

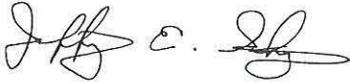


Office of Inspector General
Legal Services Corporation

3333 K Street, NW, 3rd Floor
Washington, DC 20007-3558
202.295.1660 (p) 202.337.6616 (f)
www.oig.lsc.gov

FRAUD ALERT 12-01-JS

TO: Executive Directors

FROM: Jeffrey E. Schanz
Inspector General 

DATE: January 18, 2012

SUBJECT: Advisory Bulletin on Recent Developments Regarding Fraudulent Activity Involving Checking Accounts at LSC-Funded Programs

The purpose of this Fraud Alert is to inform you about several checking account frauds against programs funded by the Legal Services Corporation (LSC). The frauds involved several instances of program checks being counterfeited or altered.

Counterfeit Check Fraud

Several programs have reported their checks being counterfeited. The checks were apparently designed and printed on personal equipment without professional help. The counterfeit checks were not exact copies but contained the program's correct checking account number and looked legitimate enough to be cashed. Several programs reported to OIG that a total of fourteen counterfeit checks were cashed for more than \$13,000 by merchants and banks.

Programs became aware of the counterfeit checks either from their bank or the program's checking account reconciliation process. In several instances, the banks noticed that the check numbers appearing on the counterfeit checks were significantly out of sequence from the checks currently being issued by the program. One of the banks also noticed that the name of the account holder printed on the check did not match the name of the program. Once alerted, the banks contacted the programs and confirmed the checks were counterfeit and the banks credited the accounts for the amount of the counterfeited checks.

Preventing Counterfeit Check Fraud

Programs probably cannot eliminate the possibility of someone designing and printing counterfeit checks, but programs can limit their exposure to counterfeit check fraud. One way to limit exposure is to consider using “positive pay” services that banks provide. When using “positive pay” services, programs provide their banks with a list of the check numbers and amounts that have been issued and are authorized to be paid. Checks that are not on the list will not be paid. Programs also can limit their exposure to counterfeit check fraud by performing a monthly reconciliation of their bank statements. The monthly bank reconciliation should ensure that the check numbers, payees, and amounts appearing on the cancelled checks accompanying the monthly bank statements agree with the program’s check register. Any discrepancy should immediately be reported to the program’s bank.

What Can Be Done After Counterfeit Checks Are Identified

Once counterfeit checks are identified, there are various ways to limit further exposure. Banks will put a “watch” on the affected checking accounts and more thoroughly review account transactions. Programs can decide to stop using the defrauded account and open a new checking account. In order to avoid having to pay “stop-payment” fees or having to re-issue checks, the old checking account can be left open with enough funds to cover only the amount of the outstanding checks.

Altered Check Fraud

Several programs also have reported that legitimate checks were altered. In one instance, a \$28,404 check payable to a vendor was diverted and the name of the payee was changed before the check was deposited. In another instance, a \$25 check was altered by the payee, a client of the program, and cashed for \$250. In both instances, the altered checks were cashed and funds were withdrawn from program checking accounts. The frauds fortunately were detected and the banks subsequently credited the programs’ checking accounts.

Preventing Altered Check Fraud

Unfortunately, altered check frauds are not uncommon. As with check counterfeiting, programs probably cannot eliminate the possibility of someone altering a check; however, preventive steps can be taken. Programs can have checks printed on security paper, which is difficult to alter, and also use special ink which reacts to tampering. Electronic payments, if feasible, can help. We also encourage programs to perform monthly reconciliations of their bank statements and to contact their banks to learn more about suggested procedures for preventing check fraud.

What Can Be Done After Altered Checks Are Identified

Once altered checks are identified, programs should promptly notify their bank. In the two instances described above, the altered checks were discovered by the programs in conjunction with their monthly checking account review and reconciliation process. In both instances, the programs notified their banks and the banks credited their checking accounts for the amount of the altered checks that had been processed against the accounts. If the programs had not done their due diligence on the accounts, the fraud may have gone undetected.

LSC Requires Bank Accounts to Be Reconciled

The Accounting Guide for LSC Recipients (2010) sets forth financial accounting and reporting standards for recipients of LSC funds, and describes the accounting policies, records, and internal control procedures to be maintained by recipients to ensure the integrity of accounting, reporting and financial systems. The Guide (p. 31) requires bank statements to be reconciled monthly to the general ledger. Proper reconciliation procedures will substantially increase the likelihood of discovering irregularities on a timely basis.

Conclusion

In all of the above cases, losses were prevented by the actions of the programs and the banks, which also credited the programs' accounts and charged the amount of the fraudulent checks back to the institutions that initially accepted the checks. The programs were inconvenienced, but through their actions and that of the banks, they did not suffer financial loss. Programs should not, however, rely solely on the efforts of their banks to detect fraudulent checks. It is essential that programs take appropriate steps to ensure the accuracy of their checking and other transactions. For further information about preventing and detecting counterfeit and altered check fraud, please see the attached publication "Check Fraud Federal Reserve System".

Utilizing the OIG as a Resource

The OIG, which has a highly-trained staff, including Certified Fraud Examiners and Certified Public Accountants, is available as a resource to help in preventing and detecting fraud. We are available to conduct Fraud Vulnerability Assessments (FVA), Fraud Awareness Briefings (FAB), or both at your program. An FVA involves a financial review of areas identified as being most vulnerable to thefts, such as purchase of supplies and services, petty cash, training, payroll advances, and travel reimbursements. Results are reported to you for your benefit.

An FAB is a presentation to program staff about topics such as who commits fraud, why people commit fraud, how fraud can be detected or prevented, and what to do if fraud is suspected. We also describe various types of fraud schemes perpetrated against LSC programs. The FAB provides an opportunity for staff to ask questions and make suggestions regarding ways to prevent fraud at their programs. The FVA and FAB programs have been responsible for helping to identify various frauds at LSC programs. Please contact us if you would like more information.

In addition to other LSC requirements, including the Accounting Guide for LSC Recipients, please remember that your program is required by LSC Grant Assurance ¶15 to contact the OIG immediately if there is reason to believe that your program has been a victim of fraud. Please periodically remind your employees that the OIG can be reached via confidential Hotline, (800) 678-8868 or (202) 295-1670, and by email at Hotline@oig.lsc.gov to report suspected fraudulent activities. They also may contact the OIG's Chief Investigator, Mike Shiohama, at (202) 295-1655, or by email at ms@oig.lsc.gov.

I hope you find this Fraud Alert useful. Of course, if you have any questions, please do not hesitate to call me directly at (202) 295-1677, or by email at js@oig.lsc.gov.

Attachment