Identify Theft

IDENTITY THEFT PREVENTION PROGRAM

In compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), and pursuant to the Federal Trade Commission's Red Flag Rule (the "Red Flag Rule"), Regional Center for Border Health, Inc. College of Health Careers (the "College") has adopted this Identity Theft Prevention Program (the "Program").

I. PURPOSE

The risk to the College and its students, faculty, staff and clients from Identity Theft is of significant concern to the College. Therefore, in accordance with the Red Flag Rule, the College adopts this Program in an effort to detect, prevent and mitigate Identity Theft in connection with the opening of a "Covered Account" or any existing "Covered Account," as defined below. The Program is further intended to help protect the College and its students, faculty, staff and clients from damages related to the fraudulent activity of Identity Theft.

This Program contains reasonable procedures that will:
1. Identify relevant Red Flags for new and existing 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 Red Flags detected to prevent and mitigate Identity Theft;
4. Ensure the Program is updated periodically to reflect changes in risks to the College's students, faculty, staff and clients or to the safety of the College from Identity Theft; and
5. Promote compliance with laws and regulations regarding Identity Theft protection.

II. DEFINITIONS; IDENTIFYING RED FLAGS

A. Covered Accounts

For the purposes of the Program, a "Covered Account" includes:
1. Any account that the College offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, such as student accounts or loans that are billed or payable monthly and administered by the College or client accounts where the clients are allowed to defer payments or make installment payments over time; and
2. Any other account that the College offers or maintains for which there is a reasonably foreseeable risk to the College's students, faculty, staff or clients or to the safety and soundness of the College from Identity Theft, including financial, operational, compliance, reputation or litigation risks.

B. Identifying Information

For the purposes of the Program, "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 any:
1. Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code; or
4. Access device, including any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.

C. Identity Theft
For the purposes of the Program, "Identity Theft" means fraud committed or attempted using the Identifying Information of another person without authority.

D. Red Flags
For the purposes of the Program, the term "Red Flags" refers to patterns, practices and specific activities that indicate the possible existence of Identity Theft with regard to new or existing Covered Accounts. In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The College hereby identifies the following as Red Flags and incorporates such into the Program:

1. *Alerts, notifications, or warnings from a consumer reporting agency*. Examples of these Red Flags include the following:
a. A fraud or active duty alert included with a consumer report;
b. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;
c. A notice of address discrepancy from a consumer reporting agency; and
d. A consumer report that indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or consumer, such as:
(i) A recent and significant increase in the volume of inquiries;
(ii) An unusual number of recently established credit relationships;
(iii) A material change in the use of credit, especially with respect to recently established credit relationships; or
(iv) An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

2. *Suspicious documents*. Examples of these Red Flags include the following:
a. Documents provided for identification appear to have been altered or forged;
b. The photograph or physical description on the identification is not consistent with the appearance of the person presenting the identification;
c. Information on the identification documents is not consistent with information provided by the person presenting the identification documents;
d. Information on the identification documents is not consistent with readily accessible information that is on file with the College; and
e. Other documents appear to have been altered or forged, or give the appearance of having been destroyed and reassembled.

3. *Suspicious personal Identifying Information*. Examples of these Red Flags include the following:
a. Personal Identifying Information provided is inconsistent when compared against external information sources used by the College. For example, the Social Security number provided has not been issued, or is listed on the Social Security Administration's Death Master File;
b. Some personal Identifying Information provided by the applicant is not consistent with other personal Identifying Information provided by the applicant;
c. Personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College. For example:
(i) The address on an application is the same as the address provided on a fraudulent application, or
(ii) The phone number on an application is the same as the 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, the address on an application is fictitious, a mail drop or a prison;
e. The Social Security number provided is the same as that submitted by another applicant or consumer;
f. 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 persons opening accounts;
ranted. If warranted, the Committee shall update the Program accordingly.
g. The person opening the Covered Account fails to provide all required personal Identifying Information on an application after receiving notification that the application is incomplete;
h. Personal Identifying Information provided is not consistent with personal Identifying Information that is on file with the College; and
i. When using security questions (mother's maiden name, pet's name, etc.), the person opening the Covered Account cannot answer any such security questions beyond those that merely require information generally available from a wallet or consumer report.

4. *Unusual use of, or suspicious activity related to, the Covered Account*. Examples of these Red Flags include the following:
a. A Covered Account is used in a manner that is not consistent with established patterns of activity on the account or is used in a manner commonly associated with known patterns of fraud;
b. Mail sent to the person is returned repeatedly as undeliverable although activity continues in connection with the Covered Account and the person has attested that he/she is currently receiving mail at that address;
c. The College is notified by the account holder that the account holder is not receiving paper or electronic account statements; and
d. The College is notified of unauthorized charges or transactions by the account holder in connection with a Covered Account.

5. *Notice from others*. Examples of this Red Flag include the College being notified by a student, faculty member, staff member, client, agent, victim of Identity Theft, law enforcement authority or any other person that (i) the College has opened a fraudulent account for a person engaged in

Identity Theft, or (ii) Identity Theft has otherwise been committed in connection with one or more Covered Accounts held by the College.

III. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new Covered Account, College personnel will take appropriate steps, such as the following, to obtain and verify the identity of the person opening the account:
1. Require certain Identifying Information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the person's identity (for instance, review a driver's license or other identification document); and
3. Review documentation showing the existence of a business entity, when applicable.

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, College personnel will take appropriate steps, such as the following, to monitor transactions with an account:
1. Verify, as appropriate, the identification of students if they request information (in person, via telephone, via facsimile, via email, etc.);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in bank information given for billing and payment purposes.

IV. RESPONDING TO RED FLAGS

Once a Red Flag, or potential Red Flag, is detected, the College must act quickly, as a rapid appropriate response can protect the College and its students, faculty, staff, clients and other constituents from damages and loss. Upon detection, the detecting College employee must gather all related documentation, write a description of the situation and present this information to the Program Administrator (defined in Article VI, below) for determination.

The Program Administrator shall complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

If a transaction is determined to be fraudulent, appropriate actions must be taken as soon as reasonably possible. Appropriate actions may include:
1. Canceling a transaction;
2. Closely monitoring or closing the account;
3. Notifying and cooperating with appropriate law enforcement;
4. Changing any passwords or other security codes/devices that permit access to the account;
5. Not opening a new account;
6. Reopening an account with a new number;
7. Not attempting to collect on the account or not selling the account to a debt collector;
8. Determining the extent of liability of the College;

9. Notifying the person whose Covered Account is in question that fraud has been attempted; and/or
10. Determining that no response is warranted under the particular circumstances.

V. PROGRAM ADMINISTRATION

A. Involvement of Management

1. Establishment of the Program is the responsibility of the RCBH Board of Directors. The Board's approval of the initial Program must be appropriately documented.
2. Responsibility for developing, implementing and updating the Program lies with an Identity Theft Committee (the "Committee"). The Committee is headed by a Program Administrator, who shall be appointed by the Chief Executive Officer (or, in the Chief Executive Officer's absence, by the Chief Financial Officer of the College). Three or more other College employees appointed by the Program Administrator shall comprise the remainder of the Committee membership. The Program Administrator will be responsible for the Program administration, for ensuring appropriate training of College employees concerning the Program, for reviewing any staff reports regarding the detection of Red Flags and their recommended steps for preventing and mitigating Identity Theft, for determining which steps of prevention and mitigation should be taken in particular circumstances and for considering periodic changes to the Program and presenting recommended changes to the Committee.

B. Employee Training

College employees 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 responsible steps to be taken when a Red Flag is detected.

C. Oversight of Service Provider Arrangements

In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College will take the following steps to ensure the service provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft:
1. Require that the service provider abide by the College's Program; or
2. Verify that the service provider has such policies and procedures of its own in place.

D. Application of Other Laws and College Policies

The Program should be read and applied in conjunction with applicable laws and other College policies. If an employee/agent is uncertain of the implications of a certain piece of information, he/she should contact the Program Administrator.

VI. PERIODIC UPDATES TO THE PROGRAM

The Committee will review this Program on an annual basis (or as otherwise directed by the Program Administrator) and will update this Program as necessary to reflect changes in Identity Theft-related risks to the College and its students, faculty, staff and clients. In doing so, the Committee will consider the College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection, prevention and mitigation methods, changes in the types of Covered Accounts offered or maintained by the College and changes in the College's business arrangements. After considering these factors, the Committee will determine whether changes to the Program, including the listing of Red Flags, are war