Identity Theft Prevention Program

In compliance with the Red Flags Rule of the Federal Trade Commission, implementing Section 114 of the Fair and Accurate Credit Transactions Act

October 1, 2009

Fisher College
Identity Theft Prevention Program

I. **Scope.** The Board of Trustees of Fisher College recognizes that certain activities of the College are subject to the provisions of the Federal Trade Commission's (FTC) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACTA Act) of 2003. After consideration of the size and complexity of the College's operations and account systems, the nature and scope of College activities, and in accordance with the requirements of this Rule, the College has developed and adopted this Identity Theft Prevention Program.

II. **Program Requirements.** This Program is designed to detect, prevent, and mitigate identity theft and provide for continued administration of the Program. Requirements and responsibilities of this Program, as mandated by the Red Flags Rule, are as follows:

- Identify Red Flags for new and existing covered accounts
- Detect these identified Red Flags
- Respond appropriately to Red Flags that are identified, and respond suitably to mitigate identity theft
- Ensure that the program is periodically updated to reflect changes in identity theft risks

III. **Definitions.** Red Flag definitions used in this program are as follows:

- "Identity Theft" is a fraud committed or attempted using the identifying information of another person without authority
- A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of identity theft
- A "Covered Account" includes all student accounts or loans that are administered by the College, or any other account that the College offers or maintains for which there is foreseeable risk to identity theft
- "Identifying Information" is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person
- The "Program Administrator" is the individual designated with the primary responsibility for oversight of the Program

IV. **Identification of Red Flags.** Detailed below, the following Red Flags are considered potential indicators of fraud. In any instance, when a Red Flag, or any situation closely resembling a Red Flag, is apparent, it should be investigated and personnel shall begin procedures to prevent and mitigate risk of identity theft and protect identifying information.

A. *Alerts, Notifications, or Warnings from a Consumer Reporting Agency*

- A fraud or active duty alert is included with a consumer report.

- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- Notice or report from a credit agency of an active duty alert for an applicant.
- A consumer-reporting agency provides a notice of address discrepancy.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer.

B. *Suspicious Documents*

- Documents provided for identification appear to have been 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 is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. *Suspicious Personal Identifying Information*

- Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor.
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor.
- The SSN provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
- For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. *Unusual Use of, or Suspicious Activity Related to, the Covered Account*

- Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns.
- A covered account is used in a manner that is not consistent with established patterns of activity on the account.
- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- 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 financial institution or creditor is notified that the customer is not receiving paper account statements.
- The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

E. *Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor.*

- The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

V. Detecting Red Flags. In order to detect Red Flags as indentified in Section IV, the College will take the following steps when establishing Covered Accounts or when monitoring existing Covered Accounts:

A. *New Accounts*

- For purposes of establishing new accounts, require certain indentifying information such name, date of birth, academic records, home address or other identification.
- Verify identity prior to the issuance of a Fisher College student identification card (review driver's license, passport, or other government-issued photo identification).

B. *Existing Accounts*

- For requests of existing account information, verify requester's identification.
- Verify validity of requests to change billing addresses
- Verify requests for changes in banking or credit information being provided for billing and payment purposes.

VI. Responding to Red Flags and Mitigating Identity Theft. In the event College personnel detect Red Flags as identified in Section IV, such personnel shall take appropriate steps to respond to the potential identity theft in accordance with the degree of risk posed by the Red Flag. These steps may include, but are not limited to, the following actions:

- Continue to monitor the account for evidence of identity theft.
- Contact the student, parent or appropriate individual whose account has been detected to be at risk.
- Change passwords or security devices that permit access to the account
- Close existing at risk account.
- Reopen an account with a new number.
- Notify law enforcement.
- Determine that no response is warranted upon review of the circumstances.

VII. Protecting Identifying Information. In order to proactively protect identifying information and diminish the likelihood of identity theft with respect to covered accounts, standard College policies and procedures provide the following guidance:

- Reasonable security and access to individual accounts on the College website must be maintained.
- Complete and secure destruction of paper documents and computer files containing at risk information must be done in accordance with departmental policies on records retention.
- Access to covered accounts through college computers and electronic devices must be password protected.
- Usage of social security numbers should be avoided unless purposes warrant such usage.
- Computer virus protection should be reasonably state-of-the-art and software versions should be current.
- Recordkeeping of information should be limited to information which is deemed necessary for College purposes.
- In the event the College engages a service provider or third party administrator in activity where covered account information is exchanged, the College shall ensure that such provider or administrator has adequate policies and procedures in place addressing identity theft.

VIII. Oversight. Responsibility of this Program lies with the College's Privacy, Security and Identity Theft Committee. The Committee is headed by a Program Administrator who shall be appointed by the President of the College. The Program Administrator shall exercise appropriate and effective supervision over the Program and shall report to the President. Two or more additional individuals appointed by the President will comprise the remainder of the Committee.

IX. Training and Implementation. The Privacy, Security and Identity Theft Committee shall be responsible for the training of College staff, as deemed necessary, in the effective implementation of this Program.

X. Program Updates. At least annually, or as otherwise determined necessary, this Program shall be reviewed, with consideration given to changes in identity theft risks, the College's experiences with identity theft, technological advances, changes in identity theft methods and other relevant factors. Following consideration of these factors, the Program Administrator shall determine whether changes to this Program are warranted, and amendments shall be incorporated accordingly.