

UHS Compliance: Understanding Fraud

A Brief for University of Houston System Employees

The following brief is made available for all University of Houston System employees to assist in understanding and preventing fraudulent activities at the University. The **University** has an obligation to secure the assets and reputation of the University through education, training and review of policies and procedures. **Employees** have an obligation to preserve the University's assets and reputation by frequent review and compliance with education, training, policies and procedures provided to protect both the University and the employee. Review the following brief on Understanding Fraud.

What is Fraud? Fraud occurs in the workplace when an employee uses their job or resources for personal benefit.

What are the Key Elements of Fraud in the Workplace? The key elements of fraud in the workplace are; the act is committed in secret, the act violates employer trust, the act benefits the employee financially (directly or indirectly), and the act costs the employer assets, revenue, or reserves.

What types of Fraud are most evident at a University? The types of fraud fall into three main categories: Asset Misappropriation, Corruption, and Falsifying Financial Statements.

Asset Misappropriation is theft or misuse of UH System assets. The following are some examples:

Cash Receipts — money stolen before (skimming) or after (cash larceny) it is recorded on the books.

Cash Disbursements — there are seven primary types of University cash disbursements that are fraudulent: payment to vendors or employees based on a fraudulent bill; fraudulent purchases made by an employee on a P-card or voucher; reimbursement of non-existent or over exaggerated expenses to an employee; fraudulent payment to an employee through check tampering; payment to an employee by fraudulent timesheet recording; fraudulent wire transfers; and false entries or non-entries on a cash register to hide removal of cash.

Non-Cash Assets — misappropriation of non-cash assets includes theft or abuse of inventory, equipment, supplies, information and securities. The most common is theft of office supplies and misuse of computers.

Confidential or Proprietary Information — this type of asset misappropriation falls into three categories: the use of confidential information to commit identity theft; the sharing of proprietary research information with another university or company; the misuse of stocks, bonds or other securities.

Corruption — occurs when a person uses their position or influence to gain favors or financial assets. Examples are:

Conflict of Interest — employee has an undisclosed conflict between his personal interests and the University. For instance, if an employee orders materials from his personal/family business or awarded a niece a scholarship.

Bribery — someone tries to influence an employee's future decisions or actions by offering them money or gifts. For example an employee processes an inflated invoice for a kickback from the vendor or provides confidential information about a competitor's bid on a contract.

Illegal Gratuities — someone gives an employee an inappropriate gift/reward for doing their job. For example an employee accepts cash or an expensive gift in appreciation for the University's business. For more information see **SAM 02.A.29**, Ethical Conduct of Employees.

Extortion — occurs when an employee uses threats to force someone to enter into a transaction. For example, if an employee refuses to place orders with a vendor unless the vendor hires on the employee's family member.

Falsifying Financial Statements — occurs when an employee purposefully alters financial statements by: concealing liabilities; creating fictitious revenues; improper asset valuations in order to mislead; improper disclosures by leaving out important information; or timing differences so that revenue and corresponding expenses are recorded in different accounting period.

Why does Fraud occur? Three things must be present to commit fraud – motive, opportunity and justification. These three elements make up the *Fraud Triangle*.

What are Direct and Indirect Costs of Fraud?

- Loss of money, supplies or equipment
- Bad publicity, loss of trust, injury to reputation
- Loss of grants, gifts or donations
- Decrease in enrollment and tuition

How Can the University and their Employee’s Reduce Asset Misappropriation?

- Create a control-conscious environment including written policies and procedures, plus training
- Restrict access to sensitive materials and further restrict authority to approve transactions
- Segregate duties so that more than one person is involved in completing transactions from start to finish
- Protect assets by locking rooms/filing cabinets, securing computers and protecting user ID and passwords
- Investigate any discrepancies on cost centers immediately to limit exposure
- Review accuracy and appropriateness of procurement or travel card transactions
- Perform a physical inventory of its controlled and capital assets once a year
- Petty cash or change funds should be monitored with unannounced and random frequency
- Follow up on any complaints or allegations of improper conduct and document investigation findings
- Verify that terminated employees are removed from payroll and any access or authority is removed
- Implement a fraud awareness and prevention program

How Can the University and their Employee’s Reduce Corruption?

- Require faculty and staff to disclose any outside employment or consulting activities annually
- Require competitive bidding unless there is a justifiable reason
- Review sole source justifications carefully
- Document and verify scholarships are awarded fairly and appropriately

What are the Red Flags of Fraud?

- Employee refuses to take vacation (may be due to the need to cover up fraudulent activity)
- Unexplained variances
- Lack of reconciliation to University records or failure to investigate reconciling items
- Missing documents, duplicate payments
- Lack of segregation of duties
- Sole source justifications to use same vendor over and over

How can University Employee’s Report Fraud? (Utilize any of the following methods)

- Report to your supervisor, who should report to one of the options below
- Report to the Director of Internal Audit 713-743-8000
- Report to the Fraud Hotline at **www.mysafecampus.com**
- Notify the State Auditor’s Office <http://fraud.state.tx.us/> or SAO Hotline 1-800-892-8348

For more information on Fraud see:

- **SAM 01.C.04** the UH System policy on Reporting and Investigation Fraudulent Acts
- **SAM 02.A.29** the UH System policy on Ethical Conduct of Employees
- UHS Mandatory Training Power Point
- **UHV Policy C-8** the UHV policy on Employee Standards of Conduct