

## Policy 1603 Identity Theft Red Flags Policy

Responsible Office	Office of the General Counsel	Effective Date	5/1/09
Responsible Official		Last Revision	

**Policy Sections** .....

1603.1 Responsibilities of Policy Administrators .....

1603.2 Responsibilities of Departments .....

1603.3 Annual Reports .....

### Reason for Policy

This Policy is designed to comply with the Federal Trade Commission's Red Flags Rule implementing sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003.

### Scope

This policy applies to all units of the University that perform Credit Activities, engage a vendor to perform Credit Activities, or use Consumer Reports.

### Definitions

**Consumer Report** means any communication of information by a Consumer Reporting Agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, reputation, personal characteristics, or mode of living, which is used as a factor in establishing the consumer's eligibility for (i) credit to be used primarily for personal, family, or household purposes, or (ii) employment purposes.

**Consumer Reporting Agency** means a person or entity that, for monetary fees or on a cooperative nonprofit basis, regularly collects, evaluates, and disseminates credit information about consumers to be used for credit evaluation and related purposes.

**Credit Activities** means activities by which the University extends credit to, offers to extend credit to, or defers payment for goods or services by an individual, and offers or maintains a credit account (a "Credit Account") for that individual that involves or is designed to permit multiple payments or transactions.

**Department** means a unit of the University that performs Credit Activities, engages a vendor to perform Credit Activities, or uses Consumer Reports.

**Identifying Information** means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

**Identity Theft** means a fraud committed or attempted using the Identifying Information of another person without authority.

**Policy Administrators** means the University's Vice President & General Counsel, Vice President for Finance & Business Operations, Associate Vice President for Student Financial & Administrative Services, Director of Financial Aid, and Director of Information Technology Services, or their respective designees.

**Red Flag** means a pattern, practice, or specific activity that indicates the possible unauthorized use of personal Identifying Information.

---

## Policy Sections

### 1603.1 Responsibilities of Policy Administrators

The Policy Administrators are responsible for implementing this Policy.

Annually, on or before June 30, the Policy Administrators shall meet to:

1. identify all Credit Activities being performed by or for the University and all Departments that perform Credit Activities, engage vendors to perform Credit Activities, or make use of Consumer Reports;
2. instruct any newly identified Department to implement the procedures required by this Policy; and
3. review the annual reports required by Section 0000.3 and, if necessary, instruct Departments to modify their existing procedures under this Policy.

The Policy Administrators shall also, on a continuing basis, advise Departments on how to respond to specific Red Flag incidents.

The power to modify this Policy is delegated in full by the Yale Corporation to the Policy Administrators.

### 1603.2 Responsibilities of Departments

Each Department is responsible for the following:

- A. Creating a Red Flags List: Each Department shall develop a written list of Red Flags appropriate to its Credit Activities. In developing this list, the Department shall consider:
  1. the example Red Flags listed in Supplement A to Appendix A to Part 681 of Title 16 of the Code of Federal Regulations;
  2. the methods it provides to open and access its Credit Accounts;
  3. its previous experiences with Identity Theft; and
  4. evolving methods of Identity Theft that reflect changes in the University's risk of experiencing Identity Theft.
- B. Detecting Red Flags: Departments shall develop written procedures to detect the Red Flags they have listed, including:
  1. methods to verify the identity of:
    - (i) persons applying for a Credit Account;

- (ii) persons requesting information about an existing Credit Account (including, as applicable, methods specific to requests made in person, by telephone, by facsimile, by e-mail, or otherwise); and
    - (iii) persons initiating Credit Account transactions;
  - 2. methods to verify the validity of change-of-address requests for Credit Accounts (including, as applicable, methods specific to requests made in person, by telephone, by facsimile, by e-mail, or otherwise); and
  - 3. methods to train Department staff, as necessary, to detect the Department's listed Red Flags.
- C. Responding to Red Flags: As soon as practicable after detecting a Red Flag, a Department shall gather all relevant documentation, write a description of the incident, present the description to a Policy Administrator, and seek the advice of the Policy Administrator in responding to the incident in a manner commensurate with the risk posed.
- D. Responding to Consumer Reporting Agency Notices of Address Discrepancies: If a Department requests a Consumer Report about an individual and, in turn, receives a notice of address discrepancy from a Consumer Reporting Agency, the Department shall take steps to verify that the Consumer Report relates to the individual at issue. These steps shall include:
- 1. comparing the information in the Consumer Report with information the Department maintains in its own records or obtains from third-party sources or directly from the individual; and
  - 2. furnishing a confirmed address for the individual to the Consumer Reporting Agency.
- E. Training: Departments shall train staff to detect and respond to Red Flags and Consumer Report address discrepancies in accordance with the procedures described above.
- F. Overseeing Vendors: Departments shall ensure that vendors engaged to perform Credit Activities follow reasonable policies and procedures to prevent Identity Theft.

### 1603.3 Annual Reports

Annually, on or before June 30, each Department shall issue a written report to the Policy Administrators, including the following information:

- 1. its list of Red Flags;
- 2. its procedures to detect Red Flags;
- 3. a description of each incident during the prior year in which a Red Flag was detected and the response taken by the Department;
- 4. a description of any incidents of Identity Theft relating to its Credit Activities during the prior year;
- 5. a description of each notice of address discrepancy the Department received during the prior year and its response; and
- 6. any recommendations for changes to this Policy.

---

**Special Situations/Exceptions**

None.

---

**Related Policies**

Policy 1602: Protecting the Security and Confidentiality of Social Security Numbers

---

**Contacts**

Subject	Contact	Phone or Email
Policy Implementation	Harold Rose, Associate General Counsel	Harold.Rose@Yale.edu

---

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.

---