

Red Flag Rules - Tuition Accounts

Background

In response to the growing threat of identity theft, the United States Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Public Law 108-159. This amendment to the Fair Credit Reporting Act charged the Federal Trade Commission with promulgating rules regarding identity theft. On November 7, 2007, the Federal Trade Commission promulgated the final rules, known as “Red Flag” rules [16 CFR 681], which had an original effective date of November 1, 2008. These rules, implementing sections 114 and 315 of FACTA, require the enactment of certain policies and procedures by the revised effective date of August 1, 2009.

FACTA applies to “financial institutions” and “creditors” with “covered accounts.” For the purposes of this legislation, a covered account is an “account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions.” This has been interpreted to include accounts such as student accounts held by colleges and universities. Entities maintaining these accounts must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account within the College.

The document outlines below the proposed program which we have created based on the requirements noted in 16 CFR 681. A subcommittee has been created to develop procedures and an implementation plan, including a timeframe for completion. One of the program requirements is that the program be initially approved by the entity’s Board of Directors (16 CFR 681.2 (d)(2)(iv)(e) Administration of the Program).

The Federal Trade Commission’s (FTC) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003, requires the establishment and implementation of an Identity Theft Program.

Identity Theft Prevention Program

References

16 CFR 681.2 Duties regarding the detection, prevention and mitigation of identity theft.

Program Statement

In accordance with the Fair and Accurate Credit Transactions Act of 2003, this program is intended to prevent, detect and mitigate identity theft in connection with establishing new covered accounts or an existing covered account held by TVCC, and to provide for continued administration of the program.

Definitions

“Board” refers to the Board of Education for Treasure Valley Community College.

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

“Authorized Person” is any person whom a student has authorized in writing to obtain information regarding their account.

“Red Flag” is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

“Covered Account” includes all student accounts or loans that are administered by the College.

“Program Administrator” is the individual designated with primary responsibility for oversight of the program.

“Institution” as used in this document refers to Treasure Valley Community College and its component units such as the Treasure Valley Community College Foundation (TVCC has no other component units).

“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.

Identification of Red Flags

Accounts offered or maintained are primarily receivable accounts that allow students to pay tuition and related charges in installments, or defer payment until financial aid is received. Accounts are opened in person only and at that time students are required to provide identifying information. Account information is accessible online or in person.

The following are considered Red Flags for the purposes of this program:

1. Documents provided for identification appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. Requests for information from individuals other than an authorized person;
4. Requests for login information after repeated unsuccessful attempts to login;
5. A request to mail something to an address not listed on file, with the exception of official transcript requests that are requested by an authorized person; and

6. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Detected Red Flags

1. Student Enrollment
 - a. Student identity will be established during the enrollment process by:
 - (1) Requiring certain identifying information such as name, date of birth, academic records, home address or other identification;
 - (2) For online enrollment we will require the student to provide a log-in name and password before making changes to enrollment or other identifying information;
 - (3) Students applying for any type of financial assistance may be required to provide additional identifying information, as required by issuer.
2. Existing Accounts

In order to protect the identities of the owners of existing covered accounts, the following steps will be taken when requests are made related to an existing account:

- a. Student identity will be verified by asking the student to provide information that would validate their identity;
- b. When the request is made in person, a valid identification document, as noted in the identifying information above; or
- c. When the request is made in person or via telephone, the student may be required to provide answers to questions that would establish their identity.

Responses to Red Flags

In the event that Red Flags are identified, one or more of the following steps should be taken, depending on the degree of risk posed by the Red Flag:

1. Notify students of requests to change significant information on their account. Significant information includes: billing address, passwords, email address, banking information. Students will be notified via mail or telephone call. These communications will include instructions for promptly reporting incorrect changes;
2. Continue to monitor a Covered Account for evidence of identity theft;
3. Deny access to the covered account until other information is available to eliminate the red flag;
4. Contact the student or applicant;
5. Change any passwords or other security devices that permit access to Covered Accounts;

6. Not open a new Covered Account;
7. Notify the Program Administrator for determination of the appropriate step(s) to take;
8. Notify law enforcement;
9. File or assist in filing a Security Report with the Program Administrator; or
10. Determine that no response is warranted under the particular circumstances.

Protect Student Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to Covered Accounts, the following steps will be taken with respect to 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. Limit the use of social security numbers;
5. Ensure computer virus protection is up to date; and
6. Require and retain only information that is necessary in the conduct of our business;
7. Ensure that documents with secure information, such as social security numbers, date of birth, etc. are not being left unsecured at copiers or left unsupervised on employee workstations.

Program Administration

Oversight

Responsibility for developing, implementing and updating this program lies with the Dean of Administrative Services, who has been designated as the Program Administrator.

The Program Administrator will be responsible for ensuring the implementation and continuation of the program, and maintenance of this document, and for obtaining approval from the Board or designated

sub-committee for any changes to the Program. The Program Administrator is responsible for identifying appropriate training of staff, for reviewing any staff reports regarding the detection of Red Flags and for ensuring staff follow the steps for preventing and mitigating identity theft, and for determining which steps of prevention and mitigation should be taken in particular circumstances.

Staff Training and Reports

TVCC personnel shall be trained, as necessary, to effectively implement the program. College employees are required to notify the Program Administrator once they become aware of an incident of identity theft or of the institution's failure to comply with this program.

At least annually or as otherwise requested by the Program Administrator, College staff responsible for development, implementation, and administration of the program shall report to the Board in writing indicating compliance with this program.

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.

Service Provider Arrangements

When contracting with service providers who perform services related to covered accounts, institutions shall require within the contract or purchase order that the service provider assert their compliance with all federal and state laws, and certify that they have taken appropriate steps to comply with the Fair and Accurate Credit Transactions Act of 2003. For those service providers contracted with TVCC, the College personnel shall be responsible for ensuring the same.

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 those responsible for developing this program and 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 employees or the public, notwithstanding any legal requirements that might require disclosure.

Program Updates

The Program Administrator will cause the program to be reviewed periodically and update this program to reflect changes in risks to students from identity theft. In doing so, 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, and changes in the institution'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.

END OF POLICY

Legal Reference(s):

[ORS 341.290](#)