# TEMPLE UNIVERSITY

# BOARD OF TRUSTEES POLICIES AND PROCEDURES MANUAL

**Title:** Identity Theft Prevention Program

Policy Number: 05.20.01

**Issuing Authority:** Board of Trustees

**Responsible Officer:** Vice President for Computer and Financial Services, and Chief

**Information Officer** 

Date Created: April 23, 2009

**Date Last Amended/Reviewed:** July 8, 2010 **Date Scheduled for Review:** April 2014

Reviewing Office: Office of the Vice President for Computer and Financial Services, and Chief

**Information Officer** 

# **Scope of Policy & Rationale**

Temple University has adopted this policy to conform its practices with respect to the prevention of identity theft comply with regulations collectively known as the Red Flag Rules (16 C.F.R. §§681.1-681.3), issued by the Federal Trade Commission (FTC) pursuant to Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act), which amended the Fair Credit Reporting Act (FCRA). This policy is applicable to certain financial activities of the university, as described below.

To promote the effectiveness of the university's Identity Theft Prevention Program (the "Program"), knowledge about specific procedures may be limited to those employees with a need to know for purposes of effective Program implementation. Any documents produced to develop or implement this Program that list or describe such specific practices and the information in those documents are considered "confidential" and should not be shared with other university employees or the public.

The Red Flags Rules (16 C.F.R. §§681.1-681.3) consist of three separate rules regarding detection, prevention and mitigation of identity theft, and require that the university establish and implement reasonable policies and procedures to:

- 1. verify the address of a consumer when the university is notified of
  - a) a discrepancy in the consumer's address by a consumer reporting agency (CRA), and
  - b) furnish the verified address to the CRA;
- 2. detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing covered account; and,

3. assess the validity of a change of address request when followed closely by a request for a replacement "debit card" issued by the university.

Temple University has implemented other guidelines and policies regarding privacy and information security. This policy does not replace or supersede any of those policies, but rather is intended to complement (and should be interpreted consistently with) such other university policies.

#### **Definitions**

Defined terms in this policy are intended to have the meaning ascribed to them by the FTC in the Red Flag Rules, as such Red Flag Rules may be amended from time to time, and shall be read consistently with the FTC's definitions. The following definitions have been modified to relate to the specific activities of the university covered by the Red Flag Rules.

- 1. "Account" means a continuing relationship established by a person with the university to obtain a product or service for personal, family, household or business purposes. Account includes:
  - (a) An extension of "credit", such as the right to make periodic payments to repay a student loan, or the purchase of property or services from the university involving a deferred payment; and
  - (b) A deposit account.

#### 2. "Covered account" means:

- (a) An account that the university offers or maintains, that involves or is designed to permit multiple payments or transactions, such as a student account or Diamond Dollars account; and
- (b) Any other account that the university offers or maintains for which there is a reasonably foreseeable risk to the account holder or to the safety and soundness of the university from identity theft, including financial, operational, compliance, reputation, or litigation risks.
- 3. "Credit" means rights granted by the university to defer payment of a debt; to incur debts and defer payment; or to purchase property or services from the university and defer payment therefor.
- 4. **"Identity theft"** means a fraud committed or attempted using the identifying information of another person without authority.
- 5. **"Red Flag"** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

6. **"Service provider"** means a person that provides a service directly to the university.

#### **Procedures**

The Program procedures shall include reasonable steps to do all of the following:

- 1. Identify the university's Covered Accounts.
- 2. Identify and establish risk factors in identifying relevant Red Flags including:
  - a. Types of Covered Accounts
  - b. Methods provided to open Covered Accounts
  - c. Methods used to access Covered Accounts
  - d. The university's previous history of identity theft
- 3. Identify specific Red Flags including:
  - a. Notification and warnings from credit reporting agencies
  - b. Suspicious documents
  - c. Suspicious identifying information
  - d. Suspicious account activity
  - e. Alerts from others
- 4. Detect Red Flags in appropriate areas including:
  - a. Student Enrollment
  - b. Existing Covered Accounts
  - c. Credit Report Requests
- 5. Take one or more of the following steps when a Red Flag is triggered:
  - a. Deny access to the Covered Account until other information is available to eliminate the Red Flag
  - b. Contact the account holder
  - c. Change any passwords, security codes or other security devices that permit access to a covered account
  - d. Notify law enforcement
  - e. Determine no response is warranted under the particular circumstances.

# **Roles and Responsibilities**

The president of the university, or other member of the senior administration as designated from time to time by the president, serves as the program administrator and is responsible for developing, implementing and updating the program. The program administrator is responsible for ensuring appropriate training of university staff on the program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the program.

University staff responsible for implementing the program will be trained in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. University staff are expected to notify the program administrator once they become aware of an incident of identity theft or of failures to comply with this program. At least annually, university staff who are charged to carry out the development, implementation, and administration of the program will report to the program administrator on compliance with this program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of covered accounts, service provider agreements, significant incidents involving identity theft and management's response, and recommendations for changes to the program.

### Service Provider Arrangements

In the event the university engages a service provider to perform an activity in connection with one or more covered accounts, the university will require that the service provider review and comply with this program including reporting any Red Flags to the Program Administrator.

#### **Notes**

## 1. Dates of official enactment and amendments:

Adopted by the Budget & Finance Committee of the Board of Trustees on April 23, 2009.

# 2. History:

The FTC is delaying enforcement of the Red Flags Rule until January 1, 2011.

Temple University has adopted this policy to conform its practices with respect to the prevention of identity theft comply with regulations collectively known as the Red Flag Rules (16 C.F.R. §§681.1-681.3), issued by the Federal Trade Commission (FTC) pursuant to Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act), which amended the Fair Credit Reporting Act (FCRA).

#### 3. Cross References

The Red Flags Rules (16 C.F.R. §§681.1-681.3)