordering office supplies through store accounts and the grantee's corporate credit cards. The OIG determined that the individual purchased a significant number of items through these accounts for personal use and consumption. The individual tried to flee but was recently arrested at an out-of-state location and is now awaiting trial.

The OIG reviewed the grantee's internal controls and concluded that the grantee's accounting processes and procedures were adequate. However, the OIG determined that internal controls were not always followed. Because the supervisor trusted this employee and was extremely busy, the supervisor did not perform the monthly review and reconciliation of the petty cash fund, and did not conduct the monthly review of the corporate credit card statements for the appropriateness of the purchases. As for the monthly petty cash review and reconciliation, the supervisor took the employee's word that supervisory review was no longer required because of changes in the petty cash system. Funds and reimbursements handled by the trusted employee were not questioned until more than $13,000 was missing. That $13,000 represents funds that could have been channeled into providing legal services to many low-income families.

In retrospect, the Executive Director has identified some of the "tell-tale" signs indicating a potential problem. The employee was not taking vacation; the employee's intimidating personality prevented peers from checking the employee's work; and the employee did not allow anyone else to open the mail, especially bank correspondence and bank statements, and review account information.

The OIG recommends that senior management perform the following checks on a periodic basis to help protect organizational assets:

1. Conduct unannounced reviews of petty cash and petty cash transactions;
2. Review travel reimbursements;
3. Review all travel advances and pay advances;
4. Examine the organization's check book, to ensure there are no missing blank checks, or checks issued out-of-sequence;
5. Examine the general checking account statements for suspicious out-of-sequence check numbers and deposit anomalies;
6. Review office supplies purchased through house accounts for purchase anomalies (limiting supply purchasing to vendors who deliver can provide an extra level of assurance);

7. Review bank statements and paid checks;
8. Review corporate credit card transactions for purchase anomalies;
9. Use counter signature checks and do not sign blank checks; and
10. Periodically rotate the staff responsibilities for reviewing bank statements and credit card statements.

Unfortunately, the investigation discussed above is not an isolated incident. During the past eight months, the OIG has opened six embezzlement investigations. Sometimes all it requires is for a supervisor to take a moment to ask, "Did I approve that?" and potential losses can been avoided.

The OIG has investigators and auditors on staff with considerable expertise detecting and investigating fraud. Please remember that Paragraph 17 of the Grant Assurances requires grantees to contact the OIG immediately if there is reason to believe that an internal theft has occurred. You may want to remind your employees that there is an OIG Hotline at (800) 678-8868 or (202) 295-1670 and callers can remain confidential.

The OIG is also available for consultations to assist any LSC grantee in making sure it has adequate internal controls to help assure that all its funds are protected from internal theft. You may contact the OIG's chief investigator, Mike Shiohama, at (202) 295-1655, or by email at ms@oig.lsc.gov.