Effective Date: **May 1, 2009**

POLICY

FINANCE AND ADMINISTRATION, INFORMATION MANAGEMENT, PRIVACY AND SECURITY

Universal Identity Theft Policy

RESPONSIBLE OFFICE

Office of the Controller

Purpose

The University adopts this Identity Theft Policy to help protect members of the University community from damages related to the loss or misuse of information contained in certain covered accounts (defined below).

This policy will:

1. Identify “red flags” (patterns, practices and activities that signal possible identity theft);
2. Describe ways to detect these red flags;
3. Describe appropriate responses to detected red flags to prevent and mitigate identity theft; and
4. Describe appropriate responses by the University when receiving address discrepancy notices from national consumer credit reporting agencies.

Background and References

In response to the growing threats of identity theft in the United States, Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended a previous law, the Fair Credit Reporting Act (FCRA). This amendment to FCRA charged the Federal Trade Commission (FTC) and several other federal agencies with promulgating rules regarding identity theft. On November 7, 2007, the FTC, in conjunction with several other federal agencies, promulgated a set of final regulations known as the “Red Flags Rule”.

Covered Parties

This Policy applies to all administrative units and personnel that have access to covered accounts (defined below), as well as to third parties with whom the University contracts to perform functions on their behalf. For example, the Red Flag Rules apply to Boston University because of our participation in the Perkins Loan program, our limited institutional loan program, our extension of credit for student accounts, and to the extent that we may request credit reports for loan programs and some potential employees.

Defined Terms

Covered accounts:

1. Any account the University offers or maintains primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions.
2. Any other account the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from Identity Theft.

For example, the Student Loan Department services the University’s loan portfolio, all of which would be covered (Perkins, HHS and Institutional Loans) by these regulations. Within the Collections Department, both student loans and student receivables accounts would be covered. In addition, all lending activity with regards to Perkins, HHS, other Federal program and/or Institutional loan programs will be covered by these regulations.

Credit: The right granted by a creditor to a debtor to defer payment of debt or to incur debt

and defer its payment or to purchase property or services and defer payment.

Creditor: An entity that regularly extends, renews, or continues credit.

Customer: Any person with a covered account with a creditor.

Identifying Information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address or routing code.

Identity Theft: A fraud committed using the identifying information of another person.

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

University Policy Statement

I. Identification of Red Flags

The following red flags are potential indicators or warning signs of potential or actual identity theft or similar fraud. Any time a red flag, or a situation resembling a red flag, is apparent, it should be investigated for verification. The examples below are meant to be illustrative. Any time an employee suspects a fraud involving personal information about an individual or individuals, the employee should assume that this Identity Theft Policy applies and follow protocols established by his/her office for investigating, reporting and mitigating identity theft.

A. Notifications and Warnings from Credit Reporting Agencies

- Report of fraud or active duty alert accompanying a credit report;
- Notice of credit freeze in response to a request for a consumer credit report; or
- Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity, such as:
    - A recent and significant increase in the volume of inquiries;

- An unusual number of recently established credit relationships;
- A material change in the use of credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. Suspicious Documents

- Identification document or card that appears to be altered or forged;
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
- Other information on the identification document is not consistent with information provided by the person opening a new covered account or customer presenting the identification; or
- Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example:
  - The address on an application is the same as the address provided on a fraudulent application; or
  - The phone number on an application is the same as the number provided on a fraudulent application.
- A person fails to provide complete personal identifying information on an application when reminded to do so; or
- A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

- Shortly following the notice of a change of address for a covered account, the University

receives a request to change the account holder's name;
- Payments stop on an otherwise consistently up-to-date account;
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account;
- The University is notified that the customer is not receiving paper account statements; or
- The University is notified of unauthorized charges or transactions in connection with a customer's covered account.

E. Alerts from Others

Notice to the University from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

II. Detecting Red Flags

A. Student Enrollment

In order to detect any of the red flags identified above associated with the enrollment of a full-time student on campus, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, academic records, home address or other appropriate identification; and
2. Verify the student's identity at time of issuance of student identification card by review of driver's license or other government-issued photo identification.

For students enrolled in distance education or other programs that do not take place at the University's campus and for part-time students, the University will take reasonable steps to verify the identity of those students.

B. Existing Accounts

In order to detect any of the red flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information (in person, via telephone,

via facsimile, via email);
2. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

III. Responding to Red Flags

Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the University from the effects of identity theft. The employee should inform his/her supervisor as soon as possible that he/she has detected an actual or potential red flag, or had identified a similar area of concern of identity theft. The supervisor should notify the Office of the Controller and conduct any necessary inquiry to determine the validity of the red flag and shall take all appropriate steps to respond and mitigate identity theft depending on the nature and degree of risk posed by the red flag, including but not limited to the following examples:

- Continue to monitor an account for evidence of identity theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account;
- Reopen an account with a new number;
- Notify law enforcement and the Office of the Controller; or
- Determine that no response is warranted under the particular circumstances.

In all situations where it is determined that a red flag has been positively identified, the office responsible for the account shall document what occurred, describe its review of the matter and any specific actions taken to mitigate the impact of the effects of the actual or potential identity theft discovered. Such documentation shall also include a description of any additional actions taken by the office (such as updating policies and procedures) in response to the identified red flag. The office shall provide a copy of those documents to the Controller.

IV. Address Discrepancies

Any University office that obtains and/or uses credit reports from a Consumer Reporting

Agency must ensure that it has procedures in place concerning address discrepancies. Those procedures must enable the office to form a reasonable belief that the consumer report the office has obtained relates to the consumer about whom it requested the report. A notice of address discrepancy means that the office has received notice that the address in the credit report is substantially different from the address in the office's file on the consumer.

The office may reasonably confirm the accuracy of the consumer's address by:

1. Verifying the address with the consumer about whom it as requested the report;
2. Reviewing its own records (e.g., applications, change of address notification forms, other customer account records) to verify the address of the consumer;
3. Verifying the address through third-party sources; or
4. Using other reasonable means.

V. Policy Administration

A. Responsible Parties

Successful implementation of the Identity Theft Policy ultimately is the responsibility of, the employees within each office that maintains accounts or databases covered by this Policy, and the University community as a whole. As permitted by the Red Flag Rules, responsibility for overseeing the administration of the Policy has been delegated by the Board of Trustees to the Office of the Controller, with annual audits to be performed by Internal Audit.

B. Oversight of Third-Party Service Providers

It is the responsibility of the University to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Before the University may engage a service provider to perform an activity in connection with one or more of the University's covered accounts, the University must take the following steps to ensure the service provider performs its activities designed in accordance with reasonable policies and procedures to detect, prevent and mitigate the risks of identity theft:

1. The University must require by contract that the service provider has such policies and procedures in place; and

2. The University must require by contract that the service provider is aware of the University's Identity Theft Policy, and will report any red flags it identifies as soon as possible to the Office of the Controller.

C. Training

Staff training is required for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the University or its customers.

The supervisor of each office that maintains a covered account under this Policy is responsible for ensuring that appropriate identity theft training for all requisite employees, officials and contractors occurs at least annually.

As part of the training, all requisite employees, officials and contractors should be informed of the contents of the University's Identity Theft Policy, and be provided with access to a copy of this document. In addition, all requisite employees, official and contractors should be trained how to identify red flags, and what to do should he/she detect a red flag or have similar concerns regarding an actual or potential fraud involving personal information.

D. Questions

Questions about this policy should be directed to the Office of the Controller.

END OF POLICY TEXT

Additional Resources Regarding This Policy

Related Policies

- Data Protection Standards

- Sensitive Data Incident Response
- FERPA Policy
- HIPAA Policy
- Policy on Access to Electronic Information
- Digital Privacy Statement
- Conditions of Use and Policy on Computing Ethics
- Network Security Monitoring Policy
- Information Security Policy
- Listing of related BU TechWeb Policies

Categories: Finance and Administration, Information Management, Privacy and Security