

**Florida Gulf Coast University Board of Trustees
April 21, 2009**

SUBJECT: Identity Theft Prevention Program

PROPOSED BOARD ACTION

Approve an Identity Theft Prevention Program and designation of authority for future handling.

BACKGROUND INFORMATION

Recently, the Federal Trade Commission (“FTC”) issued a regulation known as the “Red Flags Rule,” 16 C.F.R. Part 681 (the “Rule”), intended to reduce the risk of identity theft. The Rule requires “financial institutions” and “creditors” to develop and implement an identity theft prevention program for new and existing accounts (the “Program”). The FTC goes on to state that “[w]here non-profit and governmental entities defer payment for goods or services, they, too, are to be considered creditors.” Based on the University’s actions as a creditor (i.e. participation in various student loan programs, offering payment plans related to tuition and housing, etc.), this federal regulation would apply to it. Covered entities under the Rule must adopt and implement a written Identity Theft Prevention Program by May 1, 2009.

The Rule requires that the approval of the **initial** written Identity Theft Prevention Program be obtained from the appropriate Board or Board Committee. This Agenda item seeks the approval of the Board of Trustees of the Program and the designation of the President oversee the development, implementation and administration of the program with the understanding that the President may further designate this function as appropriate.

Supporting Documentation Included: Summary of Federal Red Flags Rule, Student Financial Services Identity Theft Policy

Prepared by: Assistant Vice President for Administrative Services and Finance/
Controller Linda Bachelor

Legal Review by: General Counsel Vee Leonard (March 30, 2009)

Submitted by: Vice President for Administrative Services and Finance Joe Shepard

Florida Gulf Coast University

Identity Theft Prevention Program

Effective beginning _____, 2009

I. PROGRAM ADOPTION

Florida Gulf Coast University ("University") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule 16CFR681. This Program was developed in consideration of the size and complexity of the University's operations and account systems, as well as the nature and scope of the University's activities.

DEFINITIONS AND PROGRAM

A. Red Flags Rule Definitions

- *Identity Theft* - A fraud committed or attempted, using the identifying information of another person without authority.
- *Red Flag* - A pattern, practice, or specific activity that indicates the possible existence of identity theft.
- *Covered Account* – Account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. A covered account is also an account for which there is a foreseeable risk of identity theft.
- *Program Administrator* - The individual designated with primary responsibility for oversight of the program. See Section VI below.
- *Identifying information* - 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.

II. 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 following items are illustrative examples of Red Flags:

A. Notifications and Warnings from Background or Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a background or 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. 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.
4. Application for service 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 student provides (example: inconsistent birth dates).
2. Identify information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application).
3. Identify 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 (such as an invalid phone number or fictitious billing address).
5. Social security number presented that is the same as one given by another student.
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 for the student.

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 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 the University that a student 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 account information.

E. Alerts from Others

Red Flag

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

III. DETECTING RED FLAG

A. Student Enrollment

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

Detect

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification.
2. Verify the student's identity at 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, University personnel will take the following steps to monitor transactions on an account:

Detect

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

C. Background and 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, University personnel will take the following steps to assist in identifying address discrepancies:

Detect

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the background or credit report is made.
2. In the event that notice of an address discrepancy is received, verify that the background or 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 University has reasonably confirmed is accurate.

IV. PREVENTING AND MITIGATING IDENTITY THEFT

In the event University personnel detect any Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft.
2. Contact the student or applicant.
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 if applicable.
6. Notify the Program Administrator for determination of the appropriate step(s) to take.
7. Program Administrator will notify University Campus Police if appropriate.
8. Program Administrator will file or assist in filing a University Campus Police Report.
9. Program Administrator will determine that no response is warranted under the particular circumstances.

V. 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 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 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.

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

VI. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft 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 appointee/designee. Two or more other individuals appointed 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 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 Program Administrator or the University employee with primary oversight of the service provider relationship.

D. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to

the Committee who developed this Program and to those employees who 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 Program Administrator shall inform the Committee and those employees who need to know the information of those documents or specific practices which should be maintained in a confidential manner.

E. Program Updates

The Committee will periodically review and update this Program to reflect changes in risks to students 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.