Florida International University

Identity Theft Prevention Program

Effective beginning August 1, 2009

I. PROGRAM ADOPTION

Florida International University developed this Identity Theft Prevention 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. This Program was developed by a working group comprised of University representatives from areas potentially impacted by the Red Flags Rule, after consideration of the size and complexity of the University's operations, and the nature and scope of the University's activities. This Program is to be presented to the Finance and Audit Committee of the Florida International University Board of Trustees for approval and shall be implemented on or before August 1, 2009.

II. DEFINITIONS AND PROGRAM

A. Red Flags Rule Definitions Used in this Program

1. "Covered Account" is an account maintained by the University that involves or is designed to permit multiple payments or transactions such as a student financial aid loan, short-term loan account, emergency loan account, or student or staff debit card account. A Covered Account is also an account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the institution from identity theft, including financial, operational, compliance, reputation, or litigation risks.

2. "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 and student identification number.

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

4. "Program Administrator" is the individual designated with primary responsibility for oversight of the program. The President shall designate the University's Program Administrator. See Section VI below.

5. "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

B. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, Florida International University is required to establish an Identity Theft Prevention Program (hereafter "the Program") tailored to its size, complexity and nature of its operations. The Program must include reasonable policies and procedures to:

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 University students and staff and to the safety and soundness of the institution from Identity Theft.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the University 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. The University identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

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.

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. The photographic or physical description on the identification document or card is not consistent with the appearance of the applicant or person.

3. Other document with information that is not consistent with existing information on file.

4. Application that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the person provides (example: inconsistent birth dates).

2. Identifying information presented that is inconsistent with other sources of information (example: 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 (example: an invalid phone number or fictitious billing address).

5. Social security number presented that is the same as one given by another person.

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.

8. A person's identifying information is not consistent with the information that is on file.

D. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the person'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 person is repeatedly returned as undeliverable.

5. Notice to the University that a person 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.

8. Unauthorized access to, or use of student or staff account information.

E. Alerts from Others

Red Flags

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

IV. DETECTION OF RED FLAGS

A. Student Enrollment and Student and Staff Issuance of FIU One Card

In order to detect any of the Red Flags identified above associated with the enrollment of a student or with the opening of a student or staff Covered Account, University personnel will take the following steps to obtain and verify the identity of the person enrolling, or opening the account. These steps are also applicable when the student, staff member, or visiting faculty member requests an FIU One Card.

Detect

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification.

2. Verify the person's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

3. Place a "hold" on the FIU One Card as soon as the person calls the FIU One Card Office, provides identifying information, and notifies the Office that his or her card has been misplaced or stolen.

4. Require personal appearance at the University's Graham Center or Wolfe Center in order to issue a replacement card, following steps #1 and 2 above.

B. Existing Accounts Involving Students

In order to detect any of the Red Flags identified above for an existing Covered Account involving a student, University personnel will take the following steps to monitor transactions on an account:

Detect

1. Verify the person's identity if they request information (in person, via telephone, via facsimile, via e-mail).

2. Ensure that the person is authorized to receive the information that is requested.

3. Verify the validity of requests to change billing addresses by mail or e-mail and provide the person with a reasonable means of promptly reporting incorrect billing address changes.

4. Verify changes in banking information given for billing and payment purposes.

C. Consumer ("Credit") Report Requests involving Applicants for Employment, Current Employees and Volunteers for which Criminal Background Checks are Sought

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

1. Require written verification that the address provided by the applicant, employee or volunteer is accurate at the time the request for the credit report is made to the consumer reporting agency.

2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant, employee or volunteer for whom the

requested report was made and report to the consumer reporting agency an address that the University has reasonably confirmed is accurate.

V. PREVENTING AND MITIGATING IDENTITY THEFT

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:

A. Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft.

2. Contact the person for which a consumer 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 person 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").

9. Determine that no response is warranted under the particular circumstances.

B. Protect Student Identifying Information

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

1. Ensure that its Web site is secure or provide clear notice that the Web site is not secure.

2. 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.

3. Ensure that office computers with access to Covered Account information are password protected.

4. Avoid use of social security numbers as, under Florida law, the collection and use of social security numbers is only permitted when either specifically authorized by law or imperative for the performance of the University's duties and responsibilities. Please note that any department/unit that collects social security numbers from individuals must provide written notification to the individuals stating the purpose for such collection. For additional safeguards regarding the use and collection of social security numbers see Section V, Subsection C below.

5. Ensure computer virus protection is up-to-date.

6. Require and keep only the kinds of student identifying information that are necessary for University purposes.

C. Use and Collection of Social Security Numbers

Identity thieves covet social security numbers (SSNs) because they can be used as tools to perpetuate fraud against individuals by facilitating the acquisition of sensitive financial, medical, and familial information. As a result, and in accordance with Florida law requirements, the University will take the following steps in order to protect SSNs:

1. Departments or units of the University may not collect an individual's social security number unless:

    a. They are specifically authorized by law to do so; or
    b. It is imperative for the performance of that department or unit's duties and responsibilities as prescribed by law; and
    c. They provide a written statement to the individuals whose SSNs they are collecting indicating the purpose for the collection and whether such collection is authorized or mandatory under federal or state law.

2. The department or unit shall identify in writing the specific federal or state law governing the collection, use, or release of SSNs for each purpose for which it is collecting the SSN, including any authorized exceptions that apply to such collection, use, or release.

3. SSNs collected by the department or unit may not be used by the department or unit for any purpose other than the purpose provided in the written statement.

4. Departments or units that collect or maintain SSNs must abide by the requirements of the University Data Stewardship Procedure.

VI. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Prevention Committee ("Committee") for the University. The Committee is headed by a Program Administrator who may be the President of the University or his or her designee. Two or more other individuals designated by the President of the University or the Program Administrator comprise the remainder of the Committee membership. The 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

University staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. University staff shall be trained, as necessary, to effectively implement the Program. University employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, University staff responsible for the development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this 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 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 mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place.

2. Require, by contract, that service providers review the University's Program and report any Red Flags to the University employee with primary oversight of the service provider relationship or the Program Administrator.

D. Program Updates

The Committee will periodically review and update this Program to reflect changes in risks to students, faculty and staff, and the soundness of the University from Identity Theft. In doing so, the Committee will consider the University's 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. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.

Florida International University Identity Theft Prevention Program. Effective Date: August 1, 2009; Revision Dates: June 4, 2010, June 5, 2012.