Indian Hills Community College
Identity Theft Prevention Program
RED FLAGS Rule

## I. Program

This document establishes a written Identity Theft Prevention Program designed to detect the warning signs or 'red flags' of identity theft in the daily operations of Indian Hills Community College employees working with student identifying information. The program addresses detection of the red flags of identity theft, actions to prevent the crime and to mitigate the damage it inflicts. The program complies with the rules and guidelines set forth in 16 CFR, Part 681 Identity Theft Rules implementing the requirements of the Fair and Accurate Credit Transactions Act (FACTA) of 2003 as enforced by the Federal Trade Commission.

## II. Purpose

The program will achieve its objectives by including procedures to:

- Identify relevant red flags for covered accounts offered by the College.
- Detect the relevant red flags as they occur.
- Respond properly to the red flags that are detected in order to prevent or mitigate identity theft.
- Assure the program is evaluated to accommodate the changes in identity theft risks on an ongoing basis.

## III. Terms and Definitions

- Identity Theft is a fraud committed or attempted using the identifying information of another person without authority.
- Red Flag – a pattern, practice, or specific activity that indicates the possible existence of identity theft.
- Covered Account – includes all student accounts, payment plans or loan proceeds that are administered by the College.
- Indentifying information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to: 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, student identification number, computer's Internet Protocol address or routing code.

## IV. Procedures and Guidelines

A. Overview of Covered Accounts

- Payment Plans – Payment plans are available to all actively enrolled students. The following identifying information is required to be an actively enrolled student:
  - College application

- Direct Loans – Loans are offered to students based on eligibility information included in the Free Application for Federal Student Aid (FAFSA). The following identifying information is included and verified by multiple government agencies:
  - Income and asset information for student and the parents of dependent students.

- Social security number of student and the parents of dependent students.
- Birth date of student and the parents of dependent students.

- Alternative Loans – Alternative loans are processed by third parties that must demonstrate effective information security programs that comply with current industry regulations.

- Loan proceeds are first applied to the student's Indian Hills account. Any excess is remitted by check to the student and can be picked up with a photo ID or mailed to the student's address on file.

- Identity Theft Risk – Indian Hills has not experienced any incidents of identity theft related to its covered accounts in the past, and evaluates that the risk is low for identity theft to occur in the future for the following reasons:
  - Account statements regarding payment plans and loans include an ID number specific to the College instead of a social security number.
  - There are effective safeguards against identity theft in the administration of loans and payment plans.
  - Third parties that perform debt collection services for the College demonstrate effective information security programs that comply with the current industry regulations.

B. Identification of Red Flags
- Payment Plans – The following situations would each constitute a red flag for the initiation of payment plans:
  - Documents that appear to have been altered or forged.
  - Discrepancies between various components of the identifying information required for active enrollment.
  - Notice from victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft.

- Loans – The following situations would each constitute a red flag for the initiation of loans:
  - Notice from other government entities that utilize FAFSA information, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft.
  - Accepted award letters from students who are not actively enrolled.

C. Detection of Red Flags – Red flags for payment plans and loans will be detected by:
- Obtaining and verifying complete identification information for inquiries regarding a covered account or payment plan.
- Maintaining lines of communication about the validity of existing covered accounts at the College.

D. Responses to Red Flags – The detection of a red flag at the College will trigger a response that is commensurate to the amount of risk associated with the red flag. Appropriate responses include:
- Closely monitor a covered account for evidence of identity theft.
- Contact the student holding the covered account.
- Close an existing covered account.
- Notify law enforcement.
- Determine that no response is necessary given the circumstances.

E. Ongoing Administration

- Oversight of the Program – The Board of Trustees will approve the initial identity theft protection program. Afterward, the College's CORE Oversight Committee will oversee implementation of the identity theft prevention program. The responsibility for detecting red flags will lie with multiple offices on campus that collect identifying information from students and/or initiate covered accounts.

- Updating the Program – The identity theft protection program will be periodically updated by the CORE Oversight Committee to reflect the following factors:
  - Changes in methods of identity theft.
  - Changes in procedures for detecting, preventing, and mitigating identity theft.
  - Changes in the types of covered accounts the College offers.
  - Changes in service provider agreements.

Date: August 2009