11-20: Identity Theft Prevention Program

- Issued: 5-9
- Revised:
- Approved: 4-09

I. PROGRAM ADOPTION

Fort Lewis College ("College") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the Fort Lewis College Board of Trustees. After consideration of the size and complexity of the College's operations and account systems, and the nature and scope of the College's activities, the Fort Lewis College Board of Trustees determined that this Program was appropriate for the College, and. therefore approved this Program on April 17, 2009.

II. DEFINITIONS AND PROGRAM

1.
    1. **Red Flags Rule Definitions Used in this Program**
        1. "Identity Theft" is a "fraud committed or attempted using the identifying information of another person without authority."
        2. A "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."
        3. A "Covered Account" includes all student accounts or loans that are administered by the College.
        4. "Program Administrator" is the individual designated with primary responsibility for oversight of the program See Section VI below.
        5. "Identifying information" is "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, or routing code.
    2. **Fulfilling Requirements of the Red Flags Rule**

        The purpose of this policy is to establish an Identity Theft Prevention 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.

Under the Red Flags Rule, the College is required to establish an "Identity Theft Prevention Program " tailored to its size, complexity and the nature of its operation Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. 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.

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

III. IDENTIFICATION OF RED FLAGS

1.
   1. The Program identifies the following red flags:
      1. Documents provided for identification appear to have been altered or forged;
      2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
      3. A request made from a non-College issued e-mail account;
      4. A request to mail something to an address not listed on file, and;
      5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.
   2. The Program considers the following risk factors in identifying relevant red flags for covered accounts:
      1. The methods provided to open covered accounts - acceptance to the College and enrollment in classes typically requires the following information:
         1. common application with personally identifying information
         2. academic transcripts
         3. official test scores, ex. ACT, SAT, Toefl
         4. immunization history
      2. The methods provided to access covered accounts:
         1. Disbursements obtained in person requires picture identification.
         2. Disbursements obtained by mail can only be mailed to an address on file.
         3. Electronic disbursement will only be established with picture identification.
      3. The College's previous history of identity theft.

IV. DETECTING RED FLAGS

1.
    1. **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:

       <u>Detect</u>
        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 driver's license or other government-issued photo identification).
    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:

       <u>Detect</u>

        1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
        2. 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
        3. Verify changes in banking information given for billing and payment purposes.
    3. **Credit and/or Background Report Request**
       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 the report is made to the reporting agency; and
        2. In the event that notice of an address discrepancy is received, verify that the report pertains to the applicant for whom the requested report was made and report to the reporting agency an address for the applicant that the College has reasonably confirmed is accurate.

V. <u>PREVENTING AND MITIGATING IDENTITY THEFT</u>

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:

<u>Prevent and Mitigate</u>

1.
    1.

1. Continue to monitor a Covered Account for evidence of Identity Theft; or
2. Deny access to the covered account until other information is available to eliminate the red flag;
3. Contact the student or applicant (for which a credit report was run);
4. Change any passwords or other security devices that permit access to Covered Accounts;
5. Not open a new Covered Account;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. File or assist in filing a Suspicious Activities Report ("SAR"); or
9. Determine that no response is warranted under the particular circumstances.

Protect 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.
   1.
      1. Ensure that its website is secure or provide clear notice that the website is not secure;
      2. 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;
      3. Ensure that office computers with access to Covered Account information are password protected;
      4. Avoid use of social security numbers;
      5. Ensure computer virus protection is up to date; and
      6. Require and keep only the kinds of student information that are necessary for College purposes.

VI. PROGRAM ADMINISTRATION

1.
   1. **Oversight**
      Theft Committee ("Committee") for the College. The Committee is headed by a Program Administrator who may be the President of the College or his or her appointee. Two or more other individuals appointed by the President of the College or the Program Administrator comprise the remainder of the • committee membership. The Program Administrator 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.

2. **Staff Training and Reports**
   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. At least annually or as otherwise requested by the Program Administrator, College staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator 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.
3. **Service Provider Arrangements**
   The College shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts.
4. **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 with a 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 the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.
5. **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 Ident it y Theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these facto rs, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.

Revision History

Previously Approved Policy migrated from Budget Office website to Policy Library – 11-20 Identity Theft Prevention Program policy, approved April 2009.