



Fraud Awareness and Reporting

Policy Statement

This policy establishes the overall roles and responsibilities of University employees for reporting and investigating potential fraud at the University. All Harvard University (Harvard) employees have a responsibility to ensure that Harvard's resources are used for valid and appropriate business needs. Administrators and all levels of management have added responsibility for establishing and maintaining proper internal controls to protect Harvard's resources from misuse. Administrators and managers should be familiar with the risks and exposures in their areas of responsibility and be alert to any indications of improper activities, misappropriation, or dishonest activity.

Reason for Policy

This policy has been developed to:

- Raise awareness of fraud within the University.
- Define roles and responsibilities for detecting and preventing fraud.
- Reinforce personal responsibility and accountability.
- Detail the procedures for reporting and investigating suspected fraud.
- Better understand the limitations in existing control procedures that allow fraud to occur.

Who Must Comply

All units of the University and all members of the University community, including:

- Faculty, including senior, junior and visiting faculty
- Other salaried and non-salaried academic appointees, including post-doctoral fellows, research fellows, and teaching assistants
- Staff, including salaried exempt workers and hourly non-exempt workers
- Students
- Contractors, including independent contractors, external consultants, workers hired through an outside employment agency, and workers employed on campus through service vendors
- Official visitors
- Volunteers

Procedures

1. **Be aware of potential fraud.** All employees, particularly administrators and managers, should be familiar with the risks and exposures in their areas of responsibility and be alert to any indications of improper activities, misappropriation, or dishonest activity.
2. **Do not accuse or investigate independently.** An employee who suspects fraudulent activity **should not** accuse any individual directly, investigate the matter personally, or discuss the matter with anyone other than his or her supervisor, local tub finance officer, local or central human resources officer, or Anonymous Reporting Hotline staff member.



3. Report the concern via the proper channels.

- A. An employee who suspects fraudulent activity is encouraged to report the concern promptly to his or her supervisor, local tub finance officer, or local or central human resources officer.
- B. Alternately, any member of the Harvard community who is uncomfortable reporting suspected fraudulent activity to a supervisor or other local tub officer can report the concern via the Anonymous Reporting Hotline. The Anonymous Reporting Hotline is an independent and confidential reporting program that registers concerns through a toll-free, 24-hour-a-day phone line or through a confidential website.
- C. Supervisors and HR officers who receive a fraud-related concern from an employee must promptly report the concern to an officer in the relevant financial dean's office, unless the concern involves an employee or employees within the financial dean's office itself. If an employee or employees of a financial dean's office are suspected of fraud, then the supervisor or human resources (HR) officer who has received the concern must report it directly to Risk Management and Auditing Services (RMAS) or report it to the Anonymous Reporting Hotline (**877-694-2275**).

4. Investigate a reported concern appropriately.

- A. Financial deans' offices have responsibility for managing the investigation of suspected fraud and should engage other university units as necessary and in keeping with this policy.
 - a. When determining how to proceed after receiving a report of suspected fraud, the financial dean's office must first review all available related supporting information. If the financial dean's office determines that the allegation of fraud is credible, that office shall notify the Office of the General Counsel (OGC) and RMAS.
 - b. The financial dean's office, in consultation with OGC and RMAS, shall determine the nature of any investigation, including the involvement of other university units such as HUPD, HR, and the Office for Sponsored Programs (and, as applicable, its corollary offices at Harvard Medical School and Harvard T.H. Chan School of Public Health), or an independent fact finder, if appropriate.
- B. RMAS must conduct fraud investigations involving an employee or employees of a financial dean's office.

5. Document investigation, findings and corrective actions.

- A. Financial deans' offices must document in writing all steps taken during an investigation, seeking guidance from other University units (like RMAS, HR, and OGC) as appropriate. Financial deans' offices must retain documents relating to the investigation for ten years after the investigation has been closed.
- B. When an investigation finds that fraud has occurred, the financial dean's office must send RMAS a written summary report that provides details of the nature and scale of the fraud, the breakdown in control that allowed the fraud to occur, and the steps to be taken to avoid recurrence.

6. Incorporate any needed additional/revised control procedures.

After receiving a report of detected fraud from a tub financial dean's office, RMAS must consider the extent of control breakdown leading to the fraud. RMAS will advise relevant University offices on additional or revised control procedures as necessary.

7. Maintain confidentiality.

All parties involved in the reporting and/or investigation of fraud must treat all information as confidential. Concerns and/or investigation results will not be disclosed or discussed with anyone other than those with a legitimate need to know. For information on protecting confidential information, see the University's Enterprise Information Security Policy.



Responsibilities and Contacts

Financial deans or equivalent tub financial officers are responsible for ensuring that local units are informed of this policy and the accompanying procedures. Financial deans' offices play a central role in advising local units on control measures and in determining how detected or suspected fraud should be investigated. Tub financial deans' offices work with Risk Management and Audit Services (RMAS), tub Human Resources offices, the Office of the General Counsel (OGC), and the Harvard University Police Department (HUPD) and other offices, as necessary, during the consideration and investigation of fraud. Financial deans' offices must report in writing all incidents of detected fraud to RMAS, providing details of the nature and scale of the fraud, the breakdown in control that allowed the fraud to occur, and the steps to be taken to avoid recurrence.

Tub Human Resources Offices (HR) provide advice and assistance on the proposed conduct of fraud-related investigations in order to ensure that employee rights are protected. HR offices are also available to provide assistance in determining employee disciplinary action in the event of detected fraud.

Contact: <http://hr.harvard.edu/local-human-resources-offices>

Risk Management and Audit Services (RMAS) provides central advice to tubs and local offices on control measures and advises on the investigation of detected or suspected fraud. RMAS may participate in the investigation of fraud at the request of tubs. RMAS considers the extent of control breakdown leading to respective frauds and advises the University community on additional or revised control procedures, as appropriate. **Contact:** <http://vpf-web.harvard.edu/rmas/>

Harvard University Police Department (HUPD) provides advice and assistance to the University community on the investigation of fraud, including the potential prosecution of offenders. HUPD may undertake fraud investigations at the request of tub financial deans' offices and/or human resources offices.

Contact: <http://www.hupd.harvard.edu/>

Office of the General Counsel (OGC) provides advice and direction on the legal aspects of fraud-related investigations and potential prosecutions. **Contact:** <http://www.ogc.harvard.edu/>

Office of the Controller (OC) is responsible for maintaining this policy and providing advice and assistance to tubs on the operation of the policy and on specific concerns, as necessary. **Contact:** (617) 384-7487

Harvard employees should report any suspected misuse of Harvard resources (aka fraud) to his or her supervisor, to a local tub finance officer, to a local or central human resources officer, or to the Anonymous Reporting Hotline. Employees are expected to cooperate fully with any and all fraud-related investigations.

Harvard administrators and managers must establish and maintain proper internal controls to protect Harvard's resources from misuse. Administrators and managers must be reasonably familiar with the risks and exposures in their area(s) of responsibility and alert to any indications of the misuse of Harvard resources (aka fraud). They must report any case of suspected fraudulent activity in their area(s) to their tub financial dean's office.



Definitions

Fraud:

1. “Any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain Source: “Managing the Business Risk of Fraud: A practical Guide”, sponsored by The Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners, April 2008.

2. “Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.” Source: Internal Auditing and Fraud, IPPF - Practice Guide, The Institute of Internal Auditors, December 2009.

Related Resources

Anonymous Reporting Hotline: <https://www.integrity-helpline.com/HarvardUniversity.jsp> or (877-694-2275)

Whistleblowing Policy: <http://hr.harvard.edu/staff-personnel-manual/general-employment-policies>

Responsibilities of Purchasers, Preparers and Approvers: <http://policies.fad.harvard.edu/responsibilities-purchasers-preparers-and-approvers>

Information Security and Privacy, Enterprise Information Security

Policy: <http://www.security.harvard.edu/enterprise-security-policy>

Revision History

1/10/2017: minor edits, updated name of reporting hotline

6/30/2013: updated format

Appendix

Categories of Occupational Fraud: includes descriptions and examples

APPENDIX: Categories of Occupational Fraud¹

1. *Asset misappropriations* are those schemes in which the perpetrator steals or misuses an organization's resources. These frauds include schemes such as skimming cash receipts, falsifying expense reports and forging company checks.
2. *Corruption* schemes involve the employee's use of his or her influence in business transactions in a way that violates his or her duty to the employer for the purpose of obtaining a benefit for him- or herself or someone else. Examples of corruption schemes include bribery, extortion and a conflict of interest.
3. *Financial statement fraud* schemes are those involving the intentional misstatement or omission of material information in the organization's financial reports. Common methods of fraudulent financial statement manipulation include recording fictitious revenues, concealing liabilities or expenses and artificially inflating reported assets.

Asset Misappropriation Sub-Categories		
Category	Description	Examples
Schemes Involving Theft of Cash Receipts		
Skimming	Any scheme in which cash is stolen from an organization <i>before</i> it is recorded on the organization's books and records	<ul style="list-style-type: none"> • Employee accepts payment from a customer, but does not record the sale, and instead pockets the money
Cash Larceny	Any scheme in which cash is stolen from an organization <i>after</i> it is recorded on the organization's books and records	<ul style="list-style-type: none"> • Employee steals cash and checks from daily receipts before they can be deposited in the bank
Schemes Involving Fraudulent Disbursements of Cash		
Billing	Any scheme in which a person causes his employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices or invoices for personal purchases	<ul style="list-style-type: none"> • Employee creates a shell company and bills employer for services not actually rendered • Employee purchases personal items and submits invoice to employer for payment
Expense Reimbursements	Any scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses	<ul style="list-style-type: none"> • Employee files fraudulent expense report, claiming personal travel, nonexistent meals, etc.
Check Tampering	Any scheme in which a person steals his employer's funds by intercepting, forging or altering a check drawn on one of the organization's bank accounts	<ul style="list-style-type: none"> • Employee steals bank company checks, makes them out to himself or an accomplice • Employee steals outgoing check to a vendor, deposits it into his own bank account
Payroll	Any scheme in which an employee causes his employer to issue a payment by making false claims for compensation	<ul style="list-style-type: none"> • Employee claims overtime for hours not worked • Employee adds ghost employees to the payroll
Cash Register Disbursements	Any scheme in which an employee makes false entries on a cash register to conceal the fraudulent removal of cash	<ul style="list-style-type: none"> • Employee fraudulently voids a sale on his cash register and steals the cash
Other Asset Misappropriation Schemes		
Cash on Hand Misappropriations	Any scheme in which the perpetrator misappropriates cash kept on hand at the victim organization's premises	<ul style="list-style-type: none"> • Employee steals cash from a company vault
Non-Cash Misappropriations	Any scheme in which an employee steals or misuses non-cash assets of the victim organization	<ul style="list-style-type: none"> • Employee steals inventory from a warehouse or storeroom • Employee steals or misuses confidential customer financial information

¹ Source: Report to the Nations on Occupational Fraud and Abuse, 2010 Global Fraud Study, Association of Certified Fraud Examiners, Inc.