Blue Mountain Community College

Administrative Procedures

Procedure Title:	**Identity Theft Prevention Program**
Procedure Number:	**01-2009-0001**
Board Policy Reference:	**IV.A.**

Accountable Administrator:	**VP, Operations**
Position responsible for updating:	**VP, Operations**
Original Date:	**March 3, 2009**
Date Approved by Cabinet:	**May 26, 2009; 03-27-12**

Authorized Signature: *Signed original of file*
Dated: May 26, 2009; 04-02-12
Date Posted on Web: 05-27-09; 04-02-12
Date Revised/Reviewed: 03-12

Purpose/Principle/Definitions:

I. Purpose

This procedure is intended to establish an Identity Theft Prevention Program ("the Program"). The Program is designed to detect, prevent and mitigate Identity Theft in connection with certain Community College accounts, programs, or procedures (including specifically installment payment contracts). This procedure applies to College accounts, programs, or procedures which either: 1) allow a person or entity to make multiple payments on student tuition accounts; or 2) present a "reasonably foreseeable risk" of Identity Theft.

As general guidance, this procedure will apply to any College account, program, or procedure which allows payments or collects, transfers, stores, or records a person's personally identifiable information.

This procedure complies with Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act) of 2003 and, by law, is deemed in compliance with the Oregon Identity Theft Act as provided by ORS 646A.622(2)(a) and (b).

II. Definitions

A covered account means:

1. An account that the College offers or maintains primarily for tuition and fees that involves or is designed to permit multiple payments or transactions. Covered accounts may include credit card accounts, checking accounts, and savings accounts; and

2. Any other account that the College offers or maintains for which there is a reasonably foreseeable risk of Identity Theft to customers or a risk to the safety and soundness of the College's utility of Identity Theft, including financial, operational, compliance, reputation or litigation risks.

Identify theft means fraud committed or attempted using the Identifying Information of another person without authority.

A Red Flag means a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

Identifying Information means 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, or unique electronic identification number.

Security Information is defined as government data or the disclosure of which would be likely to substantially jeopardize the security of Identifying Information.

III. Program

The College hereby establishes an Identity Theft Prevention Program to detect, prevent and mitigate Identity Theft. The Program includes procedures to:

1. Identify Red Flags for 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 detected Red Flags to prevent and mitigate Identity Theft; and

4. Update the Program periodically to reflect changes in risks to customers and to ensure the safety and soundness of the utility from Identity Theft.

IV. Program Administration/Oversight

Responsibility for developing, implementing and updating this Program lies with the VP of Operations. The Program Administrator is the VP of Operations.

The Program Administrator will be responsible for:

1. Program resources and planning;

2. Ensuring appropriate Program training of utility staff;

3. Reviewing any staff reports regarding Red Flag detection and Identification Theft mitigation and prevention;

4. Access the sufficiency of safe guards in place to control the identified risks;

5. Assesses risks of information storage and disposal;

6. Determining which steps of prevention and mitigation should be taken in particular circumstances commensurate with the risk posed; and

7. Considering periodic changes to the Program;

8. Regularly tests and monitors the effectiveness of key controls, systems and procedures.

Staff Training and Reports

1. Staff responsible for implementing the Program will be trained by or under the direction of the Program Administrator. Staff will provide timely reports to the Program Administrator on all incidents of Identity Theft or occurrences of Red Flags.

2. The Program Administrator is responsible for familiarizing themselves with the Program and shall meet with staff annually to assess current compliance.

3. Disposes of personal information after it is no longer needed for business purposes or as required by local, state or federal law by burning, pulverizing, shredding or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed.

Program Updates

The Program Administrator will review and update the Program at least once a year to reflect changes in risk to customers and the soundness of College programs from Identity Theft. In doing so, the Program Administrator will consider the College's experience with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, including the degree of Identity Theft risk posed, the Program Administrator will determine whether changes to the Program, including the listing of new Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the College's governing body with recommended changes and the governing body will make a determination of whether to accept, modify or reject those changes to the Program.

V. Identification of Red Flags

In order to identify Red Flags, the College considers the types of accounts or programs it offers and maintains, the methods it uses to open and access accounts, and its previous experiences with Identity Theft. The College has identified the following Red Flags in each of the listed categories:

Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;

2. Notice or report from a credit agency of a credit freeze on a customer or applicant;

3. Notice or report from a credit agency of an active duty alert for an applicant; and

4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

Suspicious Documents

Red Flags

1. Identifying Information that appears to be forged, altered or inauthentic;

2. Identifying Information on which a person's photograph or physical description is inconsistent with the person presenting the document;

3. Other document with information that is inconsistent with existing customer information (such as if a person's signature on a check appears forged);

4. Application that appears to have been altered or forged.

Suspicious Personal Identifying Information

Red Flags

1. Identifying Information presented inconsistent with other information the customer provides (example: inconsistent birth dates);

2. Identifying Information presented inconsistent with other sources of information (for instance, an address not matching an address on a credit report);

3. Identifying Information presented that is the same as information shown on other applications that were found to be fraudulent;

4. Identifying Information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

5. Social security number presented that is the same as one given by another customer;

6. An address or phone number presented that is the same as that of another person;

7. Failure to provide complete personal Identifying Information on an application when reminded to do so (however, Social Security numbers must not be required); and

8. Identifying Information inconsistent with the information on file for the customer.

Alerts from Others

Red Flag

1. Notice to the College from a customer, Identity Theft victim, law enforcement or other person that the college has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

VI. Detecting Red Flags

New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account or program which pertains to household or personal matters (such as a student account) or which presents a foreseeable risk of Identity Theft, College personnel will take the following steps to obtain and verify the identity of the person or business opening the account:

1. Require certain Identifying Information, including:

    a. Full name;
    b. Date of birth (for individual);
    c. Previous and current residential or business address;
    d. Principal place of business (for an entity); and
    e. Identification. Required identification shall include the following:

        i. For a U.S. Citizen
            1. Taxpayer Identification number (for business) or Social Security number; and/or
            2. Photo-bearing documents (original required) such as:
                a. State-issued driver's license; or
                b. State-issued identification card; or
                c. Passport from any country

        ii. For a Non-U.S. Citizen
            1. Social Security number; and/or
            2. Photo-bearing documents (original required) such as:
                a. State-issued driver’s license; or
                b. State-issued identification card; or
                c. Passport from any country; or
                d. Documents containing an alien identification number and country of issuance; or
                e. Any other photo-bearing government-issued document evidencing nationality or residence.

2. Review all documentation for Red Flags; and/or independently contact the customer.

Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account or program**, personnel will take the below steps to monitor transactions with an account. College personnel have the discretion to determine the degree of risk posed and to act accordingly.

1. Verify customer's Identifying Information if a customer requests any information on the account (this can be done in person, via telephone, via facsimile, or via email);

2. Verify the validity of requests to change billing addresses; and

3. Verify changes in banking information given for payment purposes.

VII. Preventing and Mitigating Identity Theft

1. **Ongoing Operations to Prevent Identity Theft.** In order to further prevent the likelihood of Identity Theft, BMCC authorized or designated personnel will take the below steps, commensurate with the degree of risk posed, regarding ongoing internal operating procedures. Program Administrator have the discretion to determine the degree of risk posed and to act accordingly.

    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 customer Identifying Information;
    c. Ensure that office computers are password protected;
    d. Keep offices clear of papers containing customer information;
    e. Ensure computer virus protection is up-to-date;
    f. Require and keep only information necessary for student purposes;
    g. Transmit Identifying Information using only approved methods and include the following statement on any transmitted Identifying Information:

        "This message may contain confidential and/or proprietary information, and is intended for the person/entity to which it was originally addressed. If you have received this email by error, please contact the College and then shred the original document. Any use by others is strictly prohibited.

    h. Do not use or post customer's Social Security number as an account identifier or on any other documents unless requested by customer or required by federal law (such as W-2 and 1098-T forms).

    A template has been developed for staff to utilize to help prevent identity theft related to student and staff information received or kept in paper or electronic formats. See Appendix A (includes template and related examples)

2. **Steps to take when you detect a Red Flag.** In the event authorized or designated College personnel detect Red Flags, they will take one or more of the below steps, commensurate with the degree of risk posed, to prevent and mitigate risk of Identity Theft. Program Administrator have the discretion to determine the degree of risk posed and to act accordingly.

    a. Continue to monitor an account for evidence of Identity Theft;
    b. Contact the customer either by written notice or telephone;
    c. Refuse to open a new account;
    d. Close an existing account;
    e. Reopen an account with a new number;
    f. Notify the Program Administrator for determination of the appropriate step(s) to take;
    g. Notify law enforcement; or
    h. Determine that no response is warranted under the particular circumstances.

3. **Steps to take when you receive notice of an address discrepancy.** In the event the College receives a notice of address discrepancy from a nationwide customer reporting agency indicating the address given by the consumer differs from the address contained in the consumer report, the College will reasonably confirm that an address is accurate by any of the following means:

    a. Verify the address with the customer;
    b. Review college records;
    c. Verify the address through third-party sources; or
    d. Use other reasonable means to verify the address.

    If an accurate address is confirmed, the College will furnish the customer's address to the nationwide consumer reporting agency from which it received the notice of address discrepancy if:

    a. The College establishes a continuing relationship with the customer; **and**

2. b. The College, regularly and in the ordinary course of business, furnishes information to the customer reporting agency.

VIII. Service Provider Arrangements

In the event the College engages a service provider to perform an activity in connection with a Covered Account, the College will take one of the following steps to ensure the service provider performs in accordance with the Program:

1. Require, by contract, that service providers have appropriate policies and procedures in place designed to detect, prevent, and mitigate Identity Theft; or
2. Require, by contract, that service providers review this Program and report any Red Flags to the Program Administrator; and
3. All personnel with access to data have FERPA certification.

The above specified contracts shall include indemnification provisions limiting the College's liability for the service provider's failure to detect, prevent, or mitigate Identity Theft.

IX. Non-disclosure of Specific Practices

Disclosure of specific information or practices regarding Red Flag identification, detection, mitigation and prevention practices may be limited to designated College staff and/or policymakers. Documents produced to develop or implement the Program which describe specific practices may constitute Security Information and may be non-disclosable because disclosure would likely jeopardize the security of Identifying Information and may circumvent the College's Identity Theft prevention efforts.

Legal References:
ORS 646A.622(2)(a) and (b)
OAR 166-030
ORS 192

Appendix A**Department Name**: _____

To ensure confidentiality of student and staff records, use the following as a guide to review and document department practices and or administrative procedures related to the proper storage and security of student or staff data. In addition, indicate when they receive training and by what person or department. Indicate if this is a one-time training or annual training.

Document	**Storage Method**	**If purged, method used**	**Related Admin Procedure**	**Security measure used (ie: password, locking file cabinet, etc)**	**Staff Member**	**Person or Department providing training**	**Annual or One-Time Training?**	**Date of Training**

Things to consider:

- **Thumb drives**
  - Are they password protected?
  - Where are they stored and who has access to them?
- **Shred bins**
  - Are they emptied each night? If not, they should be
  - What method do you use to shred? Example: personal shredder (cross-cut only) or locked shred bins provided by institution (contracted shredding service)
  - If using a shred bin – is it within a locked area and not in an open public walkway?
- **In box**
  - Do you remove and store items each night? If so, how do you store them?
- **Electronic files:**
  - Who has access to them?
  - Are they password protected?
- **Locking file cabinets**
  - Where are keys kept and who has access to them?
- **Forms with student/staff personally identifiable information**
  - How is it stored? i.e.: electronic or paper
    - If paper: Where do you store information and who has access to that information?
- **Record Retention and Destruction schedule**
  - Do you have one for your area? If so, who is responsible for ensuring documents or information is purged in a timely manner and recorded as such?
  - If not, are you following institutional policy and if so, who is responsible for getting information to the appropriate party to be purged?

Things to remember:

- Do not leave personally identifiable information on your desk even if you lock your door at night. It **MUST** be kept in a locked file cabinet as indicated above or stored electronically.
- If you keep things electronically, make sure they are password protected. If needed, ask for assistance from IT.
- Determine if the information you have is something you really should keep or if it should be stored by another department such as Student Records or HR.