Policy Purpose

Wofford College ("College") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the Finance Committee of the College’s Board of Trustees.

Under the Red Flags Rule, the College is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and nature of its operations. Each program must contain reasonable policies and procedures to:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
2. Detect risks when they occur in covered accounts;
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

This policy and protection program applies to employees, contractors, consultants, temporary workers, and other workers at the College, including all personnel affiliated with third parties.

SECTION I: IDENTIFICATION OF COVERED ACCOUNTS

1.1 Types of Covered Accounts

The College maintains the following types of covered accounts:

1. Student Accounts with Perkins loans
2. Student Accounts with past due balances
3. Student Accounts on SallieMae’s AMS payment plan
The student accounts listed above are "covered accounts" under the Red Flag Rules. They are maintained primarily for receipt of educational and related services and permit multiple payments or transactions over the life of the student relationship as well as posing a reasonable, foreseeable risk to students and the College from identity theft.

Covered student accounts might be the subject of identity theft in the establishment of new student accounts, in the maintenance of student accounts, in the acceptance of payment, and in referral of student accounts for collection.

Identity theft risks associated with student accounts include a student's using another person's identity or a fictional identity in setting up a new account with the College; and a student's seeking credit using the identity of an existing student, which is then billed to the existing student's account.

SECTION II: DETECTING, PREVENTING, AND MITIGATING IDENTITY THEFT

2.1 Identification of Red Flags

In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The following are relevant Red Flags, in each of the listed categories, which College personnel should be aware of and diligent in monitoring for:

A. Suspicious Documents

➢ Identification document or card that appears to be forged, altered or inauthentic;
➢ Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
➢ Other document with information that is not consistent with existing student information (such as if a person's signature on a check appears forged); and
➢ Application for service that appears to have been altered or forged.

B. Suspicious Personal Identifying Information

➢ Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
➢ Identifying information presented that is inconsistent with other sources of information;
➢ Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
➢ Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
➢ Social security number presented that is the same as one given by another student;
➢ An address or phone number presented that is the same as that of another person;
➢ A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
➢ A person's identifying information is not consistent with the information that is on file for the student.
C. Suspicious Account Activity or Unusual Use of Account

➤ Change of address for an account followed by a request to change the account holder's name;
➤ Payments stop on an otherwise consistently up-to-date account;
➤ Account used in a way that is not consistent with prior use (example: very high activity);
➤ Mail sent to the account holder is repeatedly returned as undeliverable;
➤ Notice to the College that a student is not receiving mail sent by the College;
➤ Notice to the College that an account has unauthorized activity;
➤ Breach in the College's computer system security; and
➤ Unauthorized access to or use of student account information.

D. Alerts from Others

➤ Notice to the College from a student, 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.

2.2 Detecting Red Flags

A. New Accounts

In order to detect any of the Red Flags identified above associated with the enrollment of a student, College personnel will take the following steps to obtain and verify the identity of the person opening the account:

➤ Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;
➤ Verify the student's identity (for instance, review a driver's license or other identification card);

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, College personnel will take the following steps to monitor transactions with an account:

➤ Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
➤ Verify the validity of requests to change billing addresses; and
➤ Verify changes in banking information given for billing and payment purposes.

2.3 Other Steps to Be Taken In Order To Protect Student Information
In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student identifying information:

- Ensure that its website is secure or provide clear notice that the website is not secure;
- Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
- Ensure that office computers with access to Covered Account information are password protected;
- Ensure computer virus protection is up to date;
- Require and keep only the kinds of student information that are necessary for College purposes.

2.4 Responding to Red Flags and Mitigating Identity Theft

In the event College personnel detect any identified Red Flags, such personnel 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 student or applicant;
- 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; or
- Determine that no response is warranted under the particular circumstances.

SECTION III: ASSIGNED RESPONSIBILITIES

The Coordinator of Human Resources has been designated Program Administrator. The Program Administrator shall exercise appropriate and effective oversight over the Program and shall report regularly to the President’s Cabinet on the Program.

The Program Administrator, with the assistance of other key College personnel, is responsible for developing, implementing and updating the Program throughout the College. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for identifying, 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.

SECTION IV: SERVICE PROVIDER AGREEMENTS

In the event the College engages a service provider to perform an activity in connection with one or more covered accounts, the College will take the following steps to ensure the service provider
performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

➢ Require, by contract, that service providers have such policies and procedures in place; and
➢ Require, by contract, that service providers review the College's Program and report any Red Flags to the Program Administrator.
➢ The College has identified the following service providers dealing with covered accounts:
  1. Campus Partners (Perkins Loan Administrator)
  2. Various Collection Agencies (Perkins Loans)
  3. SallieMae (TuitionPay Participants)

SECTION V: TRAINING AND ANNUAL REPORTS

College employees responsible for implementing the Program shall be trained under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

Staff dealing with covered accounts will be required to attend an initial training within one year of the Program's implementation. If changes are made to the Program or its requirements, staff will be provided additional training. As new employees are hired who will be dealing with covered accounts, they will be, at a minimum, required to read training materials. Upon completion of all training, whether in a classroom setting or through self-study, staff will be required to sign an affidavit stating that they are aware of and comply with the policy statement.

College employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the College's failure to comply with this program.

The Program Administrator will be responsible for developing and presenting the annual report on the efficacy of the Program and recommending, establishing, and implementing updates to the Program.

An annual report will be provided to the President's Cabinet each year addressing material matters concerning the Program, such as:

➢ Analyzing the effectiveness of the College's identity theft policies and procedures;
➢ Examining any and all types of new accounts the College has instituted in the previous year;
➢ Evaluating new service provider arrangements;
➢ Identifying significant incidents, if any, of identity theft, including the College's response; and
➢ Setting forth recommendations for material changes to the Program based on developments in the past year.
SECTION VI: UPDATING THE PROGRAM

The Program shall be periodically revisited and updated, as necessary, to reflect changes in risks to covered accounts or to the safety and soundness of the College from identity theft based on such factors as:

➤ The experiences of the College with identify theft;
➤ Changes in methods of identity theft;
➤ Changes in methods to detect, prevent, and mitigate identity theft;
➤ Changes in the types of accounts that the College offers or maintains; and
➤ Changes in the business arrangements of College, including alliances, joint ventures, and service provider arrangements.

This resolution will take effect immediately upon its passage.

R. Michael James
Chair of the Finance Committee

Approved this _________ day of ______________, 2009
October 20, 2009

RESOLUTION

RESOLVED: In accordance with the policies and procedures of the Wofford College Board of Trustees and based on the recommendation of the Finance Committee, the Board of Trustees of Wofford College hereby adopts the Identity Theft Policy as presented.

[Signature]
Board Chair

[Signature]
Board Secretary