SUNY ECC ERIE COMMUNITY COLLEGE POLICY	NUMBER VI-A-21	Administration And Finance
APPROVED 10/09	SUBJECT: Red Flag Policy	

Purpose - The purpose of this policy is to establish an Identity Theft Prevention Program (Program) designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. Identify and define relevant "covered accounts";
2. Identify relevant patterns, practices, and forms of activity within those accounts that are "red flags" signaling possible identity theft;
3. Detect red flags incorporated into the Program;
4. Respond appropriately to any red flags that are detected in order to prevent and mitigate identity theft; and
5. Administer the Program in a manner that ensures proper staff training, implementation, oversight and updating.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Background - The Federal Trade Commission (FTC), under the authority granted by the fair and Accurate Credit Transaction Act of 2003 (FACTA), has issued a Red Flags Rule (16 CFR 681.2) requiring that financial institutions and creditors develop Identity Theft Prevention Programs aimed at recognizing and preventing activity related to identity theft. Erie Community College (ECC), and other institutions offering payment plans to students, come within the definition of creditors and, therefore, must adopt a policy and develop an Identity Theft Prevention Program as necessary.

Scope - This policy and the Identity Theft Prevention Program applies to all College employees, contractors and consultants.

Definitions - Account: A relationship established with an institution by a student, employee, parent, or other person to obtain educational, medical, or financial services.

Covered Account: The Red Flags Regulations define the term "covered account" to mean (1) "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..." and (2) "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."
For the purposes of the College's Identity Theft Program, the term "covered account" is extended to include any College account or database (financial or otherwise) for which the College believes there is a reasonably foreseeable risk to the College, its students, faculty, staff and vendors from identity theft.

Credit: "Credit" means the right granted by a creditor to a debtor to defer payment of a debt or to incur debts and defer its payment.

Creditor: "Creditor" means any person or institution who regularly extends, renews, or continues credit; any person or institution who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew or continue credit.

Responsible Staff: "Responsible Staff" means the personnel, based on title, who regularly work with Covered Accounts and are responsible for performing the day to day application of the Program to a specific Covered Account by detecting and responding to Red Flags.

Red Flag: "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Response: "Response" means the action taken by Responsible Staff member(s) upon the detection of any Red Flag to prevent and mitigate identity theft.

Service Provider: "Service Provider" means any contractor of the College engaged to perform an activity in connection with a Covered Account.

Identity Theft: "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

Transaction: "Transaction" means any exchange of personal identification information.

Identification & Detection of Red Flags - A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. The following Red Flags are potential indicators or warning signs of potential or actual identity theft or similar fraud. Any time a Red Flag, or a situation resembling a Red Flag, is apparent, it should be investigated for verification. The examples below are meant to be illustrative and not all inclusive. Any time an employee suspects a fraud involving personal information about an individual or individuals, the employee should assume that this Identity Theft Program applies and follow the protocols established by his/her office for investigating, reporting and mitigating identity theft. The Program identifies the following Red Flags:

1. Suspicious Documents
   a. Documents provided for identification purposes appear to have been altered or forged.
   b. The photograph or physical description on the identification is not consistent with the appearance of the individual presenting the identification.
   c. Other information on the identification is not consistent with information provided by the person attempting open a covered account or retrieve information from an existing covered account.
   d. Other information on the identification is not consistent with readily accessible information that is on file with the College.
   e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
2. Suspicious Personal Identifying Information
   a. Personal identifying information provided is inconsistent when compared against external sources used by the College.
   b. Personal identifying information provided by the individual is not consistent with other personal identifying information provided by the individual.
   c. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third party sources used by the College.
   d. The social security number provided is the same as that submitted by other persons applying to the College.
   e. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons applying to the College.
   f. The person opening a Covered Account fails to provide all required personal identifying information on an application or in response to a notification that the application is incomplete.
   g. Personal identifying information provided is not consistent with personal identifying information that is on file with the College.
   h. The person opening a Covered Account cannot provide authenticating information beyond that which generally would be available from a wallet.
3. Suspicious Account Activity or Unusual Use of Account
   a. The College is notified of unauthorized charges or transactions in connection with a student's Covered Account.
   b. Mail sent to the student is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the student's Covered Account.
4. Alerts from Others
   a. The College is notified by a student, a victim of identity theft, a law enforcement authority, or any other person that it has had a potentially fraudulent account opened by a person engaged in identity theft.

Appropriately Responding to Detected Red Flags - Once potentially fraudulent activity is detected, an employee must act quickly, as a rapid appropriate response can protect customers and the College from the effects of identity theft. The

employee should inform their supervisor as soon as possible that they have detected an actual or potential Red Flag, or have identified a similar area of concern related to identity theft. The supervisor should conduct any necessary inquiry to determine the validity of the Red Flag.
If it is determined that a situation of identity theft has occurred, the supervisor should immediately contact the Chief Administrative & Financial Officer's Office to inform them of the matter so the matter is properly documented as part of the monitoring portion of the Program.
Additionally, if the Red Flag indicates that a fraudulent transaction has occurred, the supervisor should ensure that appropriate actions to mitigate the effects of the transaction are taken immediately. Appropriate actions will be dependent on the type of Red Flag identified, type of transaction, relationship with the victim of the fraud, availability of contact information for the victim of the fraud, and numerous other factors. However, by way of example, appropriate actions may include, but are not limited to:

1. Canceling the transaction;
2. Not opening the new account or closing the account in question;
3. Notifying and cooperating with law enforcement;
4. Notifying the Office of the Attorney General, and Senior Administration of the College;
5. Notifying the actual student that fraud has been attempted or that it has occurred;
6. Changing any passwords or other security features that permit access to relevant accounts and/or databases;
7. Continuing to monitor the account or database for evidence of identity theft;
8. Alternatively, it may be determined that no response is warranted after the appropriate evaluation and consideration of the particular circumstances.

In all situations where it is determined that a Red Flag has been positively identified, the office responsible for the account shall document what occurred, describe its review of the matter and any specific actions taken to mitigate the impact of the effects of the actual or potential identity theft discovered. Such documentation shall also include a description of any additional actions the office believes are systematically necessary within their office (such as updating policies and procedures) in response to the identified Red Flag and to handle or prevent similar situations in the future.

Training - Staff training is required for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with Covered Accounts or personally identifiable information that may constitute a risk to the College or its students.
The supervisor of each office that maintains a Covered Account under this Program is responsible for ensuring that appropriate identity theft training for all requisite employees, officials and contractors occurs annually.
As part of the training, all requisite employees, officials and contractors should be informed of the contents of the College's Identity Theft Program, and be provided with access to a copy of this document along with any supporting procedures and documents. In addition, all should be trained how to identify Red Flags, and what to do should they detect a Red Flag or have similar concerns regarding an actual or potential fraud involving personal information.

Program Administration and Oversight - The President has designated the Chief Administrative and Financial Officer as Program Administrator to oversee administration of this program. The Program Administrator may designate additional staff of the College to undertake responsibility for training personnel, monitoring service providers, and updating the Program, all under the supervision of the Program Administrator.

The Program Administrator or designees shall identify and train responsible staff, as necessary, to effectively implement and apply the Program. All College personnel are expected to assist the Program Administrator in implementing and maintaining the Program.

The Program Administrator or designees shall review service provider agreements and monitor service providers, where applicable, to ensure that such providers have adequate identity theft prevention programs in place. When the Program Administrator determines that a service provider is not adequately guarding against threats of identity theft, he/she shall have the authority to take necessary corrective action, including termination of the service provider's relationship with the College.

Prior to the beginning of each academic year, the Program Administrator shall evaluate the Program to determine whether it is functioning adequately. This evaluation shall include: a case-by-case assessment of incidents of identity theft or attempted identity theft that occurred during the previous academic year; interviews with Responsible Staff; and a survey of all accounts maintained by the College to identify any additional Covered Accounts. In response to this annual evaluation, the Program Administrator shall recommend amendments to this Program for approval by the President.

The Program Administrator shall maintain records relevant to the Program, including: the Written Program; documentation on training; documentation on instances of identity theft and attempted identity theft; contracts with service providers that perform activities related to Covered Accounts; and updates to the Written Program. From time to time, the College Controller, or other designated internal control officer, may perform audits to determine if various segments of the College are in compliance with the Program.