

ASU System Policy

Effective Date: April 24, 2009

Subject: Identity Theft Prevention

Category: IT, Security, Privacy & Records 3.01

1. Purpose

Arkansas State University System (ASU System) developed this Identity Theft Prevention Policy (the Program) pursuant to the Federal Trade Commission's (FTC) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The Program was developed with oversight by and approval as a policy of the ASU System Board of Trustees.

2. Definitions

Institution Program Administrator. The Institution Program Administrator is the strike campus individual designated with primary responsibility for oversight of the program on their campus.

Consumer Report. Consumer Report has the same meaning as defined in the Fair Credit Reporting Act.

Covered Account. A Covered Account includes all student and employee accounts maintained primarily for personal, family, or household purposes that involve multiple payments or transactions.

Identifying Information. Identifying information is 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.

Identity Theft. Identity theft is a fraud committed or attempted using the identifying information of another person without authority.

Red Flag. A red flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Arkansas State System (ASU System). Arkansas State University System means all the institutions within the Arkansas State University System, now and in the future.

3. Policy

ASU System maintains an identity theft prevention program tailored to its size, complexity and the nature of its operation. The program contains reasonable procedures to:

- A. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the program;
- B. Detect red flags that have been incorporated into the program;
- C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- D. Ensure the program is updated periodically to reflect changes in risks.

4. Process

Identifying Red Flags. In order to identify relevant red flags, ASU System considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with identity theft. ASU System identifies the following red flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

- I. Report of fraud accompanying a credit report;
- II. Notice or report from a credit agency of a credit freeze on an applicant;
- III. Notice or report from a credit agency of an active duty alert for an applicant;
- IV. Receipt of a notice of address discrepancy in response to a credit report request; and
- V. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

- I. Identification document or card that appears to be forged, altered, or inauthentic;
- II. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- III. Other document with information that is not consistent with existing information; and

- IV. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

- I. Identifying information presented that is inconsistent with other information the person provides (example: inconsistent birth dates);
- II. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
- III. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- IV. Identifying information presented that is inconsistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- V. Social security number presented that is the same as one given by another person;
- VI. An address or phone number presented that is the same as that of another person;
- VII. A person fails to provide complete personal identifying information on an application when reminded to do so; and
- VIII. A person's identifying information is not consistent with the information that is on file for the person.

D. Suspicious Covered Account Activity or Unusual Use of Account

- I. Change of address for an account followed by a request to change the person's name;
- II. Payments stop on an otherwise consistently up-to-date account;
- III. Account used in a way that is not consistent with prior use;
- IV. Mail sent to the person is repeatedly returned as undeliverable;
- V. Notice to ASU System that a person is not receiving mail sent by the ASU System;
- VI. Notice to ASU System that an account has unauthorized activity;
- VII. Breach in ASU System's computer system security; and
- VIII. Unauthorized access to or use of a person's account information.

E. Alerts from Others

- I. Notice to ASU System from a student, employee, identity theft victim, law enforcement or other person that ASU System 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 in this policy associated with the enrollment of a student, ASU System personnel will

take the following steps to obtain and verify the identity of the person opening the account:

- I. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
- II. Verify the student's identity at the time of issuance of a 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 an existing covered account, ASU System personnel will take the following steps to monitor transactions on an account:

- I. Verify the identification of persons if they request information (in person, via telephone, via facsimile, via email);
- II. Verify the validity of requests to change billing addresses by mail or email and provide the person a reasonable means of promptly reporting incorrect billing address changes; and
- III. Verify changes in banking information given for billing and payment purposes.

C. Consumer Report Requests. In order to detect any of the red flags identified above for an employment or volunteer position for which a consumer report is sought, ASU System personnel will take the following steps to assist in identifying address discrepancies:

- I. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
- II. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the ASU System has reasonably confirmed is accurate.

Action upon Detection of Red Flags

A. Preventing and Mitigating Identity Theft. In the event ASU System 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:

- I. Continue to monitor a covered account for evidence of identity theft;
- II. Contact the student, employee, or applicant (for which a credit report was run);
- III. Change any passwords or other security devices that permit access to covered accounts;
- IV. Refuse to open a new covered account;

- V. Provide the student or employee with a new student or employee identification number;
- VI. Notify the campus program administrator for determination of the appropriate step(s) to take;
- VII. Notify law enforcement;
- VIII. File or assist if filing a Suspicious Activities Report (“SAR”); or
- IX. Determine that no response is warranted under the particular circumstances.

Protecting Student Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the ASU System will take the following steps with respect to its internal operating procedures to protect student identifying information:

- I. Ensure that its website is secure or provide clear notice that the website is not secure;
- II. 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;
- III. Ensure that office computers with access to covered account information are password protected;
- IV. Avoid use of social security numbers;
- V. Ensure computer virus protection is up to date; and
- VI. Require and keep only the kinds of student information that are necessary for ASU System purposes.

Program Administration

- A. Oversight.** Responsibility for developing, implementing and updating the program lies with an Identify Theft Committee (“Committee”) for each institution of the ASU System. The committee is headed by a campus program administrator who may be the chancellor of the campus or his or her appointee. Each campus will have an Identity Theft Prevention Committee. Annually, each campus committee through the campus chancellor will provide a comprehensive report of activities that occurred during the past year to the President of the Arkansas State University System. The campus program administrator will be responsible for ensuring appropriate training of university staff on the program, 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.
- B. Staff Training and Reports.** ASU System staff responsible for implementing the program shall be trained either by or under the direction of the campus program administrator in the detection of red flags and the responsive steps to be taken

when a red flag is detected. ASU System staff shall be trained, as necessary, to effectively implement the program. At least annually or as otherwise requested by the campus program administrator, ASU System staff responsible for development, implementation, and administration of the program shall report to the campus program administrator on compliance with the program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of covered accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the program.

C. Service Provider Arrangements. In the event the ASU System engages a service provider to perform an activity in connection with one or more covered accounts, the ASU System 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.

- I. Require, by contract, that service providers have such policies and procedures in place; and
- II. Require, by contract, that service providers review the ASU System's program and report any red flags to the campus program administrator or the employee with primary oversight of the service provider relationship.

D. Non-disclosure of Specific Practices. For the effectiveness of the program, knowledge about specific red flag identification, detection, mitigation and prevention practices will be limited to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be shared with other university employees or the public. The campus program administrator shall inform the committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

E. Program Updates. The campus committees will periodically review and update the program to reflect changes in risks from identity theft. In doing so, the committee will consider the ASU System's experiences with identity theft situations, changes in identity theft methods, changes in identity theft methods for detection and prevention, and changes in the ASU System's business arrangements with other entities. After considering these factors, the campus program administrators will determine whether changes to the program, including the listing of red flags, are warranted. If warranted, the committee will update the program.

(Adopted by the Arkansas State University Board of Trustees on April 24, 2009,
Resolution 09-13.)