



Office of Inspector General
Legal Services Corporation

The Fraud Corner

Preventing Checking Account Fraud through Bank Reconciliations and Positive Pay

As part of its Fraud Corner Series, the Office of Inspector General (OIG) is providing Legal Services Corporation (LSC) Grantees with the following information on “best practices” to potentially aid grantees in identifying or preventing fraudulent activity. The purpose of this article is to remind grantees of check and bank frauds that impact LSC funds and to update previously recommended steps to counteract such attempted frauds with information regarding available technology.

In 2012, the OIG issued [Fraud Alert 12-01-JS](#) to inform LSC programs regarding issues involving checking account frauds at LSC funded programs. The Fraud Alert addressed preventing and identifying counterfeit and altered check frauds and actions to be taken if such frauds are identified. The Fraud Alert stressed the need for programs to take appropriate steps to ensure the accuracy of their checking and other transactions. To that end, the OIG suggested that programs perform monthly reconciliations related to their checking accounts and to immediately report any discrepancies to their banks.

The Fraud Alert further reminded programs that the LSC 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 Accounting 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.

Since issuance of the Fraud Alert, grantees continue to report to the OIG check and bank fraud issues that have resulted in stolen funds. The OIG reiterates the need for monthly reconciliations and other appropriate financial practices. In addition, the OIG recommends leveraging technology to reduce the possibility of fraudulent transactions affecting checking accounts through the use of Positive Pay.

Positive Pay is a fraud-prevention system offered by most commercial banks to customers, for a fee, to protect the customers against forged, altered, and counterfeit checks. Positive Pay allows the banks to verify that the checks they process are funded properly. Under Positive Pay, when a customer issues payroll or other types of checks for the week or month, it sends a check register list to the bank. The information transmitted to the bank includes the check number, date, payee, and dollar amount, which the bank stores in its database. As the checks are presented to the bank for payment, the bank compares the information it has on file with each check presented.

If the information for any of the checks does not match the information in the customer-provided check register list, the bank notifies its customer through an exceptions report and withholds payment until the customer advises the bank to accept or reject the check. When the information does not match, this does not necessarily mean that the check cannot clear. The bank can flag the check, notify the customer, and seek permission to clear the check. If the customer finds there was a clerical error or other minor problem, the bank can be notified to negotiate the check.

Positive Pay can also eliminate the need for programs to incur fees related to the issuance of stop payments for stale or lost checks. The program would just need to notify their bank to remove the specific checks from the approved check register list.

Individual programs should consult with their respective banks regarding the availability and cost of Positive Pay.

If you have any questions or comments or would like additional information about this post please contact Daniel O'Rourke, OIG Assistant Inspector General for Investigations at (202) 295-1651 or by email Dorourke@oig.lsc.gov.