Identity Theft Prevention Program

February 27, 2009

Table of Contents

Identity Theft Prevention Program

1. Program Description

The University adopts this Identity Theft Prevention Program (the "Program") in an effort to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account," as defined in Section 2-A.

The purpose of the Program is:

A. To identify patterns, practices, or specific activities ("Red Flags") that indicate the possible existence of identity theft with regard to new or existing covered accounts;

B. To detect Red Flags that have been incorporated into the Program;

C. To respond appropriately to any Red Flags that are detected under the Program; and

D. To ensure periodic updating of the Program, including reviewing the accounts that are covered and the identified Red Flags that are part of the Program, to reflect changes in risk to students, faculty, staff, and other constituents.

2. Identity Theft Definitions

A: Covered accounts

For the purpose of the University's Identity Theft Prevention Program, a "covered account" includes any account that involves or is designed to permit multiple payments or transactions, such as a student account that provides for payment of tuition in installments. In addition, every new and existing account maintained by the University for its students, faculty, staff, and other constituents that meets the following criteria is covered by this Program:

(1) Accounts for which there is a reasonably foreseeable risk of identity theft; or

(2) Accounts for which there is a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

B: Identifying Information

The term ``identifying information'' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any

(1) Name, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address, or routing code; or

(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)), namely, any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

3. Identity Theft Indicators: Types of Red Flags

The following Red Flags are potential indicators of fraud:

A. Suspicious documents. Examples of these Red Flags include the following:

(1) Documents provided for identification that appear to have been altered or forged;

(2) The photograph or physical description on the identification is not consistent with the appearance of the student, faculty, staff, and other constituent presenting the identification;

(3) Other information on the identification is not consistent with information provided by the person opening a new covered account or student, faculty, staff, and other constituent presenting the identification;

(4) Other information on the identification is not consistent with readily accessible information that is on file with the University; and

(5) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

B. Suspicious personally identifying information. Examples of these Red Flags include the following:

(1) Personally identifying information provided is inconsistent when compared against external information sources used by the University;

(2) Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University;

(3) Personally identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University;

(4) The social security number provided is the same as that submitted by another student, faculty, staff, or constituent;

(5) The person opening the covered account fails to provide all required personally identifying information on an application or in response to notification that the application is incomplete;

(6) Personally identifying information provided is not consistent with personal identifying information that is on file with the University; and

(7) When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

C. Unusual use of, or suspicious activity related to, the covered account. Examples of these Red Flags include the following:

(1) Shortly following the notice of a change of address for a covered account, the University receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account;

(2) A covered account is used in a manner that is not consistent with established patterns of activity on the account;

(3) A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors);

(4) Mail sent to the student, faculty, staff, or other constituent is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account;

(5) The University is notified that the student, faculty, staff, or other constituent is not receiving paper account statements;

(6) The University is notified of unauthorized charges or transactions in connection with a covered account; and

(7) The University receives notice from students, faculty, staff, or other constituents, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University;

D. Notice from Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the University. Examples of these Red Flags include the following:

The University receives notice from students, faculty, staff, or other constituents, a victim of identity theft, a law enforcement authority, or any other person that the University has opened a fraudulent account for a person engaged in identity theft.

4. Address Changes

For all Covered Accounts, the University will notify the student, faculty, staff, or other constituent that an address change has been made to their record by sending a notification to their University maintained email account. This notification will be processed within 72 hours of when the address change was made. The individual will be asked to confirm that the address change was authorized. If not authorized, the individual will be directed to notify the University for further investigation.

5. Responding to Red Flags

A. Any time a Red Flag, or a situation closely resembling a Red Flag, is detected, the University shall endeavor to respond rapidly, as follows:

(1): The Department responsible for the account shall conduct a preliminary investigation to determine whether the attempted transaction was authorized and whether departmental procedures were correctly followed.

(2) : If the attempted transaction was not authorized, or if it is discovered that a breach may have occurred, the Department responsible for the account shall quickly gather all related documentation, write a description of the situation, and present this information to the University's Vice President for Business and Finance, or his/her designee.

(3) : The University's Vice President for Business and Finance, or his/her designee, shall complete additional investigation to determine whether the attempted transaction was fraudulent or authentic.

B: If a transaction is determined to be fraudulent, appropriate actions shall be taken immediately. Actions may include:

(1) Canceling the transaction

(2) Notifying and cooperating with appropriate law enforcement;

(3) Determining the extent of liability of the University; and

(4) Notifying the student, faculty, staff, or other constituent that fraud has been attempted.

6. Periodic Updates to the Program

A: At periodic intervals as deemed necessary by the University, the Program shall be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current operational environment.

B: Periodic reviews will include an assessment of which accounts are covered by the Program.

C: As part of the review, changes in methods of identity theft, and changes in methods to detect, prevent, and mitigate identity theft shall be taken into consideration.

D: As part of the review, Red Flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate. The University shall incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the University has experienced;

(2) Methods of identity theft that the University has identified that reflect changes in identity theft risks;
(3) Applicable supervisory guidance.

E: As part of the review, the University shall determine whether to revise University Policies or procedures addressing identify theft issues.

7. Program Administration

A: Involvement of management

Operational responsibility for the Program, including but not limited to (i) the oversight, development, implementation, and administration of the Program, (ii) approval, with the concurrence of the Vice President for Legal Affairs, of needed changes to the Program, and (iii) implementation of needed changes to the Program, is delegated to the University's Vice President for Business and Finance, or his/her designee.

B: Employee training

(1): Training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by the University's Vice President of Business and Finance, or his/her designee, that the employee may come into contact with accounts or personally identifiable information that may present a risk of identity theft.

(2): Employees shall receive annual training in all elements of the Identity Theft Prevention Program.

(3) To ensure maximum effectiveness, employees shall continue to receive additional training as changes to the Program are made.

C: Oversight of service provider arrangements

(1): The University shall endeavor to provide that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

(2): A service provider that maintains its own identity theft prevention program, consistent with the guidance of the Red Flag Rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

(3): Any specific requirements should be specifically addressed in the appropriate contractual arrangements.

D: Annual Report

Staff of the University responsible for development, implementation, and administration of the Program shall report annually to the University's Vice President for Business and Finance and to the Audit Committee of the Board. Additional reporting for significant events will be made immediately to the University's Vice President for Business and Finance and will be presented at the next scheduled meeting of the Audit Committee. The report shall address material matters related to the Program and evaluate issues such as:

(1): The effectiveness of the policies and procedures of the University in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

(2): Service provider arrangements;

(3): Significant incidents involving identity theft and management's response; and

(4) : Recommendations for material changes to the Program.

8: Application of Other Laws and University Policies

This Program should be read and applied in conjunction with the Family Education Rights and Privacy Act ("FERPA"), the Gramm-Leach Bliley Act, and other applicable state and federal laws and University Policies.