SFS Identity Theft Prevention Program & Red Flags

Name of Institution: UNIVERSITY OF ARKANSAS FOR MEDICAL SCIENCES

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 UAMS Student Financial Services (SFS) 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. SFS does not create student accounts, change address/phone number or update Social Security Numbers.

Additional Resources

UAMS Policy 2.1.25
SFS Student and Third Party Authentication Policy

Program Adoption

The University of Arkansas System Board of Trustees adopted an Identity Theft Prevention Program ("Program") in compliance with Part 681 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 and pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule ("Rule"). The purpose of this program is to establish processes at the University of Arkansas campuses to:

1. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the Program.
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.
4. Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from identity theft.

Each campus is responsible for implementing a plan to:

1. Identify covered accounts.
2. Identify relevant red flags.
3. Establish policies and procedures to detect red flags and respond appropriately.
4. Establish policies and procedures to ensure appropriate and effective oversight of service providers.
5. Provide training to the appropriate staff in the detection of red flags and responsive steps required when a red flag is detected.
6. Report to the program administrator on incidents of identity theft, the effectiveness of the Program, campus compliance with the Program, and other relevant data.
7. Designate a campus administrator who is responsible for administering and implementing the Program at the campus level.

Definitions

Identity Theft - 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 - Any account the university offers or maintains that is designed to permit multiple payments or transactions or one for which there is a foreseeable risk of identity theft.

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, student identification number, computer's Internet Protocol address, or routing code.

Purpose

The program will achieve its objectives by including procedures to:

- Identify relevant red flags for covered accounts offered by SFS.
- 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.

Procedures and Guidelines

A. Overview of Covered Accounts

- Federal Student Aid (including campus-based) – Federal and campus-based aid is 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 UAMS account. Any excess is remitted by direct deposit or paper check to the student. Paper checks are mailed to the student's address on file.
- Identity Theft Risk – UAMS SFS 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 federal and campus-based aid includes an ID number specific to the College instead of a social security number.
    - There are effective safeguards against identity theft in the administration of Federal and Campus-based aid
    - Third parties that perform debt collection services for SFS demonstrate effective information security programs that comply with the current industry regulations.

B. Identification of Red Flags

- Federal Student Aid (including campus-based) – The following situation would each constitute a red flag for the initiation of Federal and/or Campus-based aid:
    - Notice from other government entities that utilize FAFSA information, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft.

C. Detection of Red Flags – Red flags for Federal and Campus-based Aid will be detected by:

- Obtaining and verifying complete identification information for inquiries regarding a covered account.
- Maintaining lines of communication about the validity of existing covered accounts.

D. Responses to Red Flags – The detection of a red flag by SFS 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 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 UAMS SFS Staff to reflect the following factors:
    - Changes in methods of identity theft.
    - Changes in procedures for detecting, preventing, and mitigating identity theft.
    - Changes in service provider agreements.