OFFICE OF INSPECTOR GENERAL
LEGAL SERVICES CORPORATION

FRAUD PREVENTION GUIDE
FOR LSC GRANTEES

OFFICE OF INSPECTOR GENERAL

AUGUST 2014

PROBLEMS (SOLUTIONS INSIDE BACK COVER)

- Problem 1: Frauds last a median of 18 months before being detected.
- Problem 2: Workplace fraud is more likely to be detected by a tip than by any other method.
- Problem 3: Workplace fraud is a significant threat to small organizations which typically employ fewer anti-fraud controls than their larger counterparts.
- Problem 4: Perpetrators with higher levels of authority tend to cause much larger losses and the longer a perpetrator has worked for an organization, the higher fraud losses tend to be.
- Problem 5: Most perpetrators are first-time offenders with clean employment histories.
- Problem 6: Most perpetrators show behavioral red flags often associated with fraudulent conduct such as financial difficulties.
- Problem 7: Nearly half of victim organizations do not recover any losses that they suffer due to fraud.

Source: Summary of Findings from the 2012 Annual Report to the Nation on Occupational Fraud and Abuse (Association of Certified Fraud Examiners)

http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

Introduction

The Office of Inspector General (OIG), Legal Services Corporation (LSC), has a statutory responsibility to conduct audits and investigations to prevent and detect fraud, waste, and abuse. Unfortunately, many LSC grant recipients have been the victims of fraud, suffering losses of hundreds of thousands of dollars or even, in one case, over one million dollars.

Frauds perpetrated against LSC grant recipients have involved false employee travel claims and office supply purchases. Employees were able to get away with falsifying travel records because of lax timekeeping practices and inadequate case management. Employees were able to make fraudulent office supply purchases because of weak internal controls, including those relating to the approval and validation of purchases.

This handbook discusses frauds involving timekeeping, travel, credit cards, accounting, payroll, office supplies, client trust funds, employee benefits, and Executive Directors. Each section is illustrated by examples drawn from actual OIG investigations and identifies which grantee personnel would most benefit from knowing about the relevant topic. The goal of the handbook is to help LSC grant recipients prevent fraud in the first place or detect fraud as soon as possible in the event it cannot be prevented.

We hope you find this information useful. Please contact the OIG at Office of Inspector General, Legal Services Corporation, 3333 K Street, NW, Washington, DC 20007, or visit us at www.oig.lsc.gov if you have any questions.

TABLE OF CONTENTS

Timekeeping

What is timekeeping fraud?
• Claiming hours not worked • Outside practice of law during grantee work hours • Claiming hours for work on grantee clients while working on restricted activities

Who should know about this topic?
• Supervisors who review and approve timesheets • Staff responsible for payroll • Executive staff with oversight responsibility

Why you should know about this topic?
• To prevent time and attendance fraud by encouraging greater supervisory review of employee work efforts and work hours. • To detect unauthorized outside practice of law by being able to identify indicators such as frequent absences or lack of work product to support hours charged. • To reduce travel fraud by identifying patterns or trends in hours charged that conflict with the timing or purpose of travel reimbursements claimed.

Title 45 C.F.R. § 1635.3(b) requires all case handlers employed by a grantee to record the amount of time spent on each case, matter, or supporting activity. Time records should be created contemporaneously and account for the amount of time spent on each activity. The importance of Part 1635.3(b) was the topic presented in an OIG podcast entitled “Timekeeping and Travel Fraud Presentation,” which is available at www.oig.lsc.gov.

A number of OIG investigations have found that grantee employees that were supposed to enter their time into the Grantee’s Case Management System (CMS) were not keeping contemporaneous time records; instead, they were recording their time as late as two weeks

from the time of the purported activity. Recipients' failure to closely review employee time entries has resulted in grantee employees:

- Working on cases while for their private clients while charging time to the grantee;
- Charging time for work on activities that are restricted under LSC guidelines;
- Claiming and receiving pay for hours not worked; and
- Falsifying hours worked in support of fraudulent travel reimbursements.

There are different CMSs available to LSC grantees to capture Part 1635.3(b) data, and each CMS contains time modules that have similar fields and formats. When conducting OIG field visits, we have observed that some grantees disabled or do not use fields that would help verify compliance with Part 1635.3(b) requirements.

In addition, OIG criminal investigations have uncovered cases in which grantee employees fabricated clients and activities that enabled them to charge time and create the illusion of work. Grantee employees also have submitted fraudulent mileage reimbursement claims in conjunction with fabricated clients. In most cases, it was the subjects' sloppiness and lack of attention to details that led to the identification of the fraud.

At the onset of a criminal or regulatory investigation dealing with time and attendance fraud, outside practice of law or other restricted activities, CMS data are one of the first types of evidence investigators request and analyze. Investigators use three data fields to identify anomalies in time and attendance entries:

- Transaction Identification Number (TRANS ID) - a CMS generated sequential number created for each activity entered by the employee.
- Creation Date - a CMS-generated date to record the date of a time entry.
- Activity Date – the date entered by the employee that represents when the work activity occurred.

Based on an analysis of these three fields, grantees can immediately identify employees who do not enter their time contemporaneously with their work. By comparing Creation Date against Activity Date, a grantee can measure the timeliness and frequency of time entries made by its employees. The Trans ID is a good way to identify employees who made their time entries in batch sequence (one after

another), and to identify transactions that were deleted from the system. By looking at the last number generated by CMS and the record count, one can quickly identify the volume of missing records.

For example, in Figure 1, the grantee employee entered his time eight work days after the work was performed. It can also be inferred that the employee made batch time entries, as the Trans ID numbers are continuous or close in sequence (i.e., there may be a gap of one or two numbers caused by other employees entering their activities into CMS at the same time).

Trans ID	Creation Date	Activity Date	EMP ID	Hours	Case No	Client ID	In Court Y(es)
131474	**2/12/10**	**2/4//10**	**1234**	3:10	13-xxyxxy	ANNNN	
131476	**2/12/10**	**2/4//10**	**1234**	4:02	12-xxxxxx	ANNNN	
131477	**2/12/10**	**2/4//10**	**1234**	1:27	Matter		

Figure 1

If your CMS does not have a Creation Date field, or the Creation Date field is not generally used, the Transaction ID number can be used to identify employees who do not make contemporaneous time entries. Since the Transaction ID is a sequential number, it is easy to detect out-of-sequence Activity Dates. By examining the highlighted fields in Figure 2, below, one can quickly see the out-of-sequence Activity Dates for employee 7777:

Trans ID	Activity Date	EMP-ID	Hours	Case No	Work Description	In Court Y(es)
1314426	2/1/2010	1234	8:00	13-xxxxx		
1314427	2/1/2010	1235	3:10	13-xyxx	Res/Read	
1314428	**1/26/2010**	**7777**	2:00	12-xxxx	Res/Read	
1314429	2/1/2010	1236	1:27	Matter	Con/Meet	
1314430	**1/26/2010**	**7777**	1:45	13-xxxx	Hearing	Y
1314431	**1/26/2010**	**7777**	2:45	13-xyxy	ResRead	
1314432	2/1/2010	1238	1:15	13-mssr	File/Copy	
1314433	**1/26/2010**	**7777**	2:00	Matter	Con/Meet	
1314434	2/1/2010	1240	5:56	13-xxxx	Res/Read	

Figure 2

After an employee has been identified as failing to adhere to the contemporaneous timekeeping requirements of Part 1635.3(b), a grantee should address the matter by performing other CMS checks, file reviews, and third-party verifications.

In most CMS there are other data fields that can be analyzed for fraud or prohibited activities. Some CMS time sections have an entry indicating whether the employee was "In Court." If the employee entered "Y(es)" there should be a corresponding entry on the court appointment calendar for the time and date of the court appearance. This is done not only to remind the employee of a court appearance but it also lets the office know that someone has to cover the appearance if the employee calls in sick. The lack of these types of entries may be indicators of fraud (or lead to complaints from the courts for missed appearances). Getting court docket information from the clerk's office is another way to determine whether an employee made an appearance. By checking with the clerk's office, you can determine if the client's case did in fact take place at the appointment time.

Good case oversight by supervisory attorneys can deter time and attendance fraud. In one OIG investigation, it became apparent that, had the supervisory attorney reviewed CMS entries made by a paralegal, the supervisor would have noticed the paralegal was making fraudulent CMS entries. Although the type of cases the paralegal handled generally involved one-time administrative court appearances for each client, with a second court appearance only required in the rare case of an appeal, the paralegal had routinely entered into the CMS system multiple court appearances relating to the same case.

Employee time entries can also be validated by comparing CMS case notes to client case files. If activities are recorded in the notes section of CMS, there should be some type of corresponding work product in the case file. In one investigation an employee entered into the CMS note section that she was picking up medical records, but the client files either had no medical records, or the medical record was received by mail and not picked up by the employee.

How can you prevent timekeeping fraud?
• Oversight and case reviews of case handlers • Compare time entries against case files • Executive and management staff setting tone at the top

Travel

What is travel fraud?
• Claiming travel expense that were not incurred • Inflating travel expenses for reimbursement • Claiming reimbursements for travel that is personal

Who should know about this topic?
• Supervisors who review and approve travel vouchers • Staff responsible for processing travel expense reimbursement • Executive staff with oversight responsibility

Why you should know about this topic?
• To deter and avoid travel fraud by clarifying the purpose of official travel • To identify trends in travel that may indicate the travel is for personal benefit with no business purpose • To reduce the risk of duplicate payments and math errors found in travel reimbursement claims

The LSC Accounting Guide for LSC Recipients requires each LSC grantee to establish and maintain adequate accounting records and internal controls procedures. As part of their internal control, grantees should develop forms and procedures for travel and especially for mileage reimbursement.

Mileage reimbursement is vulnerable to employee thefts resulting from travel claims for mileage that was not incurred, and for wages paid for hours not worked. In conducting mileage reimbursement fraud investigations, OIG investigators have observed two key control breakdowns that allowed the frauds to occur. First, the reimbursement forms lacked information to thoroughly document the mileage reimbursement; and second, the reimbursement forms were not properly reviewed.

By comparing CMS records, case files and travel forms, a determination can be made if travel was justified and actually occurred.

Analysis of frequency of travel by destination, day of week and purpose of travel also can identify suspicious travel trends. In two OIG investigations, the frequency of employees' travel to certain destinations was based on the mileage that could be claimed. By picking destinations that were the furthest from their office, the grantee employees were able to maximize the amount of money they could steal.

Even with the use of the most comprehensive mileage reimbursement form, the key to deterrence is having sound fiscal oversight. Review of travel reimbursement forms by local supervisors and fiscal staff should be thorough and not perfunctory. Amounts claimed should also be re-calculated to ensure accuracy. Employees are sometimes overpaid (or underpaid) because of miscalculations on their reimbursement claims.

In a number of OIG travel fraud investigations, we found that even where mileage was adequately recorded, the information provided on mileage reimbursement forms often lacked details about cases, clients, and the purpose of travel that would have facilitated fiscal oversight and review. Such detailed information should be included in all travel claims.

To deter mileage reimbursement fraud, a travel form should capture key information relating to the travel and the purpose for the travel. The travel form should be referenced in the grantee's policies and manuals, with clear language indicating what information is needed on the form, and specifying that reimbursements will not be made if the required information is not put into the form. Management should periodically review the implementation of these requirements.
The minimum information required on a reimbursement form to fully document mileage expense is captured in Figure 3, a sample Travel Voucher Form. The form should include the following types of information (some are self-explanatory):

- Date of travel
- Origin – states whether travel started from home, work or other location
- Destination - identifies where travel terminated
- Odometer readings – a tamper-proof number that can be verified
- Mileage claimed
- Amount of reimbursement
- Other expenses such as parking and tolls
- Case number or client name
- Purpose of travel

- Signature of the traveler and supervisor
- Date signed and date approved

The uses of mileage charts and online mapping products like MapQuest and Google Map are other methods used by grantees to calculate mileage reimbursements. The key to prevention when using one of these tools is to make sure the purpose of travel and client name or case number are required entries on the reimbursement forms.

How can you prevent travel fraud?

- In addition to the expenses incurred, have travel reimbursement forms report the purpose and details of the trip
- Require that all employees who seek reimbursement complete all required entries on the travel form, including required authorizations and approvals
- Supervisors and accounting staff conduct thorough reviews of travel vouchers to insure completeness of

Travel Reimbursement Form

Employee Name

Date	Origin	Destination	Odometer Beg	Odometer End	Mileage	Other expenses Type	Amount	Case # or Client	Purpose

Signature:_____ TOTAL @ .555 = A TOTAL = B

Approved:_____ TOTAL REIMBURSEMENT A+B=

Figure 3

Credit Cards

What is credit card fraud?
• Obtaining cash advances for non-business purposes • Purchasing items for personal uses • Using the card to pay personal bills for cell phones, gym memberships and television cable services

Who should know about this topic?
• Supervisors who review and approve credit card transactions • Accounting staff responsible for reconciling credit card transactions to credit card statements • Executive staff with oversight responsibility

Why you should know about this topic?
• To deter the misuse of credit cards for non-business or personal benefit • To identify the unauthorized uses of credit cards for cash advances • To reduce the risk of loss due to the unauthorized uses by persons unknown to the organization

Grantee credit cards have been vulnerable to employee embezzlements through the purchase of items for personal consumption, items purchased for resale, or cash advances. In a majority of the OIG cases the card holder was in grantee management. As in most credit card transactions, the card holder's activities were not transparent to the grantee staff as they were usually point-of-sales (POS) transactions, telemarketing purchases or purchases made over the internet. The same holds true for automated teller machine (ATM) withdrawals. Frauds carried out through the use of a credit or ATM card often go undetected because the only evidence of purchases or monetary withdrawals is a monthly credit card statement which may not be independently or adequately reviewed.

Improper transactions identified through OIG investigations have included the purchase of meals at restaurants; gas for personal cars; items used for private hobbies and personal businesses; and items that have a high resale value. In many cases embezzlers have avoided detection by destroying the detailed section of the credit card statements, and requesting payment by submitting only credit card statement payment vouchers. In one case an employee was able to embezzle over $40,000 by such means. Had the employee provided the detailed sections of the credit card statement for review prior to payment, accounting personnel would likely have noticed the repetitive purchases of multiple high dollar items that had no business purpose for the grantee and which were resold by the suspect on eBay.

Another weakness OIG investigators have found in the payment of credit card statements is a lack of supporting documentation for each transaction. During reviews of credit card transactions the OIG has found that POS receipts, sales invoices, or other types of documents to record the purchase of items were sometimes not submitted by the card holder. Such documentation should be provided to accounting personnel for reconciliation of the transaction with the credit card statement. A reconciliation of credit card purchases by the grantee serves two purposes: to verify that each transaction has a legitimate business purpose; and to properly allocate the costs associated with the purchase.

Many credit card cases involve senior-level employees. The Executive Director in one program and the Chief Financial Officer in another were able to get credit card cash advances through ATMs at gambling establishments. Two control breakdowns allowed these cash advances to be made. First, the employees were able to get pin numbers for grantee credit cards that had no need for cash advances; and second, the person who used the card was also the person who received and reviewed the credit card statement for payment.

For a majority of the grantees visited by the OIG the purpose of the credit card is to pay for goods, services and filing fees paid by the grantee. There is no business reason for a pin number to be activated for a credit card, as cash advances are requested by employees and issued in the form of a check to cover anticipated business travel. There is also a need to insure proper internal controls are in place so that employees who are issued a grantee credit card are not part of the review process of the credit card statement. The incidents described above could have been avoided had neutral parties reviewed the credit card statements. In the case of an ED, a Board member can review transactions and statements.

Good internal controls dictate that those who spend funds are not the same individuals who receive, review and pay for the transactions. Make sure you know how many credit cards you have, each card's dollar limit, and who has been issued a card. It is also important to make sure each financial transaction is documented and reconciled to the credit card statement before making payment. Also, you may wish to inquire whether the credit card company will decrease the amount of funds available for cash advances, or eliminate cash advances altogether.

How can you prevent credit card fraud?

- Eliminate the cash advance feature on the credit card if possible
- Make periodic checks with the card company to verify that no personal identification number (PIN) was issued for the cards
- Require that credit cards are assigned to individuals and that they maintain possession and control over the cards(s) at all times
- Require receipts for each transaction and reconcile the receipts to the monthly billing statement

Accounting

What is accounting fraud?
• Accounting staff can embezzle from the checking account under the guise of a business payment • Accounting staff can use grantee funds to pay personal expenses • Accounting staff can steal through ATM withdrawals or cash advances • Fiscal and grantee staff can steal client funds and use grantee funds to pay client fee obligations

Who should know about this topic?
• Staff responsible for bank reconciliations • Executive staff with oversight responsibility

Why you should know about this topic?
• To deter the embezzlement of grant funds through the checking account and general ledger • To identify unauthorized withdrawals from the checking account • To detect late or missing cash receipts from clients and donors

Timely and thorough bank reconciliations are instrumental in avoiding accounting frauds, external thefts and the embezzlement of client trust funds. Accounting fraud is the embezzlement of grantee funds through the general checking account under the guise of a fictitious expenditure recorded in the general ledger. External thefts are those where a counterfeit or stolen grantee check or fraudulent wire transfer is used to steal grantee funds. Client trust funds can be stolen from grantees who receive cash or money orders from their clients.

Good internal controls dictate that bank reconciliations be performed by someone who does not handle the payment of expenditures or the deposit of funds. It should include a review of voided, out-of-sequence and missing checks. In embezzlement cases investigated by the OIG, the subjects posted entries in the general ledger for what looked like a

legitimate business expenses, making the checks payable to themselves and then cashing them.

This type of accounting fraud can be prevented by a thorough and independent bank reconciliation conducted by a neutral party who is not involved in the check writing or bank deposit process. The reconciliation as depicted in Figure 4, should include a comparison of the bank statement, selected checks, and the general ledger to insure the amounts and names of payees match. In the example below, Robert Jones, the grantee's accountant, wrote a check to himself and disguised this payment in the check register and general ledger as payment for the grantee's Verizon Wireless bill.

CHECK REGISTER

Date	Check	Payee	Amount	Balance
01/03/12	18031	Water Authority	250.00	10,705.10
01/10/12	18032	Power Company	675.27	10,029.83
01/12/12	18033	Verizon Wireless	525.00	9,504.83
01/12/12	18034	Western NY Life	899.00	8,605.83
01/12/12	18035	Polish Spring Water	139.68	8,466.15

GENERAL LEDGER	Type	Date	Check Num	Name	Amount
2000 Accounts Payable	Bill Pmt -Check	1/10/12	18031	Water Authority	250.00
2000 Accounts Payable	Bill Pmt -Check	1/12/12	18032	Power Company	675.27
2000 Accounts Payable	Bill Pmt -Check	1/12/12	18033	Verizon Wireless	525.00
2000 Accounts Payable	Bill Pmt -Check	1/12/12	18034	Western NY Life	899.00
2000 Accounts Payable	Bill Pmt -Check	1/12/12	18035	Polish Spring Water	139.68

GRANTEE CHECK 18033

1/12/12

Pay to : Robert Jones $525.00

the order

Memo: _____ Program F.D

Figure 4

In cases involving stolen and counterfeit checks, bank reconciliations serve as an early warning to the program. Timely and thorough bank reconciliations can identify the external theft of grantee funds by unknown parties who are negotiating counterfeit or stolen checks from the grantee's account. Banks generally give their customers 60 days to notify them of fraudulent or erroneous transactions and take corrective actions. Once this time period has elapsed and the bank has not been

notified of a suspicious transaction, the grantee will be responsible for any resulting loss of funds.

This is another reason the OIG looks at voided checks and the securing of blank check stock: securing and defacing voided checks ensures that no one will try to negotiate them at a later date. Securing blank check stock makes it difficult for someone to get a series of checks and pass the checks for money, goods or services. If checks are stolen from the program, they will usually show up in the bank reconciliation as checks issued out-of-sequence and should be looked at closely during reconciliations.

The same process should be followed for the reconciliation of bank deposits. The person who makes the deposit should not be the person who reconciles the account. Cash receipts should be handled like checks and check stock. They are issued in sequence and voided cash receipts are retained with issued receipts. Blank cash receipt stock should be secured like check stock.

The review of cash deposits should include a comparison of the date on the cash receipt to the date the fund was posted to the general ledger or client trust, and the date of deposit.

How can you prevent accounting fraud?

- Having someone who does not write checks conduct monthly bank reconciliations
- Eliminate or place tight controls on the ATM card
- Make sure all transactions are fully documented

Payroll

What is payroll fraud?
• Payroll personnel who pay themselves multiple salary advances with no intent to repay or offset the advance • Personnel who handle payroll that steal and divert funds to their personal accounts • Personnel who handle payroll personnel adding hours to their timecard for additional pay

Who should know about this topic?
• Accounting staff who handle payroll • Human resources staff who handle personnel actions affecting payroll • Executive staff with oversight responsibility

Why you should know about this topic?
• To deter embezzlements by employees who have access to the payroll system • To identify ghost employees receiving pay • To identify trends and patterns for abuse of overtime • To identify the abuse of salary, such as payday loans

The OIG has investigated grantee payroll issues, including abuse and fraud of salary advances and the fabrication of pay records where the grantee uses a vendor payroll service. Payroll is the largest cost center for grantees, averaging 70 to 80 percent of their budgets. This section applies for grantees that allow employees to have more than one outstanding salary advance and/or use a vendor payroll service (VPS) such as ADP to process payroll.

In two OIG investigations, grantee employees paid themselves multiple salary advances, sometimes as many as six advances in one week. In the first case, an employee who worked in the accounting unit paid himself approximately $25,000 in salary advances within a four-week

period. The employee then terminated his employment with no intention of reimbursing the grantee for the salary advances.

The second case involved $120,000 in fraudulent salary advances paid to the ED and CFO, as well as a paralegal (the CFO's daughter). In an attempt to offset the advances, the ED and CFO fabricated backdated timesheets to reflect extra hours worked as compensatory time (comp time), covering the period for which the salary advances were paid. A review of timesheets disclosed that the CFO added as much as 70 hours of comp time to her 40 hour work week over a period of three months.

In an effort to offset the advances they had received, the ED and CFO tried to get the grantee Board of Directors to modify the comp time policy allowing employees to either take the time off or receive pay for each hour of comp time worked.

The OIG has also worked non-criminal cases where the grantees allow multiple salary advances and the advances are carried for a long period of time without offsets to future pay or reimbursements. Even though the grantee had policies that gave clear direction on limiting the amount of outstanding salary advances, as well as instructions on how to reimburse the advances, multiple advances were allowed to be carried over from one year to the next.

The OIG has also found financial risk for grantees that use VPS. In both OIG investigations dealing with VPS, grantee employees who had administrative (super-user) access to the VPS system were able to manipulate data to earn more pay.

In the first case, an employee with super-user access was able to change an inactive employee's direct deposit information in VPS and direct this person's pay to the super-user's own account. The employee was then able to add work hours to the VPS system for the inactive employee, resulting in a VPS paycheck being deposited in the super-user's account.

After receiving the fraudulent pay from VPS, the super-user changed the direct deposit information back to the in-active employee's account. This scheme worked for some time because the in-active employee was not expecting to be paid, and the supervisor for the in-active employee never checked the payroll register for her unit to verify pay.

In the second case, a super-user was able to add overtime hours to the VPS system for herself and a friend. The grantee had a review and

certification process in its VPS system to safeguard against unapproved overtime: prior to the release of payroll data to the VPS, unit supervisors were required to review and certify payroll for their employees. The super-user, however, was able to circumvent this review by placing the overtime pay into the VPS system after the supervisory review and certification process had been completed.

To prevent and detect these types of payroll frauds involving VPS systems, the ED, CFO, and an employee from Human Resources (HR) should request and review the VPS transaction/change report for each pay period. This report can be used to identify the following types of changes processed by a super-user:

- Overtime entered by the super-user (overtime is entered by the employee into the timekeeping system); and
- Establishment or alteration of direct deposit accounts in VPS by the super-user (this is usually an HR function).

It is also recommended that the VPS system be set up to generate emails to employees when changes are made to their VPS profile (such as changing the direct deposit account).

How can you prevent payroll fraud?

- Limit salary advances to one outstanding advance at a time
- Require that employees who receive a salary advance have an adequate leave balance to offset the amount of the advance
- Establish a firm repayment schedule to recoup advances from future pay
- Compare approved payroll summaries to actual pay
- Make a comparison of total pay for each pay period to identify any significant changes from one pay period to another
- Review and validate entries on the payroll vendor transaction report that add overtime and work hours to an employees pay

Office Supplies

What is office supplies fraud?

- Employees purchasing items for personal uses or resale
- Employees who place orders are receiving kickbacks from the vendors
- Employees purchasing items at inflated cost from relatives and family friends

Who should know about this topic?

- Supervisors who review and approve the purchase of supplies
- Staff responsible for placing orders and receiving office supplies

Why you should know about this topic?

- To deter the purchase of supplies or services that do not have a business purpose and are for personal consumption
- To identify conflicts of interest and kickback schemes between the vendor and person(s) placing supplies orders

The OIG has investigated two different fraud schemes dealing with the purchase of office supplies. The first scheme involved a vendor kickback relationship with the grantee CFO that resulted in a $2.5 million loss to the program. The second scheme involved the purchase of office supply items for personal use or resale.

In the first scheme, the CFO had a friend establish, in name only, an office supply company (OSC) as a façade to expense grant funds for conversion to cash. The CFO and his friend kept 90 percent of all grantee funds spent on office supplies, with the CFO keeping approximately 75 percent of the overall purchase transactions. The OSC kept 15 percent of the overall purchase transactions and used the remaining 10 percent to actually purchase supplies from a nationally-known vendor.

After reviewing all documents related to the transactions, OIG investigators could only track 10 percent of the funds to the actual delivery of office supplies. There was no correlation between the purchases orders placed with the OSC and items delivered to the grantee by the office supply vendor. The CFO confessed that these documents were used as a means to further the embezzlement of grantee funds. The kickback scheme between the CFO and the OSC went undetected for 10 years.

The OIG also undertook two investigations in which grantee employees purchased items for personal consumption, or items that could easily be sold on eBay. The employees were in positions at their respective programs where they placed the orders, received the items purchased, and received the invoices from the vendors. The grantees' failure to separate duties relating to the purchase of office supplies allowed the employees to conceal their embezzlements.

How can you prevent office supplies fraud?

- Compare office supply prices to a nationally known vendor's catalog
- Search the internet to see if the office supply provider has a website
- Check local telephone directories to see if the vendor is listed
- Review the purchase order or invoice to see if the purchased items fit the needs of the program
- Look for anomalies on vendor invoices
- Determine whether the quantities of items purchased seem proportionate to the needs of the program
- Ensure separation of duties in the approval process for purchasing office supplies, including placement and receipt of orders
- Use a purchase order that contains a list of office supplies that are permitted to be ordered
- Determine if the delivery address is one typically used by the program
- If the grantee has multiple branch offices that can place office supply orders, vendor invoices should be sent to central accounting

Client Trust Funds

What is client trust fund fraud?
• Employees borrowing or stealing money received by clients

Who should know about this topic?
• Supervisors who have client trust fund accounts • Staff responsible for receiving and depositing client funds • Accounting staff who conduct client trust fund account reconciliations • Executive staff with oversight responsibility

Why you should know about this topic?
• To deter the loss or theft of client funds • To identify kiting schemes in which funds are borrowed and deposited at a later date • To identify schemes in which client funds are received and kept by the employee and the employee uses grantee funds to pay for the client's fee obligation

The LSC Accounting Guide requires grantee client funds to be deposited in a separate client trust account designated only for that purpose and not commingled with the program's operating funds. Additionally, a client trust accounting system must have a process to document the receipts of a client's funds; document the disbursement of a client's funds; and ascertain at any time each client's trust balance.

Client trust fund thefts can be identified through bank reconciliations of monthly deposits as discussed previously. Programs that receive cash from their clients must have a documented process to receipt clients for cash deposited into trust accounts. Grantees' cash receipts should be numerically controlled, used in sequential order, and treated as an accounted instrument. Like voided checks, voided cash receipts should be defaced to prevent further use and then saved for future review.

Periodic review should be performed to insure that cash receipts are in the proper sequence and all receipts are accounted for, including voided receipts.

There should be adequate signage in the office to let clients know that your services are generally free, but in the event clients are required to provide money to the program, they will receive a receipt. The advocates should also make it part of their protocol to explain to clients the purpose of collecting money to pay for fees or other legal expenses, and to inform clients that they will receive a receipt if they do provide money to the program.

In one case investigated by the OIG, clients gave cash to a grantee employee to cover fees associated with their cases and were not receipted for the money. The employee kept the money and used grantee funds, or received a fee waiver to take care of the client's fee obligation. This example illustrates the need for proper signage and the proper uses of cash receipts, as the clients received the end results associated with their fees and therefore had no reason to complain. Since there were no client complaints about lack or delay of services to alert the grantee of a problem, the employee was able to continue the embezzlement scheme for 18 months.

As cash is received and receipted it should be provided to the person responsible for preparing deposits; the deposit should then be immediately posted to the bank account and the client's trust account. The cash deposit should be made as soon as practicable.

Based on OIG investigations untimely deposits of cash can lead to theft of funds and mistrust of grantee employees. In most situations multiple employees have knowledge of and access to cash received by the grantee, which can make it difficult to affix responsibility to an individual when money is stolen. If a situation arises that does not allow for the timely deposit of cash, policies and procedures should be in place to clearly place responsibility for the money on a particular individual until a deposit can be made.

How can you prevent client trust fund fraud?

- Make sure clients know they are to be receipted for money given to the program
- Use pre-numbered cash receipts, and issue the receipts in sequential order
- Account for all voided cash receipts

Employee Benefits

What is employee benefits fraud?
• Employees who improperly place individuals as beneficiaries on their grantee benefits plan who do not meet the eligibility requirements of the plan • Employees who do not remove beneficiaries from the plan when required

Who should know about this topic?
• Human Resources staff who administer the employee benefits plan • Executive staff with oversight responsibility

Why you should know about this topic?
• To deter employee benefit fraud • To reduce and avoid the cost of providing employee benefits to persons who are ineligible for coverage

The cost of healthcare, dental, or other employer-sponsored employee benefit plans is usually dependent on the employee's marital status, family size, and/or meeting a condition established by the insurance carrier for domestic partners.

During the course of OIG investigations it has been observed that grantees often do not have the expertise to prevent the improper enrollment of individuals as beneficiaries on employer-sponsored plans. Also, grantees generally do not take proactive steps, such as conducting periodic reviews, to determine changes in the eligibility status of plan beneficiaries. Among the factors that can affect eligibility are marriages and divorces; birth or adoption of a child; death of a spouse or child; and dependent children reaching their 26th birthday.

In two OIG investigations, employees included ineligible persons as beneficiaries for grantee-paid healthcare coverage. In one case an employee kept her ex-spouse on the health plan after their divorce was final. In another case, a human resources employee placed her

domestic partner on the grantee health plan knowing that the partner did not meet the criteria for coverage.

Given the high cost of healthcare and dental insurance, and the prospects of increasing cost for employers, it is more important than ever that grantees ensure that only persons who are eligible for coverage are enrolled in healthcare, dental, and other employer sponsored benefit plans.

How can you prevent employee benefits fraud?

- Clearly explain to employees the eligibility requirements for beneficiaries of employer-paid healthcare and dental coverage Periodically remind employees of their responsibility to report changes that affect beneficiary eligibility
- Ensure that enrollment forms are completed and signed (omitting information on the enrollment form or not signing could be indicators of fraud)
- Inform employees about the additional cost incurred by the program and/or employees when an ineligible person is included on the plan
- Make a particular employee responsible for knowing and enforcing healthcare and dental eligibility requirements to reduce the opportunity for improper enrollments
- Periodically review healthcare participants' coverage to identify questionable enrollments and then conduct further inquiry to determine changes in marital status or other factors that could affect eligibility
- If warranted, require submission of documentation verifying eligibility, such as a marriage certificate or affidavit.

Executive Directors

What is executive director fraud?
• Frauds involving executive directors include travel fraud, time and attendance fraud, credit card fraud, outside practice and accounting fraud

Who should know about this topic?
• Board Members • Executive Directors

Why you should know about this topic?
• Some Executive Directors have been involved in fraud and misconduct • Lax Board supervision and lack of accountability have led to problems • Board supervision of Executive Directors is critically important

The OIG has received a considerable number of complaints regarding Executive Directors of LSC-funded programs. While some complaints resulted in insignificant findings or no findings at all, a number led to findings that Executive Directors were involved in improper conduct, including fraud, questionable business expenditures, outside practice of law, time and attendance fraud, lobbying, and mismanagement. Misconduct by Executive Directors has resulted in a range of sanctions, including criminal prosecution, de-funding and closure of the program, and the imposition of special grant conditions.

The following are some examples of OIG investigative findings involving Executive Directors with fraud, questionable expenses, outside practice, lobbying, time and attendance issues, and mismanagement:

Fraud

- Embezzling over $30,000 through salary advances that were never repaid;

- Approving and receiving improper bonuses; and
- Cashing of donor checks and failing to give the proceeds to the program.

Questionable Expenses

- Charging over $100,000 in questionable expenses for cars, meals, and travel;
- Incurring over $15,000 in questionable expenses, including travel to family events;
- Charging travel and meal expenses for work performed for other organizations;
- Using the program credit card to charge $8,000 for purchases and cash advances from casinos; and
- Receiving $7,000 in travel advances and $20,000 in salary advances, most of which were not repaid.

Outside Practice

- Conducting an outside practice of law, which generated about $69,000 in fees, while using program staff and resources;
- Using the program name on outside-practice pleadings and using program staff and resources to represent family members;
- Representing a local politician in a prohibited criminal matter; and
- Performing outside consulting work without Board approval.

Lobbying

- Telling OIG that the program was asked to testify before the legislature but failing to report that the program solicited the invitation; and
- Not providing evidence of a lobbying request; using LSC funds to lobby; and failing to report lobbying to LSC.

Time & Attendance

- Being paid for 39 days while not working or taking leave;
- Not being in the office for 251 out of 505 workdays over a two-year period;

- Claiming to work on program matters while actually working on personal matters;
- Spending work time at casinos and coming to the office only a few days each week; and
- Submitting timecards for hours not worked and spending only a few days per week in the office.

Mismanagement

- Allowing three full-time staff attorneys to conduct paid outside law practices during program time;
- Authorizing an ineligible family member to be represented by the program;
- Approving personal travel expenses and payroll advances for an employee and not seeking reimbursement;
- Signing blank checks and allowing unreimbursed salary advances of over $150,000;
- Allowing a staff attorney to represent the ED's relative in a prohibited matter;
- Failing to adequately supervise an employee who embezzled $20,000 and received $13,000 in improper payroll advances and expense reimbursements;
- Failing to adequately supervise paralegals;
- Not reporting an employee theft to the OIG;
- Failing to adequately supervise two attorneys in field offices, thereby enabling them to conduct paid outside law practices; and
- Failing to adequately supervise an employee who embezzled $188,000.

As can be seen from the above examples drawn from actual OIG investigations, Executive Directors, like other employees, can find themselves doing the wrong thing for any number of reasons. Financial pressures from living expenses, tax liens, bankruptcy, gambling, drinking, and family problems have led to some of the problems with Executive Directors that the OIG identified. In many instances, improved Board supervision of ED activities would have either eliminated or at least reduced the opportunity for wrongdoing.

The prevention suggestions are not meant to be all-inclusive or mandatory. As a result of problems encountered with EDs, however, many LSC-funded programs have successfully adopted such measures. The OIG recommends that each program consider adopting

some or all of the foregoing policies as a means of ensuring appropriate supervision of their EDs.

.

How can you prevent executive director fraud?

- Identify potential financial pressures on the ED by conducting periodic credit checks
- Address addiction and similar problems that may affect EDs (and other employees) by providing an employee assistance program
- Apply all appropriate personnel rules and other program policies to the ED
- Create a code of conduct that applies to all employees, regardless of status, as well as the Board of Directors
- Require the ED to report periodically to the recipient's Board of Directors on expenses (e.g., those associated with travel) that have been approved by subordinate employees
- Pay close attention to ED's use of program credit cards, motor vehicles, and staff resources for non-business-related purposes
- Assure program employees that they can report concerns about the ED confidentially and without fear of reprisal to their Boards of Directors as well as to the OIG Hotline
- Report concerns promptly to the OIG concerning the ED and take appropriate disciplinary and legal action
- Develop a succession or continuation of operations plan in the event the ED is placed on leave or removed
- Establish an audit committee which includes at least one member (either a current Board member or an outside consultant) who is knowledgeable about fiscal oversight (e.g., a certified public accountant)
- Hire a qualified chief financial or fiscal officer to work under the ED's supervision but with authority to report directly to the Board of Directors.

APPENDIX A
SUMMARY OF RELEVANT LSC GRANT REQUIREMENTS

Under LSC Grant Assurances, the grantee will notify the OIG within two (2) business days of the discovery of any information that gives it reason to believe it has been the victim of a loss of $200 or more as a result of any crime, fraud, misappropriation, embezzlement, or theft involving property, client funds, LSC funds, or non-LSC funds used for the provision of legal assistance; or when local, state, or federal law enforcement officials are contacted by the program about a crime. It also will notify the OIG if it has been the victim of a theft of items (such as credit cards, check stock, passwords, or electronic access codes) that could lead to a loss of $200 or more. The required notice shall be provided regardless of whether the funds or property are recovered. Once the grantee has determined that a reportable event has occurred, it agrees it will contact the OIG before conducting its own investigation into the occurrence. Grantees can call the OIG Hotline (Telephone: 800-678-8868 or 202-295-1670; E-mail: hotline@oig.lsc.gov; or Fax: 202-337-7155).

Grant recipients should use the LSC Accounting Guide for LSC Recipients, Appendix VII Accounting Procedures and Internal Controls Checklist, in conjunction with this handbook, as a guide to measure their internal controls and identify areas of financial risk.

Finally, please remember that 45 C.F.R. § 1640.3, “Contractual Agreement,” requires each recipient, as a condition of receiving LSC funds, to enter into a written contractual agreement with LSC that it will be subject to the Federal laws listed in 45 C.F.R.§ 1640.2(a)(1) . The recipient must also acknowledge that all of the program’s employees and board members have been informed of such Federal laws and the consequences of violating such laws.

APPENDIX B
ACCOUNTING FRAUD CHECKLIST

YES	NO	N/A	CREDIT CARDS
			Is there a credit card policy?
			Does your program issue credit cards?
			Does the program maintain a control list that identifies card holder and credit limits?
			Does the card holder receive the monthly credit card statement?
			Are there a receipts or other type of documents to support transactions?
			Does someone other than the card holder reconcile the credit card statement?
			Does the credit card have provisions for cash advances?
			Does the account have a PIN number associated with the credit card?
			Is there way to check for cash advances on the credit card statement?
			Is the credit card secured when not in use?
			Is the credit card statement reviewed to ensure all purchases have a business purpose?
			Has your program paid any credit card finance charges or late fees?
			Does your credit card offer a rebate or rewards program?
			Do you use the rebate or reward program?
YES	NO	N/A	BANK RECONCILIATIONS
			Is there a bank reconciliation policy?
			Does the policy require monthly and timely reconciliations?
			Are all bank accounts reconciled?
			Is there a policy on voided checks?
			Are voided checks retained as required by policy?
			Are voided checks defaced as required by policy?
			Is there a policy on blank check stock?
			Is blank check stock secured as required by policy?
			Does someone other than the check preparer or signatory do the reconciliation?
			Does the program use pre-numbered cash receipts?
			Do the cash receipts identify the person who received the cash?
			Is a different person used to prepare the bank deposit?
			Is a different person used to make the bank deposit?
			Are cash deposits timely?
			If cash cannot be deposited, does the program have secure overnight storage?
			Is accountability for the cash affixed while in the custody of the grantee?
			Is there a periodic spot check between cash receipts, deposit slips and bank statements?

APPENDIX C

ACCOUNTING GUIDE FOR LSC RECIPIENTS (2010)
Chapter 3-6 - Fraud Prevention

1. Practice reasonable segregation of duties.
2. Reconcile bank accounts promptly.
3. Reconcile GL accounts promptly.
4. Keep accounting and personnel policies and procedures current.
5. Provide adequate employee training.
6. Control access to check stock, on-line banking software, accounting software and payroll software.
7. Do not share passwords.
8. Do not allow unauthorized software to be installed on business computers.
9. Limit access to financial records.
10. Limit credit card users and set credit card spending limits.
11. Maintain limited balance bank accounts for certain activities.
12. Assign permissions and authorizations deliberately and only as needed.
13. Change passwords and access codes periodically.
14. Delete old passwords and users immediately.
15. Have thorough and well documented hiring practices and procedures.
16. Employ strict office security policies and procedures.
17. Take advantage of banking services such as e-mail notifications for certain transaction, positive pay services, ACH filters, blocks on certain transactions, on-line banking features and on-line credit card account review features.
18. Make sure your computer network has robust and updated security processes, firewalls, anti-virus protection, spyware protection and other intrusion detection software.
19. Have a “Whistleblower Policy” in place that provides assurances that retaliation will not occur when an employee, board member or volunteer reports suspected fraud.
20. Have a “Conflict of interest Policy” on place for management and the board of directors.

21. Remind and refer employees to the state bar association's professional ethics requirements, applicable federal and state laws and the organization's code of conduct, at least once per year.
22. Remind board members that the applicable federal and state laws also apply to them. 45 CFR §1640.3, "Contractual Agreement" requiring the following:
23. As a condition of receiving LSC funds, a recipient must enter into a written contractual agreement with the Corporation that, with respect to its LSC funds, it will be subject to Federal laws listed in §1640.2(a)(1). The agreement shall include a statement that all of the recipient's employees and board members have been informed of such Federal law and the consequences of a violation of such law, both to the recipient and to themselves as individuals.
24. Have well defined expense reimbursement policies and strict expense documentation requirements.
25. Involve the board and executive management in internal control policies and oversight efforts.
26. Promptly follow-up on any internal control finding, discrepancies, issues, weaknesses, comments or suggestions from internal auditors, external auditors, government agencies, employees, grantors and others.
27. Have a policy for what to do if you uncover fraud. When fraud (over $200) is suspected or discovered a recipient is required to notify the LSC Office of Inspector General within two (2) working days.

[END]

Notes

Notes

Notes

SOLUTIONS (PROBLEMS INSIDE FRONT COVER)

- Solution 1: Learn about how to detect fraud sooner by reading this guide and accept fraud detection as another management responsibility.
- Solution 2: Encourage employees to report concerns and publicize the OIG Hotline and do not rely too heavily on annual audits.
- Solution 3: Employ appropriate anti-fraud controls.
- Solution 4: Hold everyone accountable.
- Solution 5: Understand that many frauds are committed by reputable employees.
- Solution 6: Refer employees having financial difficulties to available assistance programs.
- Solution 7: Maintain adequate fidelity insurance coverage as required by LSC grant conditions.

Legal Services Corporation
America's Partner For Equal Justice

OFFICE OF INSPECTOR GENERAL HOTLINE

IF YOU SUSPECT

FRAUD INVOLVING LSC GRANTS OR OTHER FUNDS
WASTE OF MONEY OR RESOURCES
ABUSE BY LSC EMPLOYEES OR GRANTEES
VIOLATIONS OF LAWS OR LSC REGULATIONS

PLEASE CALL OR WRITE TO US AT

PHONE 800-678-8868 **OR** 202-295-1670
FAX 202-337-7155
E-MAIL HOTLINE@OIG.LSC.GOV
MAIL P.O. BOX 3699
WASHINGTON, DC 20027-019

UPON REQUEST YOUR IDENTITY WILL BE KEPT CONFIDENTIAL
REPORTS MAY BE MADE ANONYMOUSLY