

## Western Wyoming Community College

### Identity Theft Prevention Program

#### I. Program Development

Western Wyoming Community College (“The College”) developed this Identity Theft Prevention Program (“Program”) pursuant to the Federal Trade Commission’s Red Flags Rule (“Rule”), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight of the Board of Trustees of Western Wyoming Community College. After consideration of the size of The College’s operations and account systems, and the nature and scope of The College’s activities, the Board of Trustees determined that this Program was appropriate for Western Wyoming Community College.

#### II. Purpose

This Program is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account, notice of an address discrepancy from a consumer reporting agency in conducting background checks on prospective employees and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. **Identify** relevant red flags for covered accounts it offers or maintains 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;
4. **Ensure** the Program is updated periodically to reflect changes in risks to students, faculty and staff and to the safety and soundness of the creditor from identity theft.

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

#### III. Definitions

**Identify Theft** means fraud committed or attempted using the identifying information of another person without authorization.

**Covered Account** means an account that a creditor offers or maintains, primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions.

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

**Program Administrator** is the individual designated with primary responsibility for oversight of the program. At The College, the Program Administrator shall be the Director of Finance.

#### **IV. Identification of Red Flags**

In order to identify relevant Red Flags, The College considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts and its previous experiences with Identity Theft. The College identifies the following Red Flags in each of the listed categories:

##### **A. Notifications and Warnings from Consumer Reporting Agencies**

###### **Red Flags**

1. Report of fraud accompanying background check report.
2. Receipt of a notice of address discrepancy in response to background check report.

##### **B. Suspicious Documents**

###### **Red Flags**

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student information; and
4. Application for service that appears to have been altered or forged.

### **C. Suspicious Personal Identifying Information**

#### **Red Flags**

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates)
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
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 telephone number or fictitious billing address);
5. Social security number presented that is the same as one given by another student;
6. A person fails to provide complete personal identifying information on an application when reminded to do so; and
7. A person's identifying information is not consistent with the information that is on file for the student.

### **D. Suspicious Covered Account Activity or Unusual Use of Account**

#### **Red Flags**

1. Change of address for an account followed by a request to change the student's name
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the student is repeatedly returned as undeliverable;
5. Notice to The College that a student is not receiving mail sent by The College;
6. Notice to The College that an account has unauthorized activity;
7. Breach in The College's computer system security; and
8. Unauthorized access to or use of student account information.

### **E. Alerts from Others**

#### **Red Flag**

1. Notice to The College from a student, 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.

## **V. Detecting Red Flags**

### **A. Student Enrollment**

In order to detect any of the Red Flags identified above associated with the enrollment of a student, The College will take the following steps to obtain and verify the identity of the person opening the account:

#### **Detect**

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 a student identification card (review of driver's license or other government-issued photo identification).

### **B. Existing Accounts**

In order to detect any of the Red Flags identified above for an existing Covered Account, The College will take the following steps to monitor transactions on an account:

#### **Detect**

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.

### **C. Consumer Report Requests**

In order to detect any of the Red Flags identified above for an employment or volunteer position for which a background report is sought, The College will take the following steps to assist in identifying address discrepancies:

#### **Detect**

1. Require verification from any applicant that the address provided by the applicant is accurate at the time the request for the background report is made to the consumer reporting agency; and

2. In the event that notice of an address discrepancy is received, verify that the background report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that The College has reasonably confirmed is accurate.

## **VI. Preventing and Mitigating Identity Theft**

In the event The College detects any identified Red Flags, The College shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag;

### **Prevent and Mitigate**

1. Continue to monitor a Covered Account for evidence of Identity Theft;
2. Contact the student or applicant;
3. Change any passwords or other security devices that permit access to Covered Accounts;
4. Not open a new Covered Account;
5. Provide the student with a new student identification number;
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;
9. Determine that no response is warranted under the particular circumstances.

### **Protect Student Identifying Information**

In order to further prevent the likelihood of Identify 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. 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. Ensure computer virus protection is up to date;
5. Require and keep only the kinds of student information that are necessary for The College purposes.

## **VII. Updating the Program**

Responsibility for developing, implementing and updating this Program lies with the Program Administrator. This Program will be periodically reviewed and updated to reflect changes in risks to students and the soundness of The College from Identity Theft. At least once per year on a set schedule, the Program Administrator will consider The College's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts The College maintains and changes in The College's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program and submit same to the Board of Trustees for approval.

## **VIII. Staff Training**

Staff employed by The College 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.

## **IX. Program Approval and Adoption**

The Board of Trustees approved and adopted this Identity Theft Program on October 12, 2009.

---

John Freeman, President

Board of Trustees

---

George Eckman, Secretary

Board of Trustees