FLORENCE-DARLINGTON TECHNICAL COLLEGE

PROCEDURE

Number:	71-13
Title:	Identity Theft Red Flag Identification and Prevention Plan
Responsibility:	Vice President of Finance and Administration
Original Approval Date:	04/28/2009
Last Cabinet Review:	04/29/2025
Last Revision:	04/07/2025

Reference (Policy and/or Procedure)

SBTCE:

FDTC: Policy# 70-23 Identity Theft Red Flag Identification and Prevention Policy

Other:

Procedure Description

Florence-Darlington Technical College recognizes that identity theft is a continuing and growing issue that can result in harm to its students and employees as well as the institution. Pursuant to the Federal Trade Commission's (FTC) Red Flag Rules, which implements the Fair and Accurate Credit Transaction Act (the FACT Act) of 2003, FDTC has enacted the Red Flag Policy to protect the College, its students and employees from Identity Theft and the related damages that may result from Identity Theft. This policy establishes procedures to:

1. Identify Covered Accounts;
2. Identify the Red Flags relevant to FDTC;
3. Detect Red Flags;
4. Respond appropriately to detected Red Flags;
5. Train responsible staff;
6. Update the program and perform risk assessment.

Scope: This policy applies to all College departments that collect and maintain personal information.

Definitions:

Account- a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes. It includes a) an extension of credit, such as the purchase of property or services involving a deferred payment, and b) a deposit account.

Covered Account- a) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and b) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from Identity Theft, including financial, operational, compliance, reputation, or litigation risks.

Identity Theft - fraud committed or attempted using the identifying information of another person without their knowledge or permission.

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

Service Provider - a person that provides a service directly to the financial institution or creditor.

PROCEDURE

Identify Covered Accounts

Each department will identify the Red Flags associated with their Covered Accounts taking into consideration the types of accounts offered and maintained, the methods provided to open and access accounts, and previous experiences with identity theft.

The following are examples of Red Flags that can be potential indicators of Identity Theft:

• Alerts, notifications, or other warnings received from consumer reporting agencies or Service Providers;

• Notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;

• Notice from customers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible identity;

• The presentation of suspicious documents;

• The presentation of suspicious personally identifying information, such as a suspicious address change;

• Personal identifying information provided is inconsistent when compared against external information sources used by the College;

• The unusual use of, or other suspicious activity related to a covered account;

Photograph or physical description of student is not consistent with the appearance of the student providing identification;

• Requests to mail information to addresses not on file with the college;

• Documents presented for the purpose of personal identification are incomplete or appear to have been altered, forged or inauthentic;

• Questions are not consistent with basic, general knowledge (lack of knowledge of basic information such as familiarity with college policy, campus attended, self-service, etc);

• Person is very vague about contact information or refused to provide it.

This is not an exhaustive list.

Detect Red Flags

Departments should develop and implement procedures to detect Red Flags associated with opening new or accessing existing Covered Accounts.

• Monitor account transactions for possible Red Flags. Require certain identifying information such as name, date of birth, residential or business address, driver license, or another photo identification.

• Require multiple factors of identification before conducting any transaction over the phone that relates to a Covered Account.

• Require authorization on file before releasing personal information to a third party;

• Require that online transactions come through a secure, password protected portal in accordance with the Standards for Securing Regulated Private Data policy.

• Thoroughly follow up on each billing inquiry, especially inquiries regarding services not received and/or billing errors.

• Verify the validity of a change of address request on an existing account and provide the customer with a means to promptly report an incorrect address.

If Red Flags are detected, one or more of the following steps may be taken:

• monitor the Covered Accounts for evidence of identity theft;

• request additional documentation to validate identity;

• contact the consumer and verify if the activity is fraudulent;

• where appropriate, disable access or change passwords, security codes, or other security devices;

• close the Covered Account, and if needed reopen with a new account number;

• refuse to open a new Covered Account for the customer;

• notify the department's supervisor;

• determine if law enforcement should be notified

• determine that no response is warranted under the particular circumstances.

Any department who is involved in a case of Identity Theft should maintain a log of the incident(s). The log should contain the date, description of the incident, what Red Flags were involved, and what actions were taken to avoid a similar situation from occurring in the future.

Train Responsible Staff

Each department having Covered Accounts will compile a list of their staff that are responsible for performing the day-to-day application of the Red Flags procedures to a specific Covered Account.

Responsible staff should receive training through their Department Heads and Data Custodians on Red Flags Identity Theft prevention and their department's Red Flag internal procedures.

SAFEGUARDS

Appropriate safeguards for the college are listed below:

1) Request a picture identification.

2) Inquire into address and other information discrepancies inconsistent with a picture identification.

3) Reading notifications from law enforcement or other valid agencies involving local identity theft that may apply to the College.

4) Notification that students or employees submitting false information may be subject to dismissal from the College.

5) During the hiring process of employees, requiring two forms of identification.

6) During the student admission/registration process, requiring proof of residency.

7) Appropriate procedures are in place to safeguard any printed or written materials in areas where personal information is accumulated.

8) Ensure our Third-party Loan Servicer has an Identity Theft Prevention Program in place that is in compliance with the Red Flags guidelines.

Program Update and Risk Assessment

The department head, Data Custodian, or their designee of a Covered Account shall conduct an annual risk assessment for their designated area. The assessment should consider prior experience with Identity Theft; changes in the methods identifying Identity Theft; changes in the detection, prevention, and mitigation of

Identity Theft; the Covered Accounts offered and administered by the College; and the potential Red Flags that may arise with respect to the Covered Accounts in their designated area. The assessment should also consider any changes in risks to students and individual account holders and to the safety and soundness of the College from Identity Theft. These documented assessments must be submitted to the College's VP of Finance and Administration (VPFA) by March 31st each year. In collaboration with the VP of Information Technology, these assessments will undergo review, remediation, and then be reported to the VPFA.