Trinity College
Policy Related to "Red Flag Rules" Resulting from the Fair and Accurate Credit Transactions Act of 2003

Effective beginning May 1, 2009

I. PROGRAM ADOPTION

In response to the threat of identity theft primarily through financial transactions, the United States Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA) Public Law 108-159, an amendment to the Fair Credit Reporting Act. In accordance with sections 114 and 315 of FACTA, the Office of the Comptroller of the Currency, Treasury; the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation; the Office of Thrift Supervision, Treasury; the National Credit Union Administration; and the Federal Trade Commission jointly adopted and promulgated rules, known as the "Red Flags Rules" that require certain entities to enact certain policies and procedures by the May 1, 2009, effective date.

Trinity College (the "College") developed this Policy (the "Policy") pursuant to the Red Flags Rules. This Policy was developed in order to satisfy the requirements of the Red Flag Rules, in consideration of the College's size and the nature of its activities, with oversight by the College's Vice President for Finance and Operations and the Audit Committee.

II. PURPOSE AND KEY DEFINITIONS

A. Policy Purpose

Under the Red Flags Rules, the College is required to establish a policy to try to prevent identity theft related to Covered Accounts that is tailored to its size, complexity and the nature of its operation. Its Policy must contain reasonable procedures to:

1. Identify relevant Red Flags for new and existing Covered Accounts and incorporate those Red Flags into the Policy;
2. Detect Red Flags that have been incorporated into the Policy;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Policy is updated periodically to reflect changes in risks to students and other College constituents from Identity Theft.

B. Key Definitions

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

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

"**Covered Account**" includes any account administered by the College that involves or is designed to permit multiple payments or transactions. New and existing accounts maintained by the College for its students, faculty, staff and other constituents for which there exists a reasonably foreseeable risk (1) to the students, faculty, staff, or other constituents related to Identity Theft or (2) to the safety and soundness of College itself from the financial, operational, compliance, reputation or litigation risks resulting from Identity Theft.

"**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:

Personal information such as
- Name
- Maiden name
- Address
- Date of Birth
- Phone number
- Student/Faculty/Staff identification number (e.g., the "L" number assigned by the College)
- Computer's internet protocol address

Credit card or other account information such as
- Credit card/Account number, in whole or in part
- Credit card/Account expiration date

Tax Identification numbers such as
- Social Security number
- Business identification number
- Employer identification number

Payroll information such as
- Paychecks
- Paystubs
- Bank account/routing information

Medical information such as
- Doctor names and claims
- Insurance claims
- Prescriptions
- Any personal medical information

Government-issued identification such as
- Driver's license number
- Alien registration number
- Passport number

III. IDENTIFICATION OF 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 following Red Flags are potential indicators of fraud that the College has identified. Any time a Red Flag, or a situation closely resembling a Red Flag, is apparent, it should be investigated for verification.

A. Notifications and Warnings from Credit Reporting Agencies Red Flag Examples

1. Report of fraud accompanying a credit report;
2. Notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Notice of address discrepancy in response to a credit report request; and

5. A consumer report that indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, 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.

B. Suspicious Documents Red Flag Examples

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.

C. Suspicious Personal Identifying Information Red Flag Examples

1. Identifying Information presented that is inconsistent with other information the person provides (e.g., lack of correlation between the Social Security Number range and the date of birth);
2. Identifying Information presented that is inconsistent when compared against external sources of information used by the College (e.g., address does not match any address in the consumer report);
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 as indicated by internal or third-party sources used by the College;
5. Social security number presented that is the same as one given by another student, faculty, staff, or constituent;
6. An address or phone number presented that is the same as that of another person;
7. Identifying Information provided is not consistent with other information already on file with the College;
8. A person fails to provide complete personal identifying information on an application for a Covered Account or in response to a reminder notification that the application in incomplete; and

9. When using security questions (mother's maiden name, pet's name, etc.) the person cannot provide authenticating information beyond which generally would be available from a wallet or consumer report.

D. Suspicious Covered Account Activity or Unusual Use of Account Red Flag Examples

1. Change of address for an account followed by a request to change the student's or other constituent's name or a request for new, additional or replacement goods or services or for the addition of authorized users on the account;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with an established pattern of activity on that account;
4. Mail sent to the student, faculty, employee, or other constituent is repeatedly returned as undeliverable although transactions continue to be conducted in connection with the Covered Account;
5. Notice to the College that a student, faculty, staff or other constituent is not receiving paper account statements sent by the College;
6. Notice to the College that a Covered Account has unauthorized activity; and
7. Awareness of a breach in the College's computer system security or the security of paper files resulting in unauthorized access to or use of account information of students, faculty, staff or other constituents.

E. Alerts from Others Red Flag Examples

1. Notice to the College from a student, faculty, staff, 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.

IV. DETECTING RED FLAGS

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, College personnel will take the following steps to obtain and verify the identity of the person opening the Covered Account by:

1. Requiring certain identifying information such as name, date of birth, academic records, home address or other identification; and

2. Verifying 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, College personnel will take the following steps to monitor that account:

1. Verify the identification of the student, employee, or other Covered Account holder 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, employee or other Covered Account holder 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, College 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 the College has reasonably confirmed is accurate.

V. PREVENTING AND MITIGATING IDENTITY THEFT

In the event College personnel detect any identified Red Flags, an employee must act quickly, as a rapid appropriate response can protect students, faculty, staff, other constituents and the College from damages and loss. If a potentially fraudulent activity is detected, all related documentation should be gathered and a description of the situation should be summarized and reported to The Vice President for Finance and Operations and The Audit Committee. Depending on the degree of risk posed by the Red Flag, appropriate actions might include:

1. Determine that no response is warranted under the particular circumstances;
2. Cancel the transaction;
3. Continue to monitor the Covered Account for evidence of Identity Theft;
4. Refuse to open a new Covered Account;
5. Contact the student, faculty, employee, applicant (for which a credit report was run) or other applicable constituent;
6. Change any passwords or other security devices that permit access to Covered Accounts;
7. Provide the student, faculty or staff member with a new identification number ("L" number);
8. Notify appropriate law enforcement;
9. File or assist in filing a Suspicious Activities Report ("SAR"); and/or
10. Determine the extent of liability of the College.

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 Identifying Information:

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure that file cabinets, desk drawers, and any other storage spaces or rooms containing documents with Identifying Information be locked when not in use or unsupervised;
3. Ensure that desks, workstations, printers, copiers, fax machines, whiteboards, dry-erase boards in common shared work areas will be cleared of all Indentifying Information when not in use.
4. Ensure complete and secure destruction of paper documents and computer files containing Identifying Information when a decision has been made to no longer maintain such information;
5. Ensure that office computers with access to Covered Account information are password protected;
6. Ensure that all electronic storage and transmission of Indentifying Information follows guidelines established by the College's Information Technology department.
7. Avoid use of social security numbers;
8. Ensure computer virus protection is up to date; and
9. Require and keep only the kinds of Identifying Information that are necessary for College purposes.

VI. POLICY ADMINISTRATION

A. Oversight

Operational responsibility for developing, implementing and updating this Policy lies with the Vice President for Finance and Operations. Additional administration members may included updating this policy such as the Director of Information Technology and/or the Director of Public Safety, among others. The Department of Human Resources and The Comptrollers office will be responsible for ensuring appropriate training of College staff on the Policy, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft in relation to Covered Accounts, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Policy.

B. Staff Training and Reports

Training shall be conducted for all College employees for whom it is reasonably foreseeable that the employee may come into contact with Covered Accounts or Identifying Information that may constitute a risk to the College, its student, faculty, employees or other constituents.

College employees are expected to notify The Vice President for Finance and Operations office once they become aware of an incident of Identity Theft or of the College's failure to comply with this Policy. At least annually or as otherwise requested by the Audit Committee, The Vice President for Finance and Operations shall report to the Audit Committee on compliance with this Policy. 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 Policy.

C. 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

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 that service providers review the College's Policy and report any Red Flags to the Policy Administrator or the College employee with primary oversight of the service provider relationship.

D. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Policy, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to The Vice President for Finance and Operations office 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 Policy that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be shared with other College employees or the public. The Vice President for Finance and Operations shall inform those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

E. Policy Updates

The Vice President for Finance and Operations will periodically review and update this Policy to reflect changes in risks to students, employees and other constituents and the soundness of the College from Identity Theft related to Covered Accounts. In doing so, the Vice President for Finance and Operations will consider the College's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the College's business arrangements with other entities. After considering these factors, the Policy Administration Committee will determine whether changes to the Policy, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Policy.