Identity Theft Prevention Program

Approved by the Arizona Board of Regents on May 1, 2009

I. Purpose & Scope

This Program was developed pursuant to the Federal Trade Commission's ("FTC") Red Flag Rules promulgated pursuant to the Fair and Accurate Credit Transactions Act (the "FACT Act"). The University's Program, as set forth herein, is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered accounts within the University, and is appropriate to the size and complexity of the University as a creditor and the nature and scope of its activities.

II. The "Red Flag Rules" Overview

The Red Flag Rules, found at 16 CFR § 681.2, require a creditor to periodically determine, by conducting a risk assessment, whether it offers or maintains covered accounts. Upon identifying any covered account(s), the creditor is required to develop and implement a written Identity Theft Prevention Program designed 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 that the Program is updated periodically to reflect changes in risks to the account holders or to the safety and soundness of the creditor from Identity Theft, as defined below.

The rules require that the creditor's Board of Regents initially approve the written Identity Theft Prevention Program, whereas continued oversight and administration of the Program may be delegated to a Board committee or an employee at the level of senior management.

III. Definitions

A. **"Account"** means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or

business purposes. It includes (i) an extension of credit, such as the purchase of property or services involving a deferred payment, and (ii) a deposit account.

B. **"Covered Account"** means (i) an account that a creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions and (ii) any other account that the creditor offers to maintain for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

C. **"Identity Theft"** means a fraud committed or attempted using the identifying information of another person without authority.

D. **"Red Flag"** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

E. **"Service Provider"** means a person that provides a service directly to the financial institution or creditor.

IV. Covered Accounts Maintained by University of Arizona

A. Federal Perkins Loan Program
B. Health Professions Loan Program
C. Nursing Loan Program
D. Institutional Loans
E. Bursar/Student Accounts
F. University Stored-Value ID Cards

V. Identification of Red Flags

In identifying below specific Red Flags unique to these covered accounts, the University considered the following risk factors: the types of covered accounts offered and maintained, the methods provided for opening and accessing each of those accounts, prior experiences with Identity Theft, and the size, complexity, nature and scope of our institution and its activities. Each of the Red Flags mentioned below may only be applicable to certain of the covered accounts administered by the University.

A. <u>Alerts, notifications or warnings from a consumer reporting agency</u>:

1. Receipt of a fraud or active duty alert accompanying a consumer credit report;
2. Receipt of a notice of credit freeze provided in response to a request for a consumer report;
3. Receipt of a notice of address discrepancy from a credit reporting agency; and
4. Receipt of a consumer report which indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of the account holder (e.g. recent and significant increase in number of inquiries; unusual number of recently established credit relationships; a material change in the use of credit).

B. Suspicious Documents

1. Documents presented for the purpose of personal identification are incomplete or appear altered, forged or inauthentic;
2. The photographic and/or physical description on the personal identification is inconsistent with the appearance of the individual presenting the document;
3. Other information contained on the personal identification is inconsistent with information provided by the individual opening a new covered account or when presenting the personal identification for verification;
4. Other information contained on the personal identification is inconsistent with readily accessible information on file with the University; and
5. An application received by the University appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious Personal Identifying Information

1. Personal identifying information provided is inconsistent when compared against external information sources used by the University (e.g. discrepancies in addresses);
2. Personal identifying information provided is inconsistent when compared against internal information held by University, such as discrepancies in addresses, phone numbers, and other personal identifying information;

3. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University, such as fictitious and/or duplicated phone numbers, addresses or SSN;
4. Personal identifying information provided is fictitious and/or the same or very similar to that submitted by others opening an account or holding existing accounts, such as addresses, telephone numbers, bank accounts, and social security numbers;
5. The student or individual opening a covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete; and
6. Challenge questions, used by University to allow students and individuals to access their covered accounts, are answered incorrectly.

D. Unusual Use of, or Suspicious Activity Related to, the Covered Account

1. Shortly following a change of address to a covered account, or a request to change the address, University receives a request to change the account holder's name, a request for the addition of authorized users on the account, or other suspect request;
2. A covered account that has been inactive for a reasonably lengthy amount of time is used in an unusual manner;
3. Mail sent to the account holder is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account;
4. The University is notified that the student or individual is not receiving paper account statements and those statements are not being returned as undeliverable; and
5. The University is notified of unauthorized changes or transactions in connection with a student's or individual's covered account.

E. Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by University

1. University is notified by a student or individual account holder, a victim of Identity Theft, a law enforcement entity, or any other person that it has

opened a fraudulent account for a person engaged in Identity Theft.

VI. Red Flag Detection

To detect the Red Flags identified above, the following actions will be taken, when appropriate given the particular covered account at issue and under the particular circumstances, to confirm the identity of students and individuals when they open and/or access their covered accounts:

A. Appropriate personal identifying information (e.g., photo identification, date of birth, academic status, user name and password, address, etc.) shall be obtained from the student or individual account holder, prior to issuing a new or replacement ID card, opening a covered account, or allowing access to a covered account.
B. When certain changes to a covered account are made online, students and individuals holding covered accounts shall receive notification to confirm the change was valid and to provide instruction in the event the change is invalid.
C. Suspicious changes made to covered accounts that relate to an account holders identity, administration of the account, and billing and payment information shall be verified.

VII. Prevention and Mitigation of Identity Theft

In addition to the efforts noted above to detect Identity Theft, University personnel involved in the administration of the covered accounts will take the following steps, where appropriate and based upon the particular circumstances, to prevent and mitigate occurrences of Identity Theft when a Red Flag is detected:

A. Monitor a covered account for evidence of Identity Theft;
B. Contact student(s) and/or individual account holder(s);
C. Request additional documentation from the student and/or individual account holder to verify identity;
D. Change passwords, security codes and other security devices permitting access to the covered account;
E. Reopen a covered account with a new account number;
F. Decline to open a new covered account;
G. Close an existing covered account;
H. Notify law enforcement;

I. Determine that no response is warranted under the particular circumstances;
J. Attempt to identify the cause and source of the Red Flag; and
K. Take appropriate steps to modify the applicable process to prevent similar activity in the future.

VIII. Program Administration

A. Approval and Oversight: The Arizona Board of Regents shall be responsible for the initial approval of this Program. Authority to implement and administer the Program and to approve all future revisions to the Program shall be delegated to the President and to those he deems appropriate.

B. Program Assessment and Update: This Program should be periodically reviewed and updated following a risk assessment of the following factors: prior experiences with identity theft; changes in the methods of identity theft; changes in the method of detection, prevention and mitigation of identity theft; the covered accounts offered and administered by the University; and the potential Red Flags that may arise with respect to the Covered Accounts. The periodic assessment should also include review of the reports required pursuant to Section C below. This periodic assessment should consider any changes in risks to students and individual account holders and to the safety and soundness of the University from identity theft.

C. Reporting: At least annually, University departments responsible for the development, implementation and administration of this Program with respect to specific covered accounts identified herein should report to the President, regarding their compliance with this Program. The report(s) should address material matters relating to the Program and evaluate the effectiveness of the Program in addressing risks of identity theft in connection with the opening of covered accounts and administering existing covered accounts. The report(s) should also, where applicable, evaluate service provider arrangements, the handling of significant instances of identity theft, and recommend necessary material changes to the Program.

D. Staff Training: University departments, delegated responsibility for the development, implementation and administration of this Program with respect to specific covered accounts, should develop and implement plans to

effectively train their staff in the identification, detection, prevention and mitigation of the Red Flags identified above that are unique to their specific covered accounts. Staff training should be conducted on a regular basis and as necessary under the circumstances related to the administration of the particular covered account.

E. Oversight of service providers: If and when the University engages a service provider to perform an activity in connection with a covered account, University departments delegated responsibility for administering this Program with respect to that particular covered account, should take steps necessary to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.