3-1014 Identity Theft

(1) Pursuant to the Federal Trade Commission's Red Flags Rule (implemented by 15 U.S.C. 1681m), this Regulation will help College staff to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or existing accounts through the Identity Theft Prevention Program (Program). An identity can be stolen with nothing more than a stolen string of numbers and malicious intent. With a few pieces of personal identifying information, an identity thief can easily secure an account in someone else's name. This information can be obtained from a variety of sources, including stolen mail, computer hacking, fraudulent address changes, and other schemes.

(2) Definitions

(a) Identity Theft - A fraud committed or attempted using the personal identifying information of another person without authority.

(b) Red Flag - A pattern, practice, or specific activity that indicates the possible existence of identity theft.

(c) Covered account – Account used mostly for personal, family, or household purposes, and that involves or is designed to permit multiple payments or transactions. A covered account is also an account for which there is a foreseeable risk of identity theft.

(d) Program Administrator - The individual designated with primary responsibility for oversight of the program. See Section (8) below.

(e) 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, credit card number, credit card expiration date, pay check, pay check stub, medical information.

(3) Fulfilling Requirements of the Red Flags Rule. Under the Red Flags Rule, the College is required to establish an "Identity Theft Prevention Program" tailored to the size, complexity, and the nature of College operations. The Program must contain reasonable policies and procedures 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;

(d) 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;

(4) Program Administration. The College must obtain approval of the initial written program by the governing body or an appropriate committee of the governing body. Annually, the designated administrator of the College's Program is to report to the governing body on the effectiveness of the program and compliance with the regulatory requirements.

(5) Identifying Red Flags. In order to identify relevant Red Flags, the College 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 College has identified the following Red Flags in each of the five listed categories below.

(a) Notification, Alerts, and Warnings from Credit Reporting Agencies or Service Providers:

1. Report of fraud or credit alert 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) Presentation of 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 appearance of the person presenting the document for identification;

3. Other information on the identification document is not consistent with existing student information on account with New College; and

4. An application for service that appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

(c) Presentation of Suspicious Personal Identifying Information:

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

2. Identifying information presented that is inconsistent with other sources of information used by or on the College's records (ie. 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 (ie. 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; 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 a Covered Account:

1. Change of address for an account followed by a request to change the person's name, or for a replacement ID Card;

2. Payments stop on an otherwise consistently up-to-date account;

3. Account used in a way that is not consistent with prior use on the account;

4. Mail sent to the person is repeatedly returned as undeliverable, although transactions continue to be conducted in connection with the account;

5. Suspicious address changes are submitted;

6. Notice to the College that a person is not receiving mail sent by the College;

7. Notice to the College that an account has unauthorized activity;

8. Breach in the College's computer system security;

9. Unauthorized access to or use of student account information; and

10. An account that has been inactive for a reasonably lengthy period of time is used.

(e) Alerts from Others – Persons, Victims, Law Enforcement Authorities: Notice to the College from an Identity Theft victim, law enforcement, or other person that the College has opened or is maintaining a fraudulent account for a person engaged in identity theft.

(6) Detecting Red Flags

(a) Student Enrollment. In order to detect any of the Red Flags identified above associated with the enrollment of a student, College 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 time of issuance of student identification card (review of non-expired driver's license or other government-issued photo identification). The identification should be scrutinized to verify that it has not been altered or forged.

(b) Existing Accounts. In order to detect any of the Red Flags identified above for an existing Covered Account, College 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) by ensuring that the information given is consistent with other information on file at the College;

2. Verify that the picture on the identification provided matches the appearance of the person presenting the identification (includes accepting in-person address changes);

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

4. Verify that request for information updates have not been altered or forged or that the paperwork gives the appearance of having been destroyed and reassembled;

5. Notify the Program Administrator immediately if the College is notified by a victim of identity theft, a law enforcement agency, or any other person that it has opened, discovered, or manipulated a fraudulent account for a person engaged in identity theft; and

6. Ensure that persons who call are not given information on an account if they cannot provide the NCF ID number and name. Be cautious about callers who attempt to get financial information without providing any substantive knowledge about the account.

(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, College 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 background or credit report is made; and

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 College has reasonably confirmed is accurate.

(7) Preventing and Mitigating Identity Theft. In the event College 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) Prevention and Mitigation Protocols

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. Refuse to 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. Program Administrator will notify law enforcement, if appropriate.
8. Program Administrator will file or assist in filing a police report.
9. Program Administrator will determine that no response is warranted under the particular circumstances and will communicate that decision to the appropriate party.

(b) Once a potentially fraudulent activity is detected, an employee must act quickly as a rapid and appropriate response can protect persons and the College from damages and loss. The employee should gather all related documents and write a description of the situation, present the information to the designated authority for determination if fraud was committed.

(c) The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authenticated. If fraudulent, the transaction will be cancelled, law enforcement will be notified and cooperated with, the extent of liability to the College will be determined and notification to the affected person will be made of the fraudulent activity.

(d) Protecting Student Identifying Information. In order to further prevent the likelihood of identity theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Make every effort to secure student information during times when their desk/office is unattended.
2. Do not leave documents or computer terminals with sensitive information (names, ID#’s, addresses, etc.) in plain view.
3. Ensure that its website is secure or provide clear notice that the website is not secure.

4. 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.

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

6. Ensure the alarm, where available, is set upon leaving the office for the day.

7. Avoid use of social security numbers.

8. Ensure computer virus protection is up to date.

9. Require and keep only the kinds of student information that are necessary for College purposes.

(8) Program Administration

(a) Oversight. Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee. The Committee, appointed by the Vice President for Finance and Administration, is comprised of individuals that routinely deal with employee and student records and business transactions and is headed by the Program Administrator, also appointed by the Vice President. The Program Administrator is responsible for ensuring appropriate training of College 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

1. College 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. College staff shall be trained, as necessary, to effectively implement the Program. College employees are expected to notify the Program Administrator once they become aware of an incident of identity theft or of the College's failure to comply with this Program.

2. At least annually or as otherwise requested by the President or his/her designee, the Program Administrator shall report to the President or his/her designee 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 College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College 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 College's Program, agree to comply with it and report any Red Flags to the Program Administrator or the College 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 College employees or the public. The Program Administrator shall inform 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 College from identity theft. In doing so, the Committee will consider the College's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the College'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 Program will be updated.

Authority: Article IX, Sec. 7, Fla. Constitution; 15 U.S.C. 1681m; Fla. Board of Governors Regulation 1.001

History: Adopted 09-10-11; Revised 02-26-17 (technical amendment)