UNIVERSITY OF CENTRAL ARKANSAS™

Identity Theft Prevention Program

I. PROGRAM ADOPTION

The following Identity Theft Prevention Program ("Program") was developed by the University of Central Arkansas ("UCA") in response to the Federal Trade Commission's ("FTC") Red Flags Rule ("Rule") and to comply with Part 681 of the Code of Federal Regulations implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The UCA Board of Trustees (the Board) met on August 17, 2018 and approved all aspects of this Program. The Board agreed that based on the size and complexity of UCA, this Program's purpose is to establish processes that:

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.

II. DEFINITIONS

The Rule defines the following that are used in the Program:

"Identity Theft" is a "fraud committed or attempted using the identifying information of another person without authority."
A "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."
A "Covered Account" includes all student accounts or loans that are administered by the University.
"Program Administrator" is the individual designated with primary responsibility for oversight of the program described in Section VI.
"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 (UCA ID), computer's Internet Protocol (IP) address, or routing code.

UNIVERSITY OF CENTRAL ARKANSAS™

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, UCA 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. UCA identifies the following Red Flags in the listed categories below:

A. Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit 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

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

1. Identifying information presented that is inconsistent with other information the student provides (e.g., inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (e.g., an address not matching an address on a loan 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 (e.g., an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another individual;
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 Covered Account Activity or Unusual Use of Account
    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 UCA that a student is not receiving mail sent by UCA;
    6. Notice to UCA that an account has unauthorized activity;
    7. Breach in UCA's computer system security; and
    8. Unauthorized access to or use of student account information.

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

IV. DETECTING RED FLAGS

A. Student Enrollment

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

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 the 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 an existing Covered Account, UCA personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
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; and
3. Verify changes in banking information given for billing and payment purposes.

C. Consumer ("Credit") Report Requests

In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, UCA personnel will take the following steps to assist in identifying address discrepancies:

1. 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
2. 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 UCA has reasonably confirmed is accurate.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event UCA 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:

1. Continue to monitor a Covered Account for evidence of Identity Theft;
2. Contact the student or applicant (for which a credit report was run);
3. Change any passwords or other security devices that permit access to Covered Accounts;
4. Not open a new Covered Account;
5. Provide the student with a new student identification number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. File or assist in filing a Suspicious Activities Report ("SAR"); and
9. Determine that no response is warranted under the particular circumstances.

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, UCA will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student information per UCA's Document Retention Guidelines;
3. Ensure that office computers with access to Covered Account information are password protected (UCA IT Network Password Policy, UCA IT Safeguarding System Passwords Policy);
4. Avoid use of social security numbers when possible;

5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of student information that are necessary for UCA purposes.

VI. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating the Program lies with the Program Administrator, the Vice President for Finance and Administration. The Program Administrator may delegate responsibilities to and/or consult with other offices as necessary to ensure appropriate training of UCA staff on the Program, to review any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, to determine which steps of prevention and mitigation should be taken in particular circumstances, and to consider periodic changes to the Program.

B. Staff Training and Reports

UCA staff responsible for implementing the Program shall be trained by or under the direction of the Program Administrator or designee(s) in the detection of Red Flags and the responsible steps to be taken when a Red Flag is detected. UCA staff shall be trained, as necessary, to effectively implement the Program. UCA employees are expected to notify the Program Administrator or designee(s) once they become aware of an incident of Identity Theft or of UCA's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, UCA staff responsible for development, implementation, and administration of the Program shall report 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 UCA engages a service provider to perform an activity in connection with one or more Covered Accounts, UCA 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:

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the Program and report any Red Flags to the Program Administrator or designee(s) or the office 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 may be limited to the Program Administrator and 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 UCA employees or the public unless required by the Arkansas Freedom of Information Act. The Program Administrator or designee(s) shall inform 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 Program Administrator or designee(s) will periodically review the Program to ensure it addresses risks to students and the soundness of UCA from Identity Theft. In doing so, they will consider UCA's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in UCA's business arrangements with other entities. After considering these factors, the Program Administrator or designee(s) will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program will be updated accordingly.

F. Effective Date

The Program is effective August 17, 2018.