BAY de NOC COMMUNITY COLLEGE BOARD OF TRUSTEES POLICIES

2000 BUSINESS AFFAIRS

2022 IDENTITY THEFT POLICY

The College is a creditor under the Fair and Accurate Credit Transaction Act of 2003 (FACTA) because it participates in the Federal Perkins Loan Program and offers tuition payment plans throughout the semester rather than requiring full payment at the beginning of the semester. In accordance with the requirements of FACTA the College is committed to developing and implementing a written identity theft prevention procedure in connection with new and existing accounts offered or maintained by the College that involve or are designed to permit multiple payments or transactions and any other account that the College offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the College from identity theft, including financial, operation, compliance, reputational or litigation risk.

PROCEDURE:

Definitions

a. Identity Theft
   This is a fraud committed or attempted using the identifying information of another person without authority.

b. Covered Account
   This is a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made periodically over time such as a tuition or fee installment payment plan. Student accounts and loans administered by the College are covered accounts.

c. Personal Information
   This is identifying information which 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, computer's Internet Protocol address, or routing code.

d. Red Flags
   These are relevant patterns, practices, and specific activities that signal possible identity theft and fall in the following five categories: alerts, notifications or warnings from consumer reporting agencies; suspicious documents; suspicious personally identifying information, such as a suspicious address change; unusual use of, or other suspicious activity related to, a student account; and notices from students,

victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with student accounts held by the College.

e. Service Provider
A service provider is a person or entity that provides a service directly to the College.

The Procedure outlined below is intended as a reasonable policy and procedure for detecting, preventing, and mitigating identity theft by:

1. Identifying relevant Red Flags for Covered Accounts;

2. Detecting Red Flags in connection with opening of Covered Accounts and existing Covered Accounts;

3. Responding appropriately to any detected Red Flags including the reasonable mitigation of Identity Theft; and

4. Ensuring that the program is updated periodically to reflect changes in risks to students and to the safety and soundness of the College.

Procedure Requirements

1. Identify Covered Accounts and relevant service provider Covered Accounts, if any.

2. Identify and establish risk factors in identifying relevant Red Flags including:
   a. Types of Covered Accounts;
   b. Methods provided to open Covered Accounts;
   c. Methods used to access Covered Accounts; and
   d. The College's previous history of Identity Theft.

3. Identify specific Red Flags: In order to identify relevant Red Flags, the College has reviewed the types of accounts offered and maintained, the methods provided to open and access these accounts, and previous experiences with identity theft. The College identified the following twenty-six (26) examples of Red Flags in the below five categories.
   a. Notification and warnings from credit reporting agencies:
      - If a fraud or active duty alert is included with a consumer report.
      - If a consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
      - If a consumer reporting agency provides a notice of address discrepancy.
      - If a consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an application, such as:
        - A recent and significant increase in the volume of inquiries;

- An unusual number of recently established credit relationships;
- A material change in the use of credit, especially with respect to recently established credit relationships, or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

b. Suspicious documents:
   - If documents provided for identification appear to have been altered, forged or inauthentic.
   - If the photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification.
   - If other information on the identification is not consistent with the information provided by the student.
   - If other information on the identification is not consistent with readily accessible information that is on file with Bay College, such as a signature on a registration form or other document.
   - If a document appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

c. Suspicious identifying information:
   - If personal identifying information provided is inconsistent when compared against external information sources used by Bay College such as inconsistent birth dates or addresses.
   - If personal identifying information provided by the student is not consistent with other personal identifying information provided by the student. For example, there is a lack of correlation between the SSN range and the date of birth.
   - If personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Colleges. For example:
     - The address on the document is the same as the address provided on a fraudulent document; or
     - The phone number on the document is the same as the number provided on a fraudulent document;
   - If personal identifying information provided is a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Colleges. For example:
     - The address on the document is fictitious, a mail drop or a prison;
     - The phone number is invalid;
     - The SSN provided is the same as that submitted by other students;

- The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other students;
- The student fails to provide all required personal identifying information on a document or in response to notification that the information is incomplete;
- Personal identifying information provided is not consistent with personal identifying information that is on file with Bay College; or
- The College uses challenge questions, the student cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

d. Suspicious account activity:
   - Shortly following the notice of a change of address for a student account, the College receives a request for the addition of other authorized users on the account.
   - A student account is used in a manner commonly associated with patterns of fraud. For example, the student fails to make the first payment or makes an initial payment but no subsequent payments.
   - A student account is used in a manner that is not consistent with established patterns of activity on the account. For example, nonpayment when there is no history of late or missed payments or a material change in usage patterns;
   - A student account that has been inactive for a reasonably lengthy period of time is used.
   - Mail sent to the student is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the student's account.
   - The College is notified that the student is not receiving paper account statements.
   - The College is notified of unauthorized charges or transactions in connection with the student's account.

e. Alerts from others:
   The College is notified by a student, a victim of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with student accounts held by the College.

4. Detect Red Flags in appropriate areas including:
   a. Student Enrollment
   b. Existing Covered Accounts
   c. Credit Report Requests

5. In the event the College detects any identified Red Flags, action steps may include, but are not limited to, one or more of the following, depending on the degree of risk posed by the Red Flag:
   a. Deny access to the Covered Account until other information is available to eliminate the Red Flag;
   b. Contact the student;
   c. Change any passwords, security codes, or other security devices that permit access to a covered account;
   d. Not open a new student account;
   e. Close an existing student account;
   f. Not attempt to collect on a student account or not selling a student account to a debt collector;
   g. Notify law enforcement; and
   h. File or assist in filing a Suspicious Activities Report or determine if no response is warranted under the particular circumstances.

   Any employee who detects a Red Flag associated with student enrollment will fill out the Maxient Red Flag form located on the College's reporting website. Submission of this form will automatically notify the Identity Theft Prevention Team and appropriate personnel.

   Identity Theft Prevention Team Representative Areas:
   - Staff Accountant
   - Director of Financial Aid
   - Executive Director of Information Technology and Security
   - Digital Web Tech Specialist
   - Registrar

   The Identity Theft Prevention Team will review any reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft.

   Prevention and Protection of Student Identifying Information
   - In order to prevent and mitigate identity theft, the College will take the following steps with respect to internal operating procedures to protect student identifying information:
     - Ensure Bay College website is secure or provide clear notice that the website is not secure;
     - 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;
     - Ensure office computers with access to student account information are password protected;
     - Limit use of social security numbers;

- Ensure computer virus protection is up to date;
- Require and keep only student information that is necessary for college purposes;
- Provide identity theft information on the College's webpage in the Consumer Information/Student Right to Know section; and
- Provide Release of Student Information Guidelines to new and current staff who work with student accounts, student records, financial aid or other personal identifiable information.

The Identity Theft Prevention Policy and Procedure is the responsibility of the Identity Theft Prevention Team.

The Identity Theft Prevention Team is responsible for monitoring and updating the program. The Identity Theft Prevention Team is responsible for ensuring appropriate training of the College's employees on the procedure, for reviewing any reports regarding the detection of Red Flags, and for reviewing the steps for preventing and mitigating identity theft. The Identity Theft Prevention Team will report annually, or as needed, to the Board of Trustees on the effectiveness of the program, significant incidents involving identity theft, and the College's response, and recommendations for material changes to the Procedure. The Identity Theft Prevention Team will update the procedure as necessary.

Training:
College employees with responsibilities in the areas of student accounts, student records, financial aid, website responsibility, and information technology will receive annual training as part of this prevention program. Training shall include detection and recognition of red flags, appropriate handling of notices, and action steps. Training shall be conducted for any other employees and all new employees for whom it is reasonably foreseeable may come into contact with student accounts or personally identifiable information. To ensure maximum effectiveness, employees will continue to receive additional training as changes to the program are made.

Service Provider Arrangements:
In the event the College engages a service provider to perform an activity in connection with one or more student accounts, the College will take the following steps to make every reasonable effort that the service provider performs its activity in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

1. Provide service providers with the College's Identity Theft Prevention Program; and

2. Request service providers to certify that they have received, and will abide by the College's Identity Theft Prevention Program, and will report any Red Flags to the Bay College employee with primary oversight of the service provider.

Updates:
The Identity Theft Prevention Team will periodically review and update this program to reflect changes in risks to students and the soundness of the College from identity theft. The program will be re-evaluated to determine whether all aspects are up to date and applicable in the current business environment. Red flags will be reviewed and may be revised, replaced, or eliminated as determined.