Introduction

The Federal Trade Commission issued the Red Flags Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act), which amended the Fair Credit Reporting Act (FCRA). The rule requires "financial institutions" and "creditors" that hold "covered accounts" to develop and implement an identity theft prevention program for new and existing accounts.

Purpose

The college adopts this Identity Theft Prevention 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. The program is further intended to help protect students, faculty, staff, and other constituents and the college from damages related to the fraudulent activity of identity theft.

This program will:

1. Identify patterns, practices, or specific activities ("Red Flags") that indicate the possible existence of identity theft with regard to new or existing covered accounts;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected under the Program;
4. Ensure periodic updating of the Program, including reviewing the accounts that are covered and the identified Red Flags that are part of the Program; and
5. Promote compliance with state and federal laws and regulation regarding identity theft protection.

Scope

This Identity Theft Prevention Program applies to students, faculty, staff, and other constituents at the college.

Identity Theft Prevention

Confidential information

Central college employees, and students working in campus offices, who because of their work have access to non-public (confidential) information about others must not disclose that information. Employees must protect from the view of visitors non-public information displayed on computer screens. Employees must agree to and observe the Employment Confidentiality Agreement and Confidentiality Policy as maintained by the Human Resources office. (See the Policy on the Acceptable Use of Information Technology and the Confidential Information Policy for additional information) Employees must also verify the identity of students, faculty, staff, or other constituents before disclosing information regarding covered accounts.

Confidential Information includes but is not limited to, the following items whether stored in electronic or printed format:

Credit card information, including:

1. Credit card number (in part of whole)
2. Credit Card expiration date
3. Cardholder name
4. Cardholder address

Tax identification numbers, including:

1. Social Security number
2. Business identification number
3. Employer identification number

Other personal information:

1. Date of birth
2. Address
3. Phone numbers
4. Names
5. Accounts numbers
6. Paychecks
7. Pay stubs

Distribution

Hard Copy Distribution

All college personnel shall comply with the following requirements:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Confidential Information must be locked when not in use.
2. Storage rooms containing documents with Confidential Information and record retention areas must be locked at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas must be cleared of all documents containing Confidential Information when not in use.
4. College records may only be destroyed in accordance with the college's retention policy and applicable law.
5. Documents containing Confidential Information must be destroyed in a secure manner. (example shredding)

Additional Prevention Efforts

Covered accounts

For the purpose of the college's Identity Theft Prevention Program, a covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing account maintained by the college for its students, faculty, staff, and other constituents that meets the following criteria is covered by this program:

1. Accounts for which there is a reasonably foreseeable risk of identity theft; or
2. Accounts for which there is a reasonably foreseeable risk to the safety or soundness of the college from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Red Flags

The following Red Flags are potential indicators of fraud. Any time a Red Flag, or a situation closely resembling a Red Flag is apparent, it should be investigated for verification.

Suspicious documents. Examples of Red Flag alerts include the following:

1. Documents provided for identification that 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, faculty, staff, and other constituent presenting the identification;
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or student, faculty, staff, and other constituent presenting the identification;
4. Other information on the identification is not consistent with readily accessible information that is on file with the college; and
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious personally identifying information. Examples of these Red Flags include the following:

1. Personally identifying information provided is inconsistent when compared against external information sources used by the college;
2. Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the college;
3. Personally identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the college;
4. The SSN provided is the same as that submitted by another student, faculty, staff, or other constituent;

5. The person opening the covered account fails to provide all required personally identifying information on an application or in response to notification that the application is incomplete; and
6. Personally identifying information provided is not consistent with personal identifying information that is on file with the college.

Unusual use of, or suspicious activity related to the covered account. Examples of Red Flags include the following:

1. Shortly following the notice of a change of address for a covered account, the college received a request for new, additional, or replacement goods/services or for the addition of authorized users on the account;
2. A covered account is used in a manner that is not consistent with established patterns of activity on the account;
3. Mail sent to the student, faculty, staff, or other constituent is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account;
4. The college is notified that the student, faculty, staff, or other constituent is not receiving their paper account statements;
5. The college is notified of unauthorized charges or transactions in connection with a covered account; and
6. The college receives notice from the students, faculty, staff, or other constituents, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the college.

Responding to Red Flags

The Program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. Contact the student, faculty, staff, or constituent;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.