TITLE: IDENTITY THEFT PREVENTION (RED FLAGS) PROGRAM

- Initial Action: 5-27-2010
- Board Resolution: 25-034
- Last Revised:
  - Policy: 5-5-2025
  - Procedure: 5-5-2025
  - Last Reviewed: 5-5-2025
- Effective: 6-1-2010
- Next Review: June 2028

Responsibility: Chief Information Officer and
Vice President of Finance and Administration

POLICY

Cecil College's Identity Theft Prevention Program (Red Flags) applies to all Authorized Users accessing the College's Technology Resources regardless of their capacity, role or function including, but not limited to, students, faculty, staff, third party contractors, visitors, guests, consultants, and employees fulfilling temporary or part-time roles. The College has adopted this Identity Theft Prevention Program ("Program") to detect, prevent, and mitigate Identify Theft in connection with the opening of a Covered Account or any existing Covered Account. The Program is intended to comply with the Federal Trade Commission's (FTC) Red Flags Rules and the Fair and Accurate Credit Transactions Act of 2003 (FACTA), to the extent they apply to the College. The Program is further intended to help protect students, faculty, staff, and other constituents and the College from damages related to the fraudulent activity of Identity Theft.

Covered Accounts

Cecil College has designed this Program to protect certain types of student and employee accounts maintained by the College. Every new and existing account that meets the following criteria is a Covered Account under this policy.

1. Any account that the College offers to students or employees that involves or is designed to permit multiple payments or transactions; or
2. Any other student or employee account offered or maintained by the College for which there is a reasonably foreseeable risk to students and/or employees or to the safety and soundness of the College from identity theft, including financial, operational, compliance, reputation or litigation risks.

PROCEDURES

A. Identity Theft Program

In accordance with the Red Flags Rule, the College's Identity Theft Prevention Program includes reasonable procedures to:

- Identify relevant Red Flags for new and existing Covered Accounts and incorporate them into the Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
- Ensure the Program is updated periodically to reflect changes in risks or to the safety and soundness of Covered Accounts and the students and employees who use them.

B. Identification of Red Flags

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 identifies the following Red Flags in each of the listed categories:

1. Notifications and Warnings from Credit Reporting Agencies
    - Report of fraud accompanying a credit report;
    - Notice or report from a credit agency of a credit freeze on an applicant;
    - Notice or report from a credit agency of an active-duty alert for an applicant;
    - Receipt of a notice of address discrepancy in response to a credit report request; and
    - Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity
2. Suspicious Documents
    - Identification document or card that appears to be forged, altered, destroyed, or inauthentic;
    - Identification document or card on which a person's photo or physical description is not consistent with the person presenting the document;
    - Document with information that is inconsistent with existing, readily available information provided by that person or other information provided by the person; and
    - An application or other request relating to a covered account appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled
3. Suspicious Personal Identifying Information (PII)
    - Information that is inconsistent with other information the individual provides (*i.e.*, inconsistent birth dates, lack or correlation between Social Security Number and date of birth);
    - Information that is inconsistent with other sources of information (*i.e.*, an address not matching an address on a loan application);

- Information that is the same as information shown on other applications that were found to be fraudulent or that is identical to another person's information in the College's systems;
- Information that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

4. Suspicious Account Activity or Unusual Use of Account
   - Change of address for an account followed by a request to change a student's name;
   - Requests related to loan disbursements or transfers from an email address other than the individual's official College email address;
   - Change in bank account information for electronic transfers;
   - Payments stop on an otherwise consistently up-to-date account;
   - Account used in a way that is inconsistent with prior use;
   - Mail sent to an individual that is consistently returned as undeliverable although transactions continue to be conducted with the individual;
   - Notice to the College (from the individual) that the individual is not receiving mail sent by the College or scheduled loan disbursement or transfer of funds;
   - Notice to the College that an account has unauthorized activity;
   - Suspicious activity in connection with an individual's online account
   - A breach in the College's information technology security system; and
   - Any unauthorized access to or use of student or employee account information

5. Alerts from Other Red Flags
   - Notice to the College from a student, 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.

C. Detecting Red Flags

1. New Accounts: In order to detect any of the Red Flags identified above associated with the opening of a new Covered Account, College personnel will take the following steps to obtain and verify the identity of the person opening the account: (a) require certain identifying information such as name, date of birth, academic records, home address or other identification; (b) verify the individual's identity at time of issuance of identification cards (review of driver's license or other government-issued photo identification); and (c) independently contact the affected individual if appropriate.

2. 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: (a) verify the identification of students if they request information (in person, via telephone, via email); (b) 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; and (c) verify changes in banking information given for billing and payment purposes.

3. 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 assist in identifying address discrepancies by: (a) requiring written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and (b) in the event that notice of an address discrepancy is received, verifying that the credit report pertains to the applicant for whom the requested report was made and reporting to the consumer reporting agency an address for the applicant that the College has reasonably confirmed is accurate.

D. Preventing and Mitigating Identify Theft

All potentially fraudulent activity must be reported by an employee to their supervisor and to the Program Administrator (see Section E below), who will work with relevant personnel to gather all related documentation and determine whether the attempted transaction was fraudulent or authentic and will respond appropriately. If it is determined by the Program Administrator that the attempted transaction was fraudulent, appropriate responses may include, but are not limited to:

- Monitoring a covered account for evidence of identity theft
- Terminating a transaction
- Contacting the customer
- Changing passwords, security codes, or other security devices that permit access to a Covered Account
- Not opening a Covered Account; closing an existing Covered Account
- Notifying and cooperating with appropriate law enforcement, and/or
- Determining that no response is warranted under the circumstances

E. Program Administration

Oversight: Responsibility for developing, implementing and updating this Program lies with the Chief Information Officer and the Vice President for Finance and Administration who have been designated as the Program Administrators. The Program Administrators will be 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.

Staff Training and Reports: College employees responsible for implementing the Program will be trained by a supervisor or under the direction of the Program Administrators in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. Appropriate College employees will be trained, as necessary, to effectively implement the Program. College employees are also expected to notify their supervisor and the Program Administrators once they become aware of an incident of Identity Theft or of the College's failure to comply with this Program. At least annually or as otherwise requested by a Program Administrator, College employees responsible for the development, implementation, and administration of the Program will report to the Program Administrator on compliance with this Program. The report shall 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.

Service Provider Arrangements: In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, it will require, by contract that the service provider have appropriate policies and procedures in place to detect Red Flags and contractually agree to report Red Flags to a Program Administrator or the College employee with primary oversight of the service provider relationship.

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 those employees with a need to know them. Any documents that may have been produced or are produced 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 employees or the public. The Program Administrators shall inform those employees with a need to know the information of those documents or specific practices which shall be maintained in a confidential manner.

Program Updates: The Program Administrators will periodically review and update this Program to reflect changes in risks to students and employees and the soundness of the College from Identity Theft. In doing so, the Program Administrators 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 Administrators will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrators will update the Program.

DEFINITIONS

Account – a continuing relationship established by a person with the College to obtain a product or service for personal, household, or business purposes, including the extension of credit or deferring payment.

Authorized Users - a person who is authorized to access or make transactions on a "covered account"

Identity Theft – fraud committed using the identifying information of another person.

Red Flags – a pattern, practice, or specific activity that indicates the possible existence of identity theft.