



**Identity Theft
Prevention Program**

| | |
|------------------------|----------------|
| Revision: | 1.0 |
| Effective Date: | March 18, 2010 |
| # Pages: | 3 |

GENERAL INFORMATION

| | |
|-------------------|---|
| Title | Identity Theft Prevention Program |
| Purpose | The VCCS Procedure for Identity Theft Prevention Program specifies the processes to be followed and the required documentation to be developed and maintained to ensure compliance with the FTC rules and VCCS policies, standards, and guidelines. This procedure is applicable for all 23 colleges system wide. |
| Supersedes | None |

METHOD(S) OF CONTACT

The Financial Aid Office, Admissions & Records, and the Business Office of all 23 colleges. Click on [College Locator](#) to find the web addresses for each of the colleges.

IDENTIFYING 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:

| | |
|--|--|
| Notifications and Warnings from Credit Reporting Agencies | <ol style="list-style-type: none"> 1. Report of fraud accompanying a credit report; 2. Notice or report from a credit agency of an active duty alert for an applicant; 3. Notice of address discrepancy in response to a credit report request; and 4. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity. |
| Suspicious Documents | <ol style="list-style-type: none"> 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 whom is 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. |
| Suspicious Personal Identifying Information | <ol style="list-style-type: none"> 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 phone 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. |
| Suspicious Covered Account Activity or Unusual Use of Account | <ol style="list-style-type: none"> 1. Change of address for an account followed by a request to change the student's name; 2. Account used in a way that is not consistent with prior use; 3. Mail sent to the student is repeatedly returned as undeliverable; 4. Notice to the college that a student is not receiving mail sent by the college; 5. Notice to the college that an account has unauthorized activity; |

IDENTIFYING RED FLAGS

| | |
|---------------------------|--|
| | <ol style="list-style-type: none"> 6. Breach in the college's computer system security; and 7. Unauthorized access to or use of student account information. |
| Alerts from Others | <ol style="list-style-type: none"> 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. |

DETECTING RED FLAGS

In order to detect any of the Red Flags identified above the college will use the listed categories below

| | |
|--|---|
| Student Enrollment | <p>College personnel will take the following steps to obtain and verify the identity of the person enrolling at the college:</p> <ol style="list-style-type: none"> 1. Require certain identifying information such as name, date of birth, academic records, home address or other identification on the application; and 2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification). |
| Existing Accounts | <p>College personnel will take the following steps to monitor transactions on an account:</p> <ol style="list-style-type: none"> 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. |
| Consumer ("Credit") Report Requests | <p>College personnel will take the following steps to assist in identifying address discrepancies:</p> <ol style="list-style-type: none"> 1. Compare the address provided by the applicant on his/her employment application to the address on the credit report that is received from the consumer reporting agency; and 2. In the event of an address discrepancy, verify that the credit 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. |

PREVENTING AND MITIGATING RED FLAGS

In the event college personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

| | |
|--|--|
| Prevent and Mitigate | <ol style="list-style-type: none"> 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; or 9. Determine that no response is warranted under the particular circumstances. |
| Protect Student Identifying Information | <p>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 student identifying information:</p> |



**Identity Theft
Prevention Program**

| | |
|------------------------|----------------|
| Revision: | 1.0 |
| Effective Date: | March 18, 2010 |
| # Pages: | 3 |

PREVENTING AND MITIGATING RED FLAGS

| | |
|--|--|
| | <ol style="list-style-type: none"> 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 have the screen saver lockout enabled, and are password protected; 4. Avoid use of social security numbers; 5. Ensure computer virus protection is up to date and malicious software filtering software is available; and 6. Require and keep only the kinds of student information that are necessary for college purposes. |
|--|--|

VERIFY SERVICE PROVIDERS

VCCS will take steps to ensure that the activity of a service provider is conducted in accordance with FTC's Red Flag Rules:

1. Require, by contract, that the service providers have policies and procedures in place; and
2. Require, by contract, that service providers review the college's program and report any red flags to the program administrator or the college employee with primary oversight of the service provider relationship.

TRAINING FOR RED FLAGS

VCCS will train relevant staff to implement the identity theft prevention program effectively.

UPDATING RED FLAGS

Once a year (at a minimum), the program administrator of the Red Flag Prevention Program policy will need to review and update to reflect changes in risks to students and the soundness of the colleges from identity theft. If warranted, the program will need to be updated.

DEFINITIONS

| Word | Definition |
|-----------------|---|
| Covered Account | An account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payment or transactions. These accounts include all student accounts or loans that are administered by the College. |
| Identity Theft | Fraud committed or attempted using the identifying information of another person without authority. |
| FTC | Federal Trade Commission. |
| Red Flag | A pattern, practice, or specific activity that indicates the possible existence of identity theft. Examples of "Red Flag" incidents include presentation of suspicious identity documents or frequent address changes. |
| VCCS | Virginia Community College System, |

REVISION HISTORY

| Date | Revision # | Description of Change |
|-------------|-------------------|--|
| 4/28/09 | 1.0 | Original – Approved March 18, 2010 by State Board for Community Colleges |
| | | |