University of Arkansas at Monticello
Identity Theft Prevention Program

Overview

The University Of Arkansas System Board Of Trustees adopted an Identity Theft Prevention Program (ITP) 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. The purpose of this program is to establish processes at the University of Arkansas campuses to:

A. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the ITP Program;
B. Detect Red Flags that have been incorporated into the ITP Program;
C. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
D. Ensure the ITP 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:

A. Identify covered accounts.
B. Identify relevant Red Flags.
C. Establish policies and procedures to detect Red Flags and respond appropriately.
D. Establish policies and procedures to ensure appropriate and effective oversight of service providers.
E. Provide training to the appropriate staff in the detection of Red Flags and responsive steps required when a Red Flag is detected.
F. Report to the ITP Program Administrator on incidents of identity theft, the effectiveness of the ITP Program, campus compliance with the ITP Program and other relevant data.
G. Designate a Campus Administrator who is responsible for administering and implementing the ITP 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 UAM offers or maintains that is designed to permit multiple payments or transactions or one which there is a foreseeable risk of Identity Theft.

Program Administrator – the Vice Chancellor for Finance and Administration is designated with primary responsibility for oversight of the ITP Program.

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

Identification of Covered Accounts

UAM has determined that covered accounts are established and maintained that fall under the requirements of FTC Rule 681.1 and 681.2 described as follows:

A. Utilization of reports from consumer reporting agencies for credit or background checks for collection purposes. (681.1)
B. Utilization of reports from consumer reporting agencies for credit or background checks of new hire applicants or employees in positions identified as requiring credit or background checks. (681.1)
C. Establishment of credit accounts for students such as deferred payment plans for tuition and fees. (681.2)

Identification of Red Flags

In order to identify relevant Red Flags, UAM considers the types of accounts that it offers and maintains, methods to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. UAM identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Consumer Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report or collection report;
2. Notice or report from a credit agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;

2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student information; and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

<u>Red Flags</u>

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on an application);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social Security Number presented that is the same as one given by another student;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so; and
8. A person's identifying information is not consistent with the information that is on file for the student.

D. Suspicious Student Account Activity or Unusual Use of Account

<u>Red Flags</u>

1. Change of address for an account followed by a request to change the student's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the student is repeatedly returned as undeliverable;
5. Notice to the university that a student is not receiving mail sent by the university;
6. Notice to the university that an account has unauthorized activity;
7. Breach in the university's computer system security; and
8. Unauthorized access to or use of student account information.

E. Alerts from Others

<u>Red Flags</u>

1. Notice to the university from a student, Identity Theft victim, law enforcement or other person that the university has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Detecting Red Flags

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

Detect

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

B. Existing Accounts – In order to detect any of the Red Flags identified above for existing Student Accounts, University personnel will take the following steps to monitor transactions on an account:

Detect

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email); and
2. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes.

Preventing and Reporting Identify Theft

A. In the event University personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Report

1. Notify the immediate supervisor, who should then notify the Vice Chancellor for Finance and Administration to determine if additional steps are needed;
2. The account holder should only be contacted upon approval from the Vice Chancellor for Finance and Administration;
3. Require and keep only the kinds of student information that are necessary for University purposes.

Program Administration

A. Oversight – Responsibility for developing, implementing, and updating this Program lies with Program Administrator.

B. Staff Training and Reports – University staff responsible for implementing the ITP program shall either be trained by or under direction of the Vice Chancellor for Finance and Administration in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. Annually, the Vice Chancellor for Finance and

Administration shall report to the University of Arkansas System on the incidents of identity theft, the effectiveness of the program, and the university's compliance.

C. Service Provider Arrangements – In the event the university engages a service provider to perform an activity in connection with one or more Covered Accounts, the university 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 report the risk of Identity Theft:

  1. Require that service providers have such policies and procedures in place and provide a copy to the university; and
  2. Require that service providers review the university's ITP program and report any Red Flags to the Vice Chancellor for Finance and Administration.

D. Program Updates – The University will periodically review and update this program to reflect changes in risks to students. The university will consider its experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the university's business arrangements with other entities and update accordingly.