

IDENTITY THEFT PREVENTION**REASON FOR POLICY**

To assist in the prevention and detection of identity theft pursuant to the red flag regulations issued by the Federal Trade Commission.

DEFINITIONS

1. Identify theft means fraud committed or attempted using the identifying information of another person without authority.

2. A covered account means:

a. An account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.

b. A **red flag** means a pattern, practice or specific activity that indicates the possible existence of identity theft.

POLICY STATEMENT

A. In order to adequately aid in the prevention and detection of identity theft, the College shall:

1. Identify relevant red flags for covered accounts it offers or maintains;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure that procedures reflect reasonably foreseeable risks to Students and to the safety and soundness of the creditor from identity theft.

B. The College has identified the following covered accounts:

1. Refund of credit balances involving Federal Direct (subsidized and unsubsidized) Stafford loans
2. Refund of credit balances, without Federal Direct (subsidized and unsubsidized) Stafford loans
3. Deferment of tuition payments
4. Emergency loans
5. Tuition payment plan administered by the College.

6. Tuition payment plan administered by third party.

C. The Program identifies the following red flags:

1. Documents provided for identification appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. A request made from a non-College issued E-mail account;
4. A request to mail something to an address not listed on file; and
5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

D. The College will detect red flags relevant to each type of covered account as follows:

1. **Refund of a credit balance involving a Federal Direct Stafford loan** – As directed by federal regulation (U.S. Department of Education) these balance are required to be refunded in the parent's name and mailed to their address on file within the time period specified. No request is required. **Red Flag** – none as this is initiated by the College.

2. **Refund of credit balance, no Federal Direct Stafford loan** – requests from current students must be made in person by presenting a picture ID or in writing from the student's college issued e-mail account. The refund check can only be mailed to an address on file or picked up in person by showing picture ID. Requests from students not currently enrolled or graduated from the college must be made in writing. **Red Flag** – Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.

3. **Deferment of tuition payment** – requests are submitted in person only and require the student's signature. **Red Flag** – none.

4. **Emergency loan** - Requests must be made in person by presenting a picture ID or in writing from the student's college issued e-mail account. The loan check can only be mailed to an address on file or picked up in person by showing picture ID. **Red Flag** - Picture ID not appearing to be authentic or not matching the appearance of the student presenting it. Request not coming from a student issued e-mail account.

5. **Tuition payment plan** – Students must contact an outside service provider and provide personally identifying information to them. **Red Flag** – none, see Oversight of Service Provider Arrangements.

E. The College shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify College Safety; or
5. Determine no response is warranted under the particular circumstances.

F. Responsibility for developing, implementing and updating this policy lies with the Vice President of Finance and Chief Business Officer or designee. The policy Administrator will be responsible for ensuring appropriate training of the College's staff regarding Red Flags, 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.

G. The College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.

Approved:

Board of Trustees
November 12, 2009