UMPQUA COMMUNITY COLLEGE

ADMINISTRATIVE PROCEDURE

TITLE: Prevention of Identity Theft in Student Financial Transactions

ADMINISTRATIVE PROCEDURE # 5800 ***(was 600.08 Red Flag Rules)***

RELATED TO POLICY # 5800 PREVENTION OF IDENTITY THEFT

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" is a fraud attempted or committed using identifying information of another person without authority.

A. A "creditor" includes government entities who defer payment for goods (for example, payment plans for tuition payments or parking tickets), issued loans or issued student debit cards. Government entities that defer payment for services provided are not considered creditors for purposes of this ITPP.

B. "Deferring payments" refers to postponing payments to a future date and/or installment payments on fines or costs.

C. A "Covered Account" includes one that involves multiple payments or transactions.

D. "Program Administrator" is the individual designated with primary responsibility for oversight of the program.

E. "Person" means any individual who is receiving goods, receives a loan, and/or is issued a debit card from the College and is making payments on a deferred basis for said goods, loan, and/or debit card.

F. "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, computer's Internet Protocol address, or routing code.

G. Detection or discovery of a "Red Flag" implicates the need to take action under this ITPP to help prevent, detect, and correct identity theft.

III. Detecting "Red Flags" For Potential 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's covered accounts;
3. the methods the College provides to access the College's 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's staff 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:

1. **Alerts, Notifications, or Warnings from a Consumer Reporting Agency:**
   a. A fraud or active duty alert is included with a consumer report the College receives as part of a background check.
   b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
   c. A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student or an employee substantially differs from the one the credit reporting agency has on file. See Section (V)(10) for specific steps that must be taken to address this situation.
   d. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant, such as:

1) A recent and significant increase in the volume of inquiries;
2) An unusual number of recently established credit relationships;
3) A material change in the use of credit, especially with respect to recently established credit relationships; or
4) An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution.

2. Suspicious Documents:

a. Documents provided for identification appear to have been forged or altered.

b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

d. 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.

e. An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

I. Suspicious Personally Identifying Information:

a. Personal identifying information provided is inconsistent when compared against external information sources used by the College.

For example:

1) The address does not match any address in the consumer report; or
2) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

b. 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.

c. Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the College. For example:

1) The address on an application is the same as the address provided on a fraudulent application;

2) The phone number on an application is the same as the phone number provided on a fraudulent application;

d. 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. For example:

1) The address on an application is fictitious, a mail drop, or a prison; or

2) The phone number is invalid, or is associated with a pager or answering service.

e. The SSN provided is the same as that submitted by other persons currently being served by the College.

1) 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.

2) 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.

3) Personal identifying information provided is not consistent with personal identifying information that is on file with the College.

4) The person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

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

a. 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.

b. A covered account is used in a manner that is not consistent with established patterns of activity on the account. For example, there is:

1) Nonpayment when there is no history of late or missed payments; or

2) A material change in electronic fund transfer patterns in connection with a payment.

c. A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active.

d. 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.

e. The College is notified that the person is not receiving paper account statements.

f. The College is notified of unauthorized transactions in connection with a person's covered account.

Notices From Customers/Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses About Possible Identity Theft in Connection with Covered Accounts:

The College is notified by a person with a covered account, a victim of identity theft, a law enforcement authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft.

IV. Measures to Detect "Red Flags"

The College shall do the following to aid in the detection of "Red Flags:"

A. When a new covered account is open, the College shall obtain identifying information about, and information verifying the identity of, the student or other person seeking to open a covered account. Two forms of identification shall be obtained (at least one of which must be a photo identification).

The following are examples of the types of valid identification that a person may provide to verify the identity of the person seeking to open the covered account: valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security Card, current residential lease, or copy of a deed to the person's home or invoice/statement for property taxes.

B. Persons with covered accounts who request a change in their personal information on file, such as a change of address, will have the requested changes verified by the College.

The person shall provide at least one written form of verification reflecting the requested changes to the personal information. For example, if an address change is requested, then documentation evidencing the new address shall be obtained. If a phone number change is requested, then documentation evidencing the new phone number, such as a phone bill, shall be obtained.

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:

A. Monitor the covered account for evidence of identity theft;

B. Contact the person who holds the covered account;

C. Change any passwords, security codes, or other security devices that permit access to a covered account;

D. Reopen the covered account with a new account number;

E. Not open a new covered account for the person;

F. Close an existing covered account;

G. Notify the Program Administrator for determination of the appropriate step(s) to take;

H. Not attempt to collect on a covered account or not sell a covered account to a debt collector;

I. Notifying law enforcement;

J. 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

K. Determine that no response is warranted under the particular circumstances.

VI. Protect 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 identifying information:

A. Ensure that its website is secure or provide clear notice that the website is not secure;

B. Ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information;

C. Ensure that office computers with access to Covered Account information are password protected;

D. Avoid use of social security numbers;

E. Ensure computer virus protection is up to date; and

F. Require and keep only the kinds of information that are necessary for College purposes.

VII. 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:

A. The experiences of the College with identity theft;

B. Changes in methods of identity theft;

1. Changes in methods to detect, prevent and mitigate identity theft;
2. Changes in the types of covered accounts that the College maintains;
3. Changes in the business arrangements of the College, including service provider arrangements.

VIII. Methods for Administering the ITPP

Oversight of the ITPP

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee ("Committee") for the College headed by a Program Administrator who may be CFO or his or her appointee. The remainder of the committee membership comprises administrative positions from the areas of Human Resources, Information Technology, and Student Services. 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.

Oversight by the Program Administrator shall include:

A. Assigning specific responsibility for the ITPP's implementation;

B. Reviewing reports prepared by the staff regarding compliance of the ITPP; and

C. Approving material changes to the ITPP as necessary to address changing identity theft risks.

IX. Reports

A. In General – Staff responsible for the development, implementation, and administration of this ITPP shall report to the Program Administrator on an annual basis.

B. 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.

C. **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.

References:
15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act (FACT ACT or FACTA))

ORS 646A.604(8) (notice exception – Oregon Consumer Identity Theft Protection Act)

RESPONSIBILITY:
The CFO is responsible for implementing and updating this procedure.

NEXT REVIEW DATE:
DATE OF ADOPTION: 2/18/2020 by CC
DATE(S) OF REVISION:
DATE(S) OF PRIOR REVIEW: