Identity Theft Prevention Program

(Red Flags Rule Regulation Response)

Policy owner: Vice-President of Business Affairs and Chief Financial Officer

Date of initial publication: October 2009
Date of latest revision: August 4, 2021

SECTION I. PURPOSE

The University of St. Thomas ("University") established its Identity Theft Prevention Program ("Program") in response to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. This Identity Theft Prevention Program and related procedures provide information to assist the University and individuals throughout the University in detecting, preventing, and mitigating identity theft involving accounts covered by the Rule. Additionally, this program provides guidance on appropriate responses and/or reporting for any red flags that are detected.

SECTION II. SCOPE AND APPLICABILITY

The expectations set forth in this policy and related procedures apply to all St. Thomas faculty and staff who, as part of their job duties, work with or have access to Covered Accounts.

SECTION III. DEFINITIONS

When used in this policy, the following terms have the following meanings:

a. **Identity theft** means fraud committed or attempted using the identifying information of another person without authority.

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

c. **Account** means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes. Accounts include services involving extension of credit, such as a deferred payment, or a deposit account.

d. **Covered Account** means: (a) a consumer account offered or maintained by the University that involves or is designed to permit multiple payments or transactions, such as a loan or account that is billed or payable in installments, and/or (b) an account offered or maintained by the University for which there is a reasonably foreseeable risk to customers or to the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

SECTION IV. Identity Theft Protection Program

A. Identity Theft Prevention Program

Faculty and staff who work with or have access to Covered Accounts are expected to comply with this policy and the related procedures for identifying, detecting and responding to red flags in connection with Covered Accounts. Appendix A contains procedures for identifying, detecting, and responding to red flags.

The program will be updated periodically to reflect changes in risks related to identity theft. This policy and its related procedures are determined to be appropriate to the size and complexity of the University and the nature and scope of University activities.

B. Covered Accounts Maintained by the University of St. Thomas

The following have been identified as accounts administered by the University (and/or service provider) that are Covered Accounts under the Rule:

- Participation in the Federal Perkins Loan Program
- Refund of credit balances, with/without PLUS loans
- Payment plans for student accounts
- Deferment of tuition payments
- Emergency loan funds
- Accounts for which credit reports are requested
- eXpress accounts
- COVID-19 Relief Payments
- Flexible Spending Accounts (FSAs)
- Health Savings Account (HSA)

C. Program Administration

The Vice-President of Business Affairs and Chief Financial Officer is responsible for oversight of the program and may assign specific responsibility for the program's implementation to appropriate University personnel. A committee, chaired by the Director of the Business Office, shall assist the Vice-President of Business Affairs and Chief Financial Officer with oversight, development, implementation, training, and review of the program. This committee will meet at least annually to address matters related to the program and evaluate issues, including the effectiveness of the policies and procedures, service provider arrangements, significant incidents, and recommended change to the program. The committee will create and provide to the Vice-President of Business Affairs and Chief Financial Officer a report addressing these issues. The Program (including the Red Flags determined to be relevant) will be updated periodically to reflect changes in risks to customers or to the safety and soundness of the University from identity theft. The Vice-President of Business Affairs and Chief Financial Officer will approve material changes to the Program as necessary to address changing identity theft risks.

D. Training

All employees who process any information related to Covered Accounts shall receive training following appointment on the procedures outlined in this document. Refresher training may be available periodically.

E. Oversight of Service Providers

Whenever the University engages a service provider to perform an activity in connection with one or more covered accounts the University will obtain a written agreement to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

Appendix A to
Identity Theft Prevention Program

Procedures for Identifying, Detecting, and Responding to Red Flags

Date of initial publication: October 2009
Date of latest revision: August 4, 2021

The following procedures have been adopted to help identify, detect, and respond appropriately to Red Flags.

SECTION I. Identifying Red Flags

The following red flags, listed by category, have been identified as relevant to the activities carried out by the University as related to Covered Accounts:

A. Alerts, Notifications and Warnings from Credit Reporting Agencies

- Report of fraud accompanying a credit report
- Notice or report from a credit agency of a credit freeze on an applicant/customer
- Notice or report from a credit agency of an active duty alert for an applicant/customer
- Receipt of a notice of address discrepancy in response to a credit report request
- Indication from a credit report of activity that is inconsistent with an applicant's/customer's usual pattern of activity, such as:
  - Recent and significant increase in volume of inquiries
  - Unusual number of recently established credit relationships
  - Material change in the use of credit, especially with respect to recently established credit relationships
  - An account closed for cause or identified for abuse of account privileges by a financial institution or creditor

B. Suspicious Documents

- Documents provided for identification appear to have been altered or forged
- The photograph or physical description on the identification is not consistent with the appearance of the applicant/customer presenting the identification
- Other information on the identification is not consistent with information provided by the person opening a new Covered Account or customer presenting identification
- Other information on the identification documentation is not consistent with readily accessible information currently on file for the applicant/customer
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled

C. Suspicious Personal Identifying information

- Personal identifying information provided is inconsistent when compared against external information sources (such as address does not match consumer report, SSN has not been issued or is on the SSA Death Master File)
- Personal identifying information provided by the applicant/customer is not consistent with other personal identifying information provided by the customer (for example, inconsistent birth dates)
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or external sources (for example, phone number or address given is known to be invalid or fictitious)
- The SSN, address, and/or phone number provided is the same as listed by another/multiple other applicants/customers
- The applicant/customer fails to provide all required personal identifying information as requested, especially after being reminded to do so
- Personal identifying information is not consistent with information on file with the University

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

- Change of address request shortly followed by a request from the applicant/customer for a name change or the addition of authorized users on the account
- Payments stop on an otherwise consistently up to date account
- Account used in a way inconsistent with prior use
- Mail sent to applicant/customer is repeatedly returned as undeliverable although transactions continue to be conducted in connection with the customer's covered account
- Notice is given to University that an applicant/customer is not receiving mail or e-mail sent by the University
- Notice to University that account has unauthorized activity
- Breach in the University's computer system security
- Unauthorized access to or use of covered account information

E. Alerts from Others Regarding Possible Identity Theft

- Notice to the University by an applicant/customer, victim of identity theft, a law enforcement authority, or any other person that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft

SECTION II. Detecting Red Flags

A. New and Existing Accounts

In order to detect any of the previously identified Red Flags, University personnel involved with either the opening of Covered Accounts and/or continuing transactions for existing Covered Accounts will:

- Obtain and verify identity of applicants/customers (including students)
- Review the authenticity of identifying documentation
- Require UST username and password or other identity verification to change billing address and provide applicants/customers a reasonable means of promptly reporting incorrect billing address changes

B. Credit Reports

In order to detect any of the previously identified Red Flags for Covered Accounts for an applicant/customer for which a credit or background report is sought, University personnel will take the following steps to assist in identifying address discrepancies:

- When address is different than address on file in Banner, 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
- In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant/customer for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate

SECTION III. Responding to Red Flags - Preventing and Mitigating Identity Theft

In the event University personnel detect any of the previously identified Red Flags, such personnel shall respond appropriately, which may include one or more of the following actions as appropriate:

- Review and monitor covered account for evidence of identity theft
- Contact the applicant/customer (including students)
- Change any passwords, security codes, or other devices that permit access to the covered account
- Do not open a new covered account
- Provide applicant/customer with new Banner identification number if needed
- Close an existing covered account
- Notify the Program Administrator for determination of appropriate response as necessary
- Notify law enforcement through the Public Safety Department as necessary
- Determine that no response is warranted under the particular circumstances
- Consider any aggravating factors that might heighten the risk of identity theft, such as a data security breach

The action(s) taken will depend on the particular facts and circumstances.