AP 5800 Prevention of Identity Theft in Student Financial Transactions

Reference:

15 U.S. Code Section 1681m(e), (Fair and Accurate Credit Transactions Act)
ORS 646A.600 to 646A.628 (Oregon Consumer Information Protection Act)
OR Senate Bill 684 (Data Protection Bill)

I. The Purpose of the Identity Theft Prevention Program

The purpose of this Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to students from identity theft, by providing for the identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could indicate identity theft.

II. Definitions

Identity Theft - a fraud attempted or committed using identifying information of another person without authority. The fraudulent acquisition and use of a person's private identifying information, usually for financial gain.

Installment Payments - payments at a future date for tuition and fees

Covered account - one that involves multiple payments or transactions

Personal Identifying Information - credit card information, tax identification numbers, Social Security numbers, payroll information, medical information, account security codes or PIN numbers, or any other information associated with an individual that could identify a specific person by itself or in combination with other information

Red Flags – patterns, practices, and specific forms of activity that indicate possible opportunities for identity theft

Third Party Contractor – an external entity that, in order to provide a contracted service to the College, has access to College "covered accounts", College "covered accounts" applications, and/or any "personal identifying information" associated with those accounts or with College employees or service providers

III. Procedures for Detecting "Red Flags" For Potential Identity Theft

The intent of this policy is to protect students, faculty, staff, and other College constituents, and the College itself from damages resulting from the fraudulent activity of identity theft. Detection or discovery of a "Red Flag" implicates the need to act under this ITPP to help prevent, detect, and correct identity theft.

A. **Risk Factors for Identifying "Red Flags"**

The College will consider the following factors in identifying relevant "Red Flags:"

1. the types of covered accounts the College offers or maintains;
2. the methods the College provides to open the College covered accounts;
3. the methods the College provides to access the College covered accounts; and
4. the College's previous experience(s) with identity theft.

B. **Sources of "Red Flags"**

The College will continue to incorporate relevant "Red Flags" into this ITPP from the following sources:

1. incidents of identity theft that the College has experienced;
2. methods of identity theft that the College identifies that reflects changes in identity theft risks; and
3. guidance from the College supervisors who identify changes in identity theft risks.

C. **Categories of "Red Flags"**

The following Red Flags have been identified for the College's covered accounts:

Alerts, Notifications, or Warnings from a Consumer Reporting Agency:

1. A fraud or active duty alert is included with a consumer report the College receives as part of a background check.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student substantially differs from the one the credit reporting agency has on file. See Section (V)(9) for specific steps that must be taken to address this situation.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant.

Suspicious Documents:

1. Documents provided for identification appear to have been forged or altered.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
4. Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check.
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

Suspicious Personally Identifying Information:

1. Personal identifying information provided is inconsistent when compared against external information sources used by the College.
2. Personal identifying information provided by a person is not consistent with other personal identifying information provided by the person. For example, there is a lack of correlation between the SSN range and date of birth.
3. Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the College.
4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College.
5. The SSN provided is the same as that submitted by other persons currently being served by the College.
6. The address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of other persons being served by the College.
7. The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
8. Personal identifying information provided is not consistent with personal identifying information that is on file with the College.
9. The person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use Of – Or Suspicious Activity Relating To – A Covered Account:

1. A new covered account is used in a manner that is commonly associated with known patterns of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments made.
2. A covered account is used in a manner that is not consistent with established patterns of activity on the account.
3. A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active.
4. Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person's covered account.
5. The College is notified that the person is not receiving paper account statements.
6. The College is notified of unauthorized transactions in connection with a person's covered account.

IV. Measures to Detect "Red Flags"

Red Flags signal potential identity theft situations. Each employee or contractor who comes in contact with personal identifying information in any form must be aware of

the potential identity theft situations for his/her area and job responsibilities as outlined in the schools or department's Identity Theft Prevention Program. The employee must be prepared to initiate the appropriate action steps to be taken in accordance with the school's or department's Identity Theft Prevention Program when fraudulent activity is suspected. Any time an employee suspects fraudulent activity involving personal identifying information and/or College accounts, the employee should assume that the school's or department's Identity Theft Prevention Program applies and s/he should immediately follow protocols established by his/her unit for reporting the suspected identity theft incident.

If an employee suspects fraudulent activity, reports the activity to their supervisor or other designated individual in the department.

V. Preventing and Mitigating Identity Theft

One or more of the following measures, as deemed appropriate under the particular circumstances, shall be implemented to respond to "Red Flags" that are detected:

1. Monitor the covered account for evidence of identity theft;
2. Contact the person who holds the covered account;
3. Change any passwords, security codes, or other security devices that permit access to a covered account;
4. Reopen the covered account with a new account number;
5. Not open a new covered account for the person;
6. Close an existing covered account;
7. Not attempt to collect on a covered account or not sell a covered account to a debt collector;
8. Notifying law enforcement;
9. Where a consumer reporting agency provides an address for a consumer that substantially differs from the address that the consumer provided, the College shall take the necessary steps to for a reasonable belief that the College knows the identity of the person for whom the College obtained a credit report, and reconcile the address of the consumer with the credit reporting agency, if the College establishes a continuing relationship with the consumer, and regularly, and in the course of business, provides information to the credit reporting agency; or
10. Determine that no response is warranted under the particular circumstances.

VI. Updating the ITPP

The College shall update this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, or to reflect changes in risks to the safety and soundness of the College from identity theft, based on the following factors:

1. The experiences of the College with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;
4. Changes in the types of covered accounts that the College maintains;

5. Changes in the business arrangements of the College, including service provider arrangements.

VII. Methods for Administering the ITPP

A. Oversight of the ITPP

Oversight by the College's Chief Information Officer shall include:

1. Assigning specific responsibility for the ITPP's implementation;
2. Reviewing reports prepared by the staff regarding compliance of the ITPP; and
3. Approving material changes to the ITPP as necessary to address changing identity theft risks.

B. Reports

1. **In General** – Staff responsible for the development, implementation, and administration of this ITPP shall report to the Board of Education on an annual basis.
2. **Contents of Report** – The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the ITPP.
3. **Oversight of Service Provider Arrangements** – Whenever the College engages a service provider to perform an activity in connection with one or more covered accounts the College shall take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. To that end, the College shall require our service contractors, by contract, to have policies and procedures to detect relevant "Red Flags" that may arise in the performance of the service provider's activities, and either report the "Red Flags" to the College, or to take appropriate steps to prevent or mitigate identity theft.

Rescinds Policy Number: IV.A.090

Approved: December 3, 2019

Revised: January 4, 2022