


PREVENTION OF
FRAUD, WASTE AND
ABUSE

TRAINING FOR
GRANTEE STAFF
V 8.3.21

Illinois Department of
Commerce and
Economic Opportunity
Office of Community
Assistance

Integrity – the quality of being honest and having strong moral principles.



Nothing is easier than spending the public money. It does not appear to belong to anybody. The temptation is overwhelming to bestow it on somebody.

(Calvin Coolidge)

IZQuotes

FRAUD *Waste Abuse*



In this training we will:

- ❖ Define Fraud, Waste and Abuse, Ethics Violations
- ❖ Review how to Recognize Fraud, Waste and Abuse
- ❖ Address real CSBG, LIHEAP and IHWAP scenarios
- ❖ Examples of ways to prevent Fraud, Waste and Abuse

The Fraud Triangle

Rationalization

Justification of dishonest actions.

Stupid people deserve to be cheated. They had it coming. If we did not do it someone else would have. They need our leadership.

Opaque and unnecessarily complicated systems involving rigged transactions, naive and trusting public, and weak regulators. Privileged connections, positions of trust, access to people's money.

Opportunity

Ability to carry out misappropriation of cash or organizational assets.

FRAUD

Insatiable greed and lust for power with little balance from moral principles and human empathy.

Pressure

Motivation or incentive to commit fraud.

Fraud

305 ILCS 5/12-4.25(G-5)(5)(A)

“Fraud” means an intentional deception or misrepresentation made by a person with the knowledge that **the deception could result in some unauthorized benefit to himself or herself or some other person**. It includes any act that constitutes fraud under applicable federal or State law.

- Using funds, equipment or services for personal gain
- Actions that benefit a customer but are not in agreement with program rules



Improper practices that result in use of funding or resources that don't rise to the level of a criminal act.

- Buying an expensive vehicle for a program instead of purchasing a cheaper model.
- Buying materials that are never used for the program.



Abuse

Abuse means practices that are inconsistent with sound fiscal, business, or organization practices and that result in an unnecessary cost to the program.

- Wasting time while on the job.
- Falsifying time records saying you are working but not actually working at home or in the office.

Ethics Violations

Ethics pertain to “right” and “wrong”.

- Human resources - nepotism (hiring relatives that directly report)
- Integrity of accounting (“cooking the books”)
- Procurement (bid rigging, preferred treatment of certain vendors)
- Program violations (preferred customers, falsified refunds, etc.)
- Theft/misappropriation of resources
- Renting from or working part time for an agency contractor
- Contractor can’t perform tests on measures (doors, windows, stoves, water heaters) to be replaced that the Agency staff should be doing themselves for the waiver process



COMMUNITY ACTION AGENCIES AND COUNTY OFFICES

Possible agency vulnerabilities

Financial

- Lack of internal controls in accounting
- Only one staff person in fiscal
- Poorly trained fiscal staff
- Large grants from multiple funding sources
- Deficient IT systems
- Staff falsification of time records, documentation
- Staff using the Agency credit card for unauthorized expenditures

Possible agency vulnerabilities

Agency Culture

- The staff are trusting of people
- Remote working with no supervision
- Not protecting Personal Identifiable Information (PII) in email, hard copy files or while working remotely
- Each department is independent
- Small staff size, part-time staff
- Unethical behavior and decision making by managers, coordinators, or intake staff

Possible agency vulnerabilities

Teleworking - WiFi

Working from home raises new security challenges. Protect your devices and personal information from hackers, scammers and identity thieves.

Do not use public unsecured WiFi.

Lock down your WiFi:

- Change default name of your home WiFi
- Make your wireless network password long, strong and unique that are at least 12 characters with a mix of numbers, symbols, and capital and lowercase letters.
- Turn off network name broadcasting
- Keep your router's software up to date
- Make sure you have a good firewall

Possible agency vulnerabilities

Teleworking – Technical Security

Technical Security Assurances

[Agencies have been subject to ransomware attacks.](#) These suggestions are good for the office too. To prevent unauthorized access, acquisition, use, modification, disclosure or destruction to confidential information:

- Use **secure access** established by your agency to connect to the network
- Enable **network encryption** to scramble information received and transmitted over the network
- Keep laptop and devices **password-protected**, locked and secure.
- Ensure **security software** is up to date, and laptop and devices have anti-virus and latest updates.
- Implement **multi-factor authentication** where possible.
- **Do not open or download suspicious attachments** via email; attachments can bring malware, viruses, spyware or other unwanted software onto your device.
- Separate sensitive customer data from non-sensitive data to **protect confidential information.**
- **Use passwords for video conferences** with Zoom, WebEx, etc. to reduce chances for hacking.

Possible agency vulnerabilities

Teleworking – Physical Security

Physical Security Assurances

- **Your home has become an extension of your office.** Securely store confidential information and sensitive customer files. When there's a legitimate business need to physically transfer documents with personal information, keep it out of sight and under lock and key. If you don't have a file cabinet at home, use a locked room.
- Dispose of sensitive data securely. Instead of throwing it in the trash or recycling bin, shred it. Paperwork you no longer need can be treasure to identity thieves if it includes personal information about customers or employees.
- Never leave laptop and devices unattended. This includes your family having access or ability to view sensitive data.
- Follow your employer's security practices. Keep up to date on policies and procedures and make sure you're aware of any updated security protocols implemented.



RECOGNIZING FRAUD, WASTE AND ABUSE

Common Fraud Schemes

Bid Rigging and Procurement Fraud

- Improper use of minority companies
- Different rules for different vendors
- Material substitution
- Change order game
- Giving potential bidders information on current vendor
- Using the same company for 20 years without bidding the contract

Common Fraud Schemes

Fiscal

- Payroll: ghost employees, falsified time records, failure to terminate
- Expense reimbursement
- Check tampering
- Taking money from one account to pay the shortages in another
- Refund manipulation
- Allowing one program to use equipment without reimbursement to the program which purchased the equipment

Bank reconciliations can miss the fraud.

Fiscal Scenario

An Agency submits a cash draw from the LIHEAP program. Supporting documents submitted with the requests indicate that the cash will be used to pay utility vendors. The cash request was processed. Three weeks later OCA receives notification that the Agency is late in paying LIHEAP utility vendors. OCA contacts the Agency. The Agency states that they were short of funds elsewhere and used these funds to pay for expenses in another program.

Answer: The Agency has committed fraud. The funds drawn were utilized for something other than the purpose presented to OCA. Under no circumstances should grant funds be expended for any other program and/or purpose than those specifically related to the grant program.

CSBG Scenario

A renter is temporarily dislocated from their apartment due to a bug problem in the unit. The landlord needs to fumigate, and the renter must move out. The CSBG program pays for five days at a hotel. The renter contacts the case worker on the fifth day and says the apartment isn't ready. The renter is given another five days in the hotel. Which may go on for a month.

Answer: The Coordinator must ask the Grant Manager for approval for the additional hotel expense. The Coordinator should be contacting the landlord to make sure the work is done in time. At this point enough funds have been paid in hotel costs that would have paid a month's rent at another apartment. While there is no fraud, unless the renter is lying to try to stay at the hotel longer, the Coordinator should make sure the funds are not wasted.

LIHEAP Scenario 1

A woman applies for PIPP. A monitoring reveals the applicant was the wife of the PIPP Coordinator and the application did not include the Coordinator in the household, so his income was not included.

Answer: The Coordinator committed fraud by not including the wife's income. He then processed the application and received the benefits. This employee would be terminated by the agency. A refund would be due and/or final wages would be garnished.

LIHEAP Scenario 2

A customer applies for LIHEAP. The household size is two people, and she is claiming zero income. The intake worker knows her and has seen on Facebook that she has a boyfriend living with her and a son. Both she and the boyfriend work.

Answer: The intake worker has the right to ask for additional information, including bank statements and pay stubs. Anything on Facebook is public. While we don't mandate that agencies research every applicant, if other information is known it is permissible to ask for more information from the customer. However, it may be difficult to prove that a boyfriend is living at a residence versus staying on a temporary basis. If you cannot prove otherwise, drop it.

IHWAP Scenario 1

An Agency staff member manipulates the database/energy audit data entry in order to achieve favorable Savings to Investment Ratios. This would result in the manipulation of outcomes on the Scope of Work and **measures would be installed that would not normally qualify for replacement.** Is there anything wrong with this practice?

Answer: This is fraud. The Agency staff member is committing fraud by manipulating the data. This is waste because measures that don't need to be replaced will be costing additional federal funds to be dispensed. The Agency staff member may not personally benefit from the fraud unless they receive some form of kickback. Using up the funding on fewer projects is obvious waste.

IHWAP Scenario 2

An Agency staff member conspires with a contractor (friend) to over charge the project. A contractor misrepresents quantities of units installed (charging for materials not installed). The final inspector willingly works with the contractor to over charge for work completed or when not performed. Is this an acceptable practice?

Answer: This is fraud and waste. It is the final inspector's job to verify the assessor's data entry. The contractor is billing for Services Not Rendered – Installing less quantities of measures on a home but charging full price (installing 6” of insulation when 12” was billed). The contractor and the field staff are friends, and the field staff is helping their friend skim the system or is also getting a kickback for the extra material costs.

IHWAP Scenario 3

The work order says to install an ASHRAE fan, but the contractor installs a regular exhaust fan. The difference in labor and materials is \$300. The contractor bills for 16 SEER A/C unit but installs a 14 SEER A/C unit, a \$500 difference.

The contractor bills for 140 linear feet of box sill and only installs 40 linear feet of material and labor. At \$5/linear feet, this is an overbilling of \$500.

The work order says to replace a pane of glass that costs \$80, but the contractor installs a new window and bills it as a pane of glass replacement for \$400.

Answer: This is fraud. They are over billing the grant for materials that were not installed. Replacing what was installed with a lower price item and keeping the difference. **The final inspector should flag this as a disallowed cost.** The final inspector is in collusion if they do not flag this.

Customer Issues

Ways a customer could commit fraud:

- Not reporting benefits or cash income
- Self-employed customer using receipts from the business to deduct expenses that are not business related
- Falsifying a “zero income” affidavit, but has income
- Including SSNs of children that do not live with them
- Applying for a furnace for a rental property
- Customer in process of selling home while acquiring IHWAP services
- Landlord misrepresenting tenant population in multi-family building



A customer found to have committed any of these actions may be denied benefits, be required to refund or repay benefits already received in the current or prior year when the action took place and be subject to denial of further benefits in future years.

Staff Issues

Ways a staff person could commit fraud:

- Intake staff tells a customer they will get them LIHEAP if they pay them \$60.
- Intake staff enters their own application for LIHEAP (and/or PIPP) benefits and falsifies income.
- Furnace Assistance: Agency field staff conspire with contractors (overcharging for work). A contractor may misrepresent quantities of units installed over charging for materials or work not performed.
- Field staff misrepresent age of equipment to obtain replacement instead of repair.

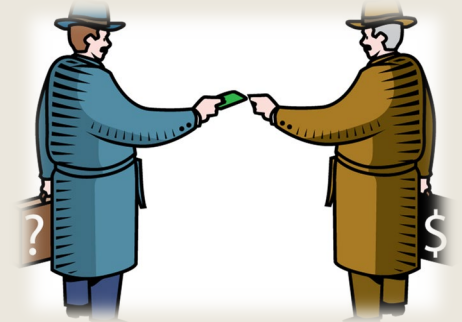


Staff who commit fraud are subject to their agency policies and procedures which may include termination. The Office of Community Assistance will not authorize payments from LIHEAP, CSBG and Weatherization funds to pay those staff who commit fraud.

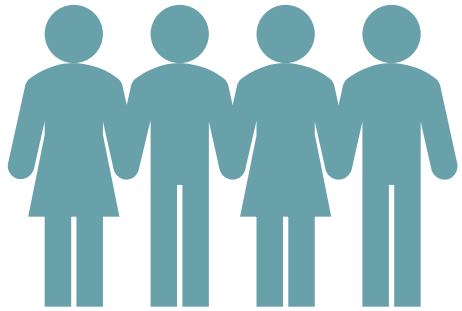
Ethics Issues

Ethics violations from an agency perspective:

- Leapfrogging customers – moving customers up on the priority list for an appointment. These benefitting customers may or may not be relatives, friends or acquaintances.
- For Furnace Assistance/IHWAP:
 - Embezzlement and Bid Rigging
 - Offering services to other employees/contractors/inspectors/monitors.
 - Kickbacks – Offering to provide benefits to a contractor, inspector or monitor.
- Allowing IHWAP purchased equipment:
 - To be used for other programs without cost allocation;
 - To be used for either personal use or financial gain;
 - To be used by contractors for little or no cost.



Offering to give someone a furnace or other services who is not income eligible is FRAUD.



Prevention and Protection

Fraud Prevention

The tone should be set at the top:

- **Fraud or embezzlement will not be tolerated.**
- There is no reasonable expectation of privacy in the course of normal business; computers, phones, etc. are all subject to search and monitoring at will.
- All employees will take regular vacations and will be cross-trained on duties.
- Separation of duties in all operational areas.
- Internal audits will be frequent and by surprise.
- All vendors will be subject to audit on demand.



Whistleblower Protection

Are you aware of fraud occurring at your Agency?

Reporting an issue under your Agency's **Whistleblower Policy** should be confidential. See your employee handbook for the specific policy.

Under the **Whistleblower Act, 740 ILCS 174/20.2**, and **Article 15 of the Ethics Act**, it is generally unlawful for **any employer**, to retaliate or threaten **retaliation** for an employee's disclosure of information to a government or law enforcement agency if the employee has reasonable cause to believe that the information discloses a violation of a state or federal law, rule, or regulation.

Retaliatory action means the reprimand, discharge, suspension, denial of promotion, demotion, transfer, or change in the terms or conditions of the employee's employment, taken in retaliation for an employee's involvement in a protected activity.

Office of the Executive Inspector General (OEIG)

- The **Office of the Executive Inspector General (OEIG)** is an independent state agency. Its primary function is to investigate fraud, waste, abuse, and violations of the Ethics Act. The OEIG investigates allegations of misconduct by employees under its jurisdiction and has the responsibility for investigating alleged violations by those doing business with entities under its jurisdiction.
- The identity of a complainant must be kept confidential by the OEIG unless the individual consents to disclosure of her or his identity, or disclosure of her or his identity is otherwise required by law.
- To report a non-emergency violation you should contact the OEIG via its toll-free hotline at (866) 814-1113. Reports of alleged violations may also be submitted via the internet at www2.inspectorgeneral.illinois.gov or by mail:

OEIG
69 West Washington, Suite 3400
Chicago, IL 60602

607 East Adams, 14th Floor
Springfield, IL 62701