

---

# Fair & Accurate Credit Transaction Act (Red Flag Rules) Policy and Procedures

*Revised March 2009*  
TABLE OF CONTENTS

	Page
I. POLICY ON THE DETECTION OF ADDRESS INACCURACIES.....	2
II. POLICY ON DETECTION AND PREVENTION OF IDENTITY THEFT.....	3
III. POLICY ON CONTRACTORS & 3 <sup>rd</sup> PARTY SERVICE PROVIDERS.....	9

## **TRINITY UNIVERSITY'S POLICY UNDER THE FAIR & ACCURATE CREDIT TRANSACTION ACT (RED FLAG RULES)**

It is the policy of Trinity University to comply with the regulations of the Federal Trade Commission pertaining to the detection and prevention of identity theft, the "Red Flags Rules," which became effective November 1, 2008 and enforceable on May 1, 2009.

Trinity University shall comply with the regulations, where applicable, as set forth below:

---

### **I. POLICY ON THE DETECTION OF ADDRESS INACCURACIES**

#### **A. Applicability**

This policy applies to Trinity University insofar as it uses consumer reports from consumer reporting agencies for a purpose permitted by the Fair Credit Reporting Act, such as for employment or credit verification purposes.

#### **B. Required Response to Notice from Consumer Reporting Agency**

##### **1. Verification of Information**

If Trinity University receives a notice from a consumer reporting agency that a consumer's address that the University provided to the consumer reporting agency for the purpose of obtaining a consumer report is substantially different than the address that the agency has on file for the consumer, Trinity University shall take reasonable steps to verify that the consumer report requested relates to the consumer about whom the University is seeking information.

Such reasonable steps include, but are not limited to:

- Comparing the information received in the consumer report with the information the University obtains and uses to verify the consumer's identity.
- Comparing the information received in the consumer report with the information the University maintains in its own records, such as applications, change of address notifications, etc.
- Verifying the information in the consumer report with the consumer about whom the information is sought.

##### **2. Response to Consumer Reporting Agency**

Once Trinity University has verified that the consumer about whom information is sought is reasonably related to the consumer identified by the consumer reporting agency, the University will furnish the consumer's address to the consumer reporting agency as part of the

information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

---

## **II. POLICY DETECTION AND PREVENTION OF IDENTITY THEFT**

### **A. Applicability**

This policy applies to Trinity University insofar as it offers covered accounts as defined by this policy and the Fair & Accurate Credit Transaction Act (“FACTA”). In accordance with FACTA, the University has developed and implemented a written Identity Theft Prevention Program (“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. This policy may also apply to the University’s service providers to the extent that they provide covered accounts on behalf of Trinity University. Where applicable, the University requires its service providers to comply with FACTA. If a service provider of the University does not have a stated policy and identity theft prevention program that complies with FACTA, the service provider must comply with this policy.

It is recognized that not all definitions and red flag identifications listed below are applicable to Trinity University; however, definitions and red flag identifications (as defined by FACTA) are listed in order to fully disclose and identify possible and/or future applicability.

### **B. Definitions**

*Covered account* means:

- a. An account that the University offers or maintains that involves or is designed to permit multiple payments or transactions, such as a credit card account, loans, phone accounts, utility accounts, checking account, or savings account; and
- b. Any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of Trinity University from identity theft, including financial, operational, compliance, reputation, or litigation risks.
- c. Covered accounts do not include stored value cards (such as laundry cards or dining hall cards prepaid by the cardholder) if the stored value cards do not require an electronic fund transfer from the cardholder’s account held by the University for the purpose of transferring money between accounts or in exchange for money, property, goods, services or cash.

*Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

**C. Trinity University’s Identity Theft Prevention Program**

As a means of detecting and mitigating identity theft, Trinity University’s Program requires the University to:

1. Identify relevant Red Flags for the covered accounts that the University offers or maintains, and incorporate those Red Flags into its Program;
2. Detect Red Flags that have been incorporated into any Program of the University;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to covered account holders and to the safety and soundness of the University from identity theft.

**D. Identifying Red Flags**

1. Sources of Red Flags

When identifying Red Flags, Trinity University will consider:

- Incidents of identity theft that the University has experienced;
- Methods of identity theft that the University has identified that reflect changes in identity theft risks; and
- Applicable supervisory guidance.

2. Categories of Red Flags

When identifying Red Flags, Trinity University will consider:

**Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, including but not limited to:**

- A fraud or active duty alert included with a consumer report.
- A notice of credit freeze issued in response to a request to a consumer reporting agency for a consumer report.
- A notice of address discrepancy from a consumer reporting agency.
- A consumer report indicating 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 a financial institution or creditor.

**The presentation of suspicious documents, including but not limited to:**

- Documents provided for identification that appears to have been altered or forged.
- Identification documents where the photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Identification documents where the identification information is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Identification documents where the identification information is not consistent with readily accessible information that is on file with the University, such as a signature card or a recent check.
- An application that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

**The presentation of suspicious personal identifying information, including but not limited to:**

- Personal identifying information that is inconsistent when compared against external information sources used by Trinity University. For example:
  - The address does not match any address in the consumer report; or
  - The Social Security Number (“SSN”) has not been issued, or is listed on the Social Security Administration's Death Master File.
- Personal identifying information that is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- Personal identifying information that is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. 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.
- Personal identifying information that is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Trinity University. For example:
  - a. The address on an application is fictitious, a mail drop, or a prison; or
  - b. The phone number is invalid, or is associated with a pager or answering service.
- A SSN that is the same as that submitted by other persons opening an account or other covered account holders.
- An address or telephone number that is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other covered account holders.
- An incomplete application or response to request for additional information that is incomplete.
- Personal identifying information that is not consistent with personal identifying information that is on file with the University.

**The unusual use of, or other suspicious activity related to, a covered account, including but not limited to:**

- A request for a new, additional, or replacement card, or for the addition of authorized users on the account, shortly after receiving a notice of a change of address for a covered account, that the University receives.
- Use of a new revolving credit account in a manner commonly associated with known patterns of fraud patterns. For example:
  - a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash; or
  - b. The covered account holder fails to make the first payment or makes an initial payment but no subsequent payments.
- Use of a covered account in a manner that is not consistent with established patterns of activity on the account. 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
- Use of a covered account that has been inactive for a reasonably lengthy period of time (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
  - Circumstances where mail sent to the covered account holders is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account holders' covered account.
  - Circumstances where the University is notified that the covered account holder is not receiving paper account statements.
  - Circumstances where the University is notified of unauthorized charges or transactions in connection with a covered account holders' covered account.
  - Notice regarding possible identity theft in connection with covered accounts held by the University, including but not limited to:

Circumstances where Trinity University is notified by a covered account holder, 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.

#### **E. Detecting Red Flags**

In order to detect Red Flags in connection with the opening of covered accounts and existing covered accounts, it is the policy of Trinity University to:

- (1) Obtain identifying information about, and verify the identity of, a person opening a covered account, and
- (2) Authenticate covered account holders, monitor transactions, and verify the validity of change of address requests, in the case of existing covered accounts.

#### **F. Responding to Detected Red Flags**

Trinity University shall take appropriate responsive action to the Red Flags that the University has detected, commensurate with the degree of risk posed. In determining an appropriate response, the University shall consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a covered account holders' account records held by the University or notice that a covered account holder has provided information related to a covered account held by the University to someone fraudulently claiming to represent Trinity University or to a fraudulent website. Appropriate responses may include the following:

- Monitoring a covered account for evidence of identity theft;
- Contacting the covered account holder;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

**G. Administration & Oversight of the Program**

In order to comply with its obligations under FACTA, Trinity University shall:

1. Obtain approval of the initial written Program from the Executive Committee of the Trinity University Board of Trustees;
2. Involve the Office of Fiscal Affairs in the oversight, development, implementation and administration of the Program;
3. Train staff, as necessary, to effectively implement the Program; and
4. Exercise appropriate and effective oversight of service provider arrangements.

Appropriate and effective oversight of the Program shall include oversight by the by the Office of Fiscal Affairs that is:

- Assigned specific responsibility for the Program's implementation;
- Responsible for reviewing reports prepared by staff regarding compliance by Trinity University
- Approving material changes to the Program as necessary to address changing identity theft risks.

**H. Annual Report to the Board**

The staff of Trinity University who are responsible for development, implementation, and administration of its Program should report to the Board of Trustees, at least annually, on compliance by the University with this policy. The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the University in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider

arrangements; significant incidents involving identity theft and the University's response; and recommendations for material changes to the Program.

#### **I. Annual Assessment of Covered Accounts**

Trinity University shall annually determine whether it offers or maintains covered accounts. As a part of this determination, the University shall conduct a risk assessment to determine whether it offers or maintains covered accounts, taking into consideration:

1. The methods it provides to open its accounts;
2. The methods it provides to access its accounts; and
3. Its previous experiences with identity theft.

#### **J. Program Updates**

Trinity University shall update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to covered account holders or to the safety and soundness of the University from identity theft, based on factors such as:

- The experiences of the University with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that the University offers; and
- Changes in the business arrangements of the University, including changes in service provider arrangements.

---

### **III. POLICY ON CONTRACTORS & 3<sup>rd</sup> PARTY SERVICE PROVIDERS**

The Program shall exercise appropriate and effective oversight of service provider arrangements.

- A. It is the responsibility of Trinity University to ensure that the activities of all service providers and contractors are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
- B. A service provider or contractor that maintains its own Identity Theft Prevention Program, consistent with the guidance of the red flag rules (16 C.F.R. Part 681) and validated by appropriate due diligence, may be considered to be meeting these requirements.

- C. Any specific requirements should be specifically addressed in appropriate contract arrangements.
  - D. Contractors and service providers must notify Trinity University of any security incidents experienced, even if such incidents may not have led to any actual compromise of Trinity's data.
-