Office of Inspector General
Legal Services Corporation

Inspector General
Jeffrey E. Schanz

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

FRAUD ALERT
21-0154-A-FA

TO: Executive Directors

FROM: Jeffrey E. Schanz,
Inspector General

DATE: September 20, 2021

SUBJECT: Fraud Alert: Prompt Reporting of Potential Fraud Indicators to the Office of Inspector General

---

Every few years, the Office of Inspector General (OIG) for the Legal Services Corporation (LSC) distributes a Fraud Alert that describes the most recent fraud indicators the OIG has observed when investigating grant fraud schemes at LSC-funded programs.

Previously issued Fraud Alerts describing potential fraud indicators as observed by the OIG:

Fraud Alert 15-01 (issued April 10, 2015)

Fraud Alert 18-0053-A-FA (issued March 28, 2018)

Note: Although not directly addressed in the current alert, it is important for grantees to be aware of previous indicators because the threat posed by those indicators still exist.

The OIG recognizes that many grantees implement strong internal controls in your programs. This Fraud Alert is being issued to grantees to inform you of fraud indicators uncovered by OIG investigations since 2018 and to highlight the importance of grantee employees alerting the OIG to potential indicators of fraud, waste, and abuse of program funds. In doing so, the OIG intends to help prevent your program from being a victim of fraud.

LSC Grant Terms and Conditions require a grantee to notify the LSC OIG Hotline within two business days of:

- discovering information indicating that you have been the victim of a loss of $200 or more as a result of any willful misrepresentation or theft, fraud, misappropriation, embezzlement, or theft involving property, client funds, LSC funds, and/or non-LSC funds used for the provision of legal assistance;
- reporting a crime to local, state, or federal law enforcement officials;
- discovering that you have 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; or
- that any of your key officials or employees with control over your finances are charged with fraud, misappropriation, embezzlement, theft, or any similar offense, or are suspended or disciplined by a professional licensing organization.

LSC Grant Terms and Conditions provide a broad overview of issues which are required to be reported to the OIG. Such reports must be made before initiating your own investigation, including hiring an outside party (independent law firm) to conduct an internal investigation in lieu of notifying the OIG.

Our recent investigative work has disclosed the following fraud indicators found to be associated with larger schemes involving the theft or misuse of program funds. These are among the types of schemes that should be reported to the OIG, should you be the target.

Cyber Threat Fraud Indicators

- Any requests to change payment or money transfer information should be considered suspect;
- Hyperlinks that contain misspellings or changes to the actual domain name;
- URL spoofing, which is when a fraudulent link is masked to look like a legitimate and/or familiar source;
- Urgent or unusual requests from a person of authority at the organization;
- An email or text requesting personal or sensitive information;
- An email or text asking an employee to click on a link;
- An email or text requesting verification of direct deposit information;
- International IP addresses that are accessing your systems, especially email systems;
- To guard against the success of these schemes, your internal controls should include multiple steps to verify the legitimacy of these types of requests.

OIG Resources Related to Cyber Threat Best Practices

Webpage - LSC-OIG Cyber Security Resources

Subgrant Fraud and Program Integrity Fraud Indicators

- Reporting Private Attorney Involvement cases as volunteer attorney cases when legal advice was provided by non-attorney staff;
- Charging LSC eligible clients for legal assistance and using cash received from clients for personal gain;
- Lack of documentation and business purpose for purchases made by staff using program checks and credit cards;
- Contracting and hiring relatives for jobs for which no work is performed;
- When the Executive Director (ED) or staff obligate grantee funds for program expenditures and has a personal, fiscal, or business relationship with the entity receiving the funds.

OIG Resource Related to Subgrant Oversight Best Practices
Subgrant Capstone Report (October 1, 2015)

Outside Practice of Law and Outside Employment Fraud Indicators

- Referral of clients during the intake process to an employee's outside business for notary, document preparation, or adoption services;
- Not requiring staff to report outside employment that may conflict with their duties at the grantee;
- Unreported outside practice of law by a full-time staff attorney during program time;
- Lack of grantee oversight of newly hired program attorney's winding down of their prior law practice.

OIG Resources Related to Outside Practice of Law and Outside Employment Best Practices
Fraud Alert – Unauthorized Outside Practice of Law (July 31, 2018)
Fraud Alert – Outside Employment (August 9, 2017)

Abuse of Power and Conflicts of Interest Fraud Indicators

- Booking hotel stays for staff travel on the ED's or other staff member's personal hotel rewards account, which would allow the use of the points earned for personal travel;

- Creating a pattern/culture of nepotism in grantee hiring practices including hiring a significant number of relatives, especially relatives of management employees;
- Eluding board oversight of questionable expenses and purchases by excluding items for Board review when grantee policy requires Board approval;
- Hiring and contracting with relatives without prior disclosure of the conflict to the Board of Directors;
- Failing to disclose a conflict of interest during the contract process when a staff member possesses a personal, fiscal, or business relationship with a potential contractor. If a conflict does exist, the employee should recuse themselves from the contract process.

OIG Resources Related to Abuse of Power and Conflicts of Interest Best Practices
Fraud Corner – The Impact of Nepotism (December 19, 2019)
Fraud Alert – Conflict of Interest Policy (April 22, 2015)

Travel Fraud Indicators

- Providing the ED with a monthly travel stipend in addition to travel reimbursements (double dipping);
- Insufficient oversight of staff travel including providing hotel, per diem, and meal reimbursements for overnight stays located within the employee's city of residence/office;
- Reimbursing staff for travel despite a pattern of missing receipts and the inability to substantiate expenses listed on the travel reimbursement form.

OIG Resources Related to Travel Fraud Best Practices
Fraud Alert – Local Travel (March 7, 2019)
Fraud Corner – Travel Reimbursement Fraud (July 16, 2018)

Time and Attendance Fraud Indicators

- Employees who work their outside business during program time and without taking leave;
- Submission of inaccurate timesheets including double time entries by grantee employees;
- Falsifying time activities in the grantee case management system;
- Allowing staff to make timesheet entries well after payroll has been processed;
- Lack of separation of duties within payroll processing; for instance, the verification of staff time should not solely be a payroll function and should be done by the employee's manager and/or an employee not part of the payroll process.

OIG Resources Related to Time and Attendance Fraud Best Practices

Fraud Alert – Payroll Fraud and Timekeeping (September 1, 2020)
Fraud Alert – Fraudulent Travel and Timekeeping Submissions (September 30, 2011)

Credit Card Abuse and Fraud Indicators

- Categorizing the cost of staff meals at local restaurants as staff development, manager meetings, or staff celebrations and allocating the cost of the lunches to LSC funds;
- Using LSC funds for staff meal/food purchases that had no legitimate business purpose;
- Providing managers with a monthly credit card allowance for staff celebrations that were funded by LSC;
- Lack of Board oversight of ED activity including their credit card expenses;
- Withholding questionable or unallowable credit card purchases, such as alcohol purchases, from Board oversight.

Resource Related to Credit Card Fraud Best Practices
General Services Administration (GSA) Resource Related to Credit Card Misuse/Abuse and Fraud

External Fraud Scheme Indicators such as Checking Account Fraud, Burglaries, Retainer Fee Fraud, ACH Transaction Fraud

- Monthly bank reconciliations or notifications from your bank that identify forged, altered, or counterfeit checks (positive pay is a tool to prevent fraudulent bank activity);
- Burglaries at grantee offices (on the rise due to increased telework);
- Reports by clients that they are being solicited by people impersonating the grantee for payments such as retainer fees;
- Improper payments made against grantee accounts through ACH payments.

OIG Resources Related to External Fraud Scheme Best Practices

Fraud Corner – Preventing Checking Account Fraud through Bank Reconciliations and Positive Pay (March 25, 2019)
Fraud Corner – Retainer Fee Fraud Scheme (June 14, 2021)
Fraud Corner – ACH Transactions during COVID-19 (July 20, 2020)
Webpage – COVID-19 Fraud Prevention

I hope you find this Fraud Alert useful. If you have any questions concerning this Fraud Alert, please contact Daniel O'Rourke, Assistant Inspector General for Investigations, LSC OIG, at 202-295-1651; email dorourke@oig.lsc.gov.

To report concerns of fraud, waste, or abuse please contact the LSC-OIG Hotline. The OIG's Fraud Hotline telephone number is 800-678-8868 or 202-295-1670; our email address is hotline@oig.lsc.gov; and our fax number is 202-337-7155.

For more information on other fraud topics please refer to our Fraud Alerts and Best Practices and Fraud Corner webpages.