

Central Oregon Community College

Identity Theft Prevention Program

Effective beginning May 1, 2009

I. PROGRAM ADOPTION

This program has been created to put COCC in compliance with Section 41.90 under the FTC's Red Flag Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act). This requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 41.90(b)(3) to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are to be used by COCC to have a program in place and maintain it, so that COCC satisfies the requirements of § 41.90.

The Program: In designing its Program, COCC will incorporate, as appropriate, into its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to students and customers, or to the safety and soundness of COCC from identity theft.

II. DEFINITIONS AND PROGRAM

A. Red Flags Rule Definitions Used in this Program

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

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

A "Covered Account" includes all student accounts or loans that are administered by COCC.

"Program Administrator" is the individual designated with primary responsibility for oversight of the program. See Section VI below.

"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, or student identification number.

B. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, COCC is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

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 that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from Identity Theft.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, COCC 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. COCC identifies the following Red Flags in each of the listed categories:

A. 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 an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

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 phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another student;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete personal identifying information on an application when reminded to do so; and
8. 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 COCC that a student is not receiving mail sent by COCC;
6. Notice to COCC that an account has unauthorized activity;
7. Breach in COCC's computer system security; and
8. Unauthorized access to or use of student account information.

E. Alerts from Others

Red Flag

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

IV. DETECTING RED FLAGS

The Program's policies and procedures address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by obtaining identifying information about, and verifying the identity of, a person opening a covered account; and authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, COCC personnel 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 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, COCC personnel 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 ("Credit") Report Requests

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

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that notice of an address discrepancy is received, 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 COCC has reasonably confirmed is accurate.

V. PREVENTING AND MITIGATING IDENTITY THEFT

The Program's policies and procedures provide for appropriate responses to the Red Flags that COCC has detected that are commensurate with the degree of risk posed. In determining an appropriate response, COCC will consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by COCC or a third party, or notice that a customer has provided information related to a covered account held by COCC to someone fraudulently claiming to represent COCC or to a fraudulent website.

In the event COCC 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

1. Continue to monitor a Covered Account for evidence of Identity Theft;
2. Contact the student or applicant (for which a credit report was run);
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 ("SAR"); or
9. Determine that no response is warranted under the particular circumstances.
10. 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 COCC and then shred the original document. Any use by others is strictly prohibited."

Protect Student Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, COCC 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;

N:\Dept\ITS\FTC Red Flag Rules\COCCRedFlagRulesUpdatedFinal_Mar09.doc

4. Avoid use of social security numbers (See COCC Information Use Policy);
5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of student information that are necessary for COCC purposes.

VI. PROGRAM ADMINISTRATION

A. Oversight

Oversight by the COCC board of directors, an appropriate committee of the board, or an employee designated by the board, at the level of senior management and identified as the Program Administrator, will include:

- (1) Assigning specific responsibility for the Program's implementation;
- (2) Reviewing reports prepared by staff regarding compliance by COCC with § 41.90 of this part; and
- (3) Approving material changes to the Program as necessary to address changing identity theft risks.

The Program Administrator will be responsible for ensuring appropriate training of COCC 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.

B. Staff Training and Reports

In General: COCC staff 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. COCC staff shall be trained, as necessary, to effectively implement the Program. COCC employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of COCC's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, COCC staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program.

Report Contents: The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

C. Service Provider Arrangements

In the event COCC engages a service provider to perform an activity in connection with one or more Covered Accounts, COCC will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review COCC's Program and report any Red Flags to the Program Administrator or the COCC employee with primary oversight of the service provider relationship.
3. Contractor agrees to comply with all FERPA and 2002 Gramm-Lech-Bliley Act requirements as they relate to any confidential information. Contractor shall be liable for any breach of this provision caused by the act or omission of such party's officers, employees, agents, attorneys, or representatives. Confidential Information shall mean any information provided under this agreement by one party to the other and that is designated by the providing party, or applicable statute, as "confidential".

D. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to the Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be shared with other COCC employees or the public. The Program Administrator shall inform the Committee and those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

E. Program Updates

The Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of COCC from Identity Theft. In doing so, the Committee will consider COCC's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in COCC'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 Committee will update the Program.

Appendix A

Red Flags Of Concern

Following are the 26 Red Flags of Concern identified by the FTC at the time of the creation of this plan in 2009 which are in connection with covered accounts. These 26 Red Flags are covered in the document above:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries;
 - b. An unusual number of recently established credit relationships;
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that was closed for cause or identified for abuse of account privileges by COCC.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. Other information on the identification is not consistent with readily accessible information that is on file with COCC, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by COCC. For example:
 - a. The address does not match any address in the consumer report; or
 - b. The Social Security Number (SSN) has not been issued, or is noticed to be listed on the Social Security Administration's Death Master File.
11. Personal identifying information provided by the student is not consistent with other personal identifying information provided by the student. For example, there is a lack of correlation between the SSN range and date of birth.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources that may be used by COCC. For example:
 - a. The address on an application is the same as the address provided on a fraudulent application; or
 - b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources that may be used by COCC. For example:
 - a. The address on an application is fictitious or a mail drop; or
 - b. The phone number is invalid, or is associated with a pager or answering service.
14. The SSN provided is the same as that submitted by other persons opening an account or other students.
15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other students or other persons opening accounts.
16. The student or other 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.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with COCC.
18. If COCC uses challenge questions, the student or other person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, COCC receives a request for a change to the student's name or a request for the addition of authorized users on a covered account.
20. Payments stop on an otherwise consistently up-to-date account;
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - a. Nonpayment when there is no history of late or missed payments;
 - b. A material increase in the use of available credit;
 - c. A material change in purchasing or spending patterns;
 - d. A material change in electronic fund transfer patterns in connection with a deposit account; or
 - e. A material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for a reasonably lengthy period of time is suddenly used (taking into consideration the expected pattern of usage and other relevant factors).
23. Mail sent to the student or other customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the student or customer's covered account.
24. COCC is notified that the customer is not receiving paper account statements.
25. COCC is notified of unauthorized charges or transactions in connection with a student or other customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. COCC is notified by a customer, 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.