University of Minnesota

Identity Theft Prevention Program

Introduction

The Fair and Accurate Credit Transactions Act (FACTA) of 2003 directed the Federal Trade Commission (FTC) to issue regulations and guidelines regarding the duties of financial institutions and creditors with respect to the prevention of identity theft. In November 2007, the FTC issued a regulation commonly known as the Red Flags Rule ("Rule"). This regulation became effective December 31, 2010. The University must comply with the Red Flags Rule since it engages in activities subject to the regulation, such as issuing student loans and extending credit for purchases.

The Rule requires financial institutions and creditors that offer or maintain one or more covered accounts to develop and implement a written **Identity Theft Prevention Program** ("Program") designed to detect, prevent, and mitigate identity theft in connection with covered accounts. The Controller's Office has oversight for this Program. Guidance and training documents are available at the Controller's Office website or by contacting controller@umn.edu or (612) 624-1617.

Definitions

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. It includes:

(a) An extension of credit, such as the purchase of property or services involving a deferred payment, and
(b) A deposit account.

Covered Account means:

(a) An account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Examples include credit card accounts, checking or savings accounts, cell phone accounts and student loans.
(b) Any other account offered or maintained by the creditor for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Creditor means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew or continue credit.

Financial institution under Red Flags legislation is defined by activities rather than an organization's line of work. University departments or units are in-scope if they act as a bank or credit union, or hold a consumer transaction account from which a consumer can make payments or transfers to third parties.

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

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

University of Minnesota Identity Theft Prevention Program

The following is the University of Minnesota's official **Identity Theft Prevention Program**. This Program sets the framework for mitigating the risk of identity theft to the University's students, faculty, staff, and individuals who have an ongoing relationship in connection with a covered account provided by the University.

There are four main elements to the University's Identity Theft Prevention Program:

1. Identification of Red Flags.
2. Detection of Red Flags.
3. Response to Red Flags.
4. Program Review.

Each college or major administrative unit must assess the risks of identity theft associated with their day-to-day operations regarding covered accounts, and develop reasonable processes and procedures that include each of the above four elements. To the extent possible, the college or major administrative unit may incorporate existing policies and procedures that mitigate identified risks, and control reasonably foreseeable risks to customers and to the safety and soundness of the University. Examples of existing policies and procedures include:

- Practice Safe Computing
- Information Security
- Report Information Security Incidents
- Notification of an Information Security Breach
- Reporting and Notifying Individuals of Security Breaches

1. Identification of Red Flags

Red Flags are warning signs of possible identity theft. According to the Red Flags Rule, a red flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

In identifying relevant Red Flags for covered accounts, the following risk factors should be considered:

- The types of covered accounts offered or maintained,
- The provided methods to open a covered accounts,
- The provided methods to access covered accounts, and
- Previous experiences with identify theft.

When developing reasonable processes and procedures, the collegiate or administrative unit should incorporate relevant red flags from sources such as:

- The Red Flags Rule which provides twenty-six examples of Red Flags,
- Incidents of identity theft that the college, administrative unit, or University has experienced,
- Methods of identity theft that the college, administrative unit, or University has identified could reflect changes in their identity theft risks, and
- Any applicable supervisory guidance.

The college or major administrative unit should include relevant Red Flags from the following categories, as appropriate. These categories are derived from the FTC list of Red Flag examples.

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services,
- The presentation of suspicious documents,
- The presentation of suspicious personal identifying information, such as a suspicious address change,
- The unusual use of, or other suspicious activity related to, a covered account, and
- Notices from customers, victims of identity theft, law enforcement authorities, or other persons

regarding possible identity theft in connection with covered accounts held by the collegiate or administrative unit.

2. Detection of Red Flags

Each college or major administrative unit responsible for managing or maintaining covered accounts must establish processes and procedures to detect Red Flags in connection with opening or managing a covered account. The specific controls and procedures for detecting Red Flags may differ across University locations and departments. Examples of Red Flag detection controls and procedures may include (not a comprehensive list):

- Requiring the presentation of government-issued identification documents to verify identity.
- Comparing the information provided on an application for credit with information provided by a consumer reporting agency.
- Using credible references to validate information provided by an individual.

3. Response to Red Flags

Each college or major administrative unit responsible for managing or maintaining covered accounts must implement processes and procedures for appropriately responding to Red Flags that are detected. Responses should be commensurate with the degree of risk posed. Department size, location, constituent base, use of third party service providers, and other factors may affect risk levels. Additional aggravating factors that may heighten the risk of identity theft should be considered in determining an appropriate response. Examples of aggravating factors include a data security incident that results in unauthorized access to covered accounts, or notice of fraudulent activity related to a customer account. Examples of appropriate responses to Red Flag detection include:

- Monitor a covered account for evidence of identity theft.
- Contact the customer.
- Change any passwords, security codes, or other security devices that permit access to a covered account.
- Re-open a covered account with a new account number.
- Do not open a new covered account.
- Close an existing covered account.
- Do not attempt to collect on a covered account, or do not sell a covered account to a debt collector.
- Notify law enforcement.
- Determine that no response is warranted under the particular circumstances.

4. Program Review

Each college or major administrative unit must assess the risks of identity theft associated with their covered activities at least annually. This review should include an update to processes and procedures to reflect any changes in Red Flags, and risks to customers or to the University 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 or maintains.
- Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

The University's Identity Theft Prevention Program will be reviewed at least annually by the Controller's Office and updated as needed.

Special Duties of Card Issuers

Colleges or major administrative units that issue credit or debit cards (including declining balance accounts such as Gopher Gold or payroll deduct cards) must establish reasonable policies and procedures to assess the validity of a change of address.

When the college or major administrative unit receives notification of a change of address for a consumer's debit or credit card account, and within a short period of time afterward the card issuer receives a request for an additional or replacement card for the same account, the card issuer must not issue the card until the card issuer:

- Notifies the cardholder of the request at the cardholder's former address, or by another means of communication the card issuer and card holder have previously agreed to use, and
- Provides the cardholder with a reasonable means to promptly report the incorrect address change, or
- Assesses the validity of the change of address in accordance with policies and procedures established under the Red Flags Rule section of this Program.

Program Oversight Responsibilities

The Controller's Office is responsible for oversight of the Program. The Controller's Office will:

- Arrange for appropriate communication of the Program details to colleges and major administrative units.
- Provide basic training materials for colleges and major administrative units to use to train employees.
- Provide optional templates to assist colleges and major administrative units in completing processes and procedures.
- Maintain copies of annual compliance certification forms from colleges or major administrative units.
- Provide oversight of third-party service providers through Purchasing Services.
- Prepare an annual summary report for the President or the President's designee.
- Annually review the Program for potential changes.