


PROCEDURE

Subject	Identity Theft Prevention	Number: 1.07.02
Source	Vice President, Finance and Administrative Services	Reference (Rule #) 6HX14-1.07
President's Approval/Date:	 12/21/2017	

POLICY: The College has established a Procedure for the assessment, detection, mitigation and implementation of an identity theft “Red Flag” Program. The procedure is consistent with Florida Statutes and State Board of Education Rules and the *Fair and Accurate Credit Transactions Act* (FACT Act) of 2003(the “Red Flags Rule”).

PURPOSE: This procedure is intended to identify third party arrangements and “red flags” involving College activities that will:

- Alert College employees when new or existing billing accounts are opened using false information;
- Protect against the establishment of false student or other customer accounts;
- Provide methods to ensure that existing accounts are not opened using false information;
- Provide protection and safekeeping of covered account information; and
- Provide measures to respond to such events.

Within the context of this procedure, “Red Flag” means a pattern, practice, or specific activity that indicates possible identity theft.

SCOPE: This procedure applies to “covered accounts,” “creditors,” credit report usage and third party arrangements within the meaning of the Red Flags Rule.

1. General Guidelines and Definitions

- A. “Covered accounts” under the Red Flags Rule are consumer accounts that involve multiple payments or transactions, such as a loan that is billed or payable monthly. The Red Flags Rule and related FTC guidance indicate that covered accounts include certain types of arrangements in which an individual establishes a “continuing relationship” with the institution, including billing for previous services rendered. Certain payment arrangements, such as payment of tuition in full at the beginning of each term, either by the student’s family or through a third-party student loan provider (see also Section 3 “Oversight of Third Party), do not meet the “continuing relationship” standard in the “covered account”

definition. Any type of account or payment that involves multiple transactions or multiple payments in arrears, however, likely is a covered account.

- B. A “creditor” under the Red Flags Rule includes any person who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month. The College is considered a “creditor” under the Red Flags Rule because it offers student deferments, and bills for tuition and fees, and other goods and services (space rental, performances, etc.). It also offers institutional loans to students and staff in cases of extreme emergency.
- C. The procedure also applies when the College uses “consumer reports” to conduct credit or background checks.

2. Responsibilities and Delegation of Authority

The purpose of this Program is to identify potential red flags that will alert College employees when accounts are opened or changed using false information, to protect against the establishment of false accounts, to establish methods to ensure existing accounts were not opened using false information, and to define measures to respond to such events.

The Director, Institutional Compliance is responsible for the oversight of the Program as well as the implementation, administration and annual review of the program.

3. Internal Risk Assessment

SCF has conducted an internal risk assessment to evaluate how at-risk its procedures are for the creation of fraudulent accounts and to evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts are opened and the methods used to access account information. This risk assessment also reviewed third party service arrangements and situations where a credit report is used as part of the hiring process. Using this information, the College identified areas of highest risk for review and compliance:

- New accounts opened in person
- New accounts opened via web
- Account information accessed in person and any request for account modification
- Account information accessed via telephone and any request for account modification
- Account information accessed via web and any request for account modification
- Delinquent accounts placed with an outside collection agency
- Employee’s credit report “pulled” as part of the hiring process

Oversight of Third Party Service Providers:

The College will, as part of its contracts with third party service providers (e.g., collection agencies and student refund partner), require that these providers have policies, procedures and programs that comply with the “Red Flags” Rule. Further, service providers must notify the

College of any security incidents they experience, even if the incidents may not have led to an actual compromise of the College's data.

4. Identifying Red Flags

The College adopts the following "red flags" to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- Fraud or active duty alerts included with consumer reports
- Notice of credit freeze provided by consumer reporting agency
- Notice of address discrepancy provided by consumer reporting agency
- Inconsistent activity patterns indicated by consumer report such as:
 - Recent and significant increase in volume of inquiries
 - Accounts placed on hold for financial delinquency
- Identification documents appear to be altered
- Photo and physical description do not match appearance of applicant
- Other information is inconsistent with information provided by applicant
- Other information provided by applicant is inconsistent with information on file
- Application appears altered or destroyed and reassembled
- Personal information provided by applicant does not match other sources of information (e.g. credit reports, social security number not issued or listed as deceased)
- Lack of correlation between the social security number's range and date of birth
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of prior fraudulent activity)
- Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- Social security number, address, or telephone number is the same as that of another applicant at College
- Applicant fails to provide all information requested
- Personal information provided is inconsistent with information on file for applicant
- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- Identity theft is reported or discovered

5. Response to Attempted/Suspected Fraudulent Use of Identity

Any employee that may suspect or detect a red flag will implement the following response as applicable.

Internal Notification

Any College employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customer's identity must notify his immediate supervisor who will then notify the Director, Institutional Compliance.

External Notification

Affected Individual – The College will notify the affected individual(s), if possible, of any actual identity theft. The following information will be included in the notice:

- General information about the incident;
- The type of identifying information involved;
- The College e-mail address and telephone number that the affected individual can call for further information and assistance;
- The local Law Enforcement Agency with proper jurisdiction;
- The Federal Trade Commission (FTC) Telephone Number: 877-438-4338 and the FTC ID Theft website: <http://www.consumer.gov/idtheft>
- Advise affected individual to place fraud alerts on their credit reports by contacting the Credit Reporting Agencies:
 - Equifax: (800) 525-6285 or <http://www.equifax.com>
 - Experian: (800) 397-3742 or <http://www.experian.com>
 - TransUnion: (800) 916-8800 or <http://www.transunion.com>

Method of Contact:

- Written notice: certified mail to last known “good address” if identity theft involves alteration of correct address of record.
- Telephone: provided the contact is made directly with the verified, affected person and appropriately documented.
- E-mail notice to students’ College e-mail address

Local Law Enforcement:

In all cases, the College will notify Public Safety and Local Law Enforcement having proper jurisdiction of any attempted or actual identity theft.

6. Employee Training

The College will implement periodic training to emphasize the importance of meaningful data security practices and to create a “culture of security.” The College acknowledges that a well-trained workforce is the best defense against identity theft and data breaches.

- Periodically explain the Program rules & procedures to relevant staff, and train them to spot security vulnerabilities, and update them about new risks and vulnerabilities.
- Inform employees of College “Identity Theft Prevention” Procedure 1.07.02
- Inform employees of College’s Code of Ethical Behavior Rule (6HX-142.55) and Procedure (2.55.01) and Fraud Reporting Procedure (2.55.02).
- Inform employees of FERPA Guidelines

7. Identity Theft Prevention Procedure Review and Approval

The Director, Institutional Compliance will review the procedure at least annually, or after each and every verified attempt at identity theft. A report will be prepared annually and submitted to the Vice President, Finance and Administrative Service to include matters related to the procedure, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the procedure, if any.

8. Violation of the College's security policies is grounds for discipline, up to, and including, dismissal.