

# **University of Connecticut**

## **IDENTITY THEFT PREVENTION PROGRAM**

- I. BACKGROUND**
- II. PURPOSE AND SCOPE**
- III. DEFINITIONS**
- IV. IDENTIFICATION & DETECTION OF RED FLAGS**
- V. APPROPRIATELY RESPONDING WHEN RED FLAGS ARE DETECTED**
- VI. CONSUMER REPORTS—ADDRESS VERIFICATION**
- VII. TRAINING**
- VIII. OVERSIGHT OF THIRD PARTY SERVICE PROVIDERS**
- IX. PROGRAM ADMINISTRATION**
- X. UPDATING THE PROGRAM**
- XI. BOARD APPROVAL**

## **BACKGROUND**

In response to the growing threats of identity theft in the United States, Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended a previous law, the Fair Credit Reporting Act (FCRA). This amendment to FCRA charged the Federal Trade Commission (FTC) and several other federal agencies with promulgating rules regarding identity theft. On November 7, 2007, the FTC, in conjunction with several other federal agencies, promulgated a set of final regulations known as the “Red Flags Rule”. The Red Flags Rule became effective November 1, 2008, however, the FTC has deferred its enforcement of the rule through May 1, 2009 in order to permit institutions additional time in which to develop and implement the written identity theft prevention programs required by the Red Flags Rule regulations.

The Red Flags Rule regulations require entities with accounts covered by the Red Flags Rule regulations, including universities, to develop and implement a written Identity Theft Prevention Program (hereinafter, the “Program” or the “Identity Theft Program”) for combating identity theft in connection with certain accounts. The Program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft and enable the entity with covered accounts to:

1. Identify relevant patterns, practices, and activities, dubbed “Red Flags”, signaling possible identity theft and incorporate those Red Flags into the Program;
2. Detect Red Flags;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
4. Ensure the program is updated periodically to reflect changes in risks.

This document outlines the required Red Flags Rule Program of the University of Connecticut, but is extended to encompass not just financial or credit accounts, but any University account or database for which the University believes there is a reasonably foreseeable risk to the University, its students, faculty, staff, patients, constituents or customers from identity theft.

## **II. PURPOSE AND SCOPE**

The purpose of this Program is to ensure the compliance of the University of Connecticut with the Red Flags Rule regulations, to identify risks associated with identity theft, and to mitigate the effects of identity theft upon the University, its employees, its students, its patients, its constituents and its customers.

The requirements of this Program apply to the University of Connecticut Storrs and Regional Campuses and the University of Connecticut Health Center (collectively, “UCONN”), to the employees of such campuses, and the third parties with whom UCONN contracts to perform certain functions on its behalf.

### III. DEFINITIONS

Account: Account means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

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

Covered Account: The Red Flags Regulations define the term “covered account” to mean (1) “an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions...” and (2) “any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers, or to the safety and soundness of the financial institution, or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.”

*For the purposes of the University’s Identity Theft Program, the term “covered account” is extended to include any University account or database (financially based or otherwise) for which the University believes there is a reasonably foreseeable risk to the University, its students, faculty, staff, patients, constituents or customers from identity theft.*

Credit: “Credit” means “the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.”

Creditor: “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: “Financial institution” means “a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer.”

Identity Theft: “Identity theft” means “fraud committed using the identifying information of another person.”

Red Flag: “Red Flag” means “a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”

Service Provider: “Service provider” means “a person that provides a service directly to the financial institution or creditor.”

Transaction Account: “Transaction account” means “a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. Such term includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.”

#### **IV. IDENTIFICATION & DETECTION OF RED FLAGS**

A “Red Flag” is a pattern, practice, or specific activity that indicates the possible existence of identity theft. The following Red Flags are potential indicators or warning signs of potential or actual identity theft or similar fraud. Any time a Red Flag, or a situation resembling a Red Flag, is apparent, it should be investigated for verification. The examples below are meant to be illustrative. Any time an employee suspects a fraud involving personal information about an individual or individuals, the employee should assume that this Identity Theft Program applies and follow protocols established by his/her office for investigating, reporting and mitigating identity theft.

##### **Examples of Red Flags:**

###### *Alerts, Notifications or Warnings from a Consumer Reporting Agency*

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy.
4. A consumer report indicates 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.

###### *Suspicious Documents*

5. Documents provided for identification appear to have been altered or forged.

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

***Suspicious Personal Identifying Information***

10. Personal identifying information provided is inconsistent when compared against external information sources used by the University. For example:
  - a. The address does not match any address in the consumer report; or
  - b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11. Personal identifying information provided by the customer 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.
12. Personal identifying information provided 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.
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the 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.
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided 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 customers.
16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the University.
18. The person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report (such as answers to “challenge questions”).

***Suspicious Account Activity or Unusual Use of Account***

19. Shortly following the notice of a change of address for a covered account, the University receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
20. A new revolving credit account is used 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 (e.g., electronics equipment or jewelry); or
  - b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, 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
  - e. A material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24. The University is notified that the customer is not receiving paper account statements.
25. The University is notified of unauthorized charges or transactions in connection with a customer's covered account.

***Alerts from Other***

26. The University is notified by a customer, 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.

**V. APPROPRIATELY RESPONDING TO DETECTED RED FLAGS**

Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the University from the effects of identity theft. The employee should inform his/her supervisor as soon as possible that he/she has detected an actual or potential Red Flag, or had identified a similar area of concern of identity theft. The supervisor should conduct any necessary inquiry to determine the validity of the Red Flag.

If it is determined that a situation of identity theft has occurred, the Division or Department Head should immediately contact the Office of Audit, Compliance & Ethics (OACE) to inform them of the matter so that the matter is properly documented as part of the monitoring portion of this Program.

If the Red Flag indicates that a fraudulent transaction has occurred, the Division or Department Head should ensure that appropriate actions to mitigate the effects of the transaction are taken immediately. Appropriate actions will be dependent on the type of Red Flag identified, type of transaction, relationship with the victim of the fraud, availability of contact information for the victim of the fraud, and numerous other factors. However, by way of example, appropriate actions may include, but are not limited to:

1. Canceling the transaction;
2. Not opening a new account or closing the account in question;
3. Notifying and cooperating with appropriate law enforcement;
4. Notifying the Office of the Attorney General, the OACE, and Senior Administration of the University; and/or
5. Utilizing the University's Security Breach Protocol and/or Security Breach Team by contacting the OACE;

6. Notifying the actual customer that fraud has been attempted or that it has occurred;
7. Changing any passwords or other security devices that permit access to relevant accounts and/or databases; and/or
8. Continuing to monitor the account or database for evidence of identity theft.
9. Alternatively, it may be determined that no response is warranted after appropriate evaluation and consideration of the particular circumstances.

In all situations where it is determined that a Red Flag has been positively identified, the office responsible for the account shall document what occurred, describe its review of the matter and any specific actions taken to mitigate the impact of the effects of the actual or potential identity theft discovered. Such documentation shall also include an description of any additional actions the office believes are systemically necessary within their office (such as updating policies and procedures) in response to identified Red Flag to handle or prevent similar situations in the future.

## **VI. CONSUMER REPORTS—ADDRESS VERIFICATION**

Any University office that obtains and/or uses consumer reports from a Consumer Reporting Agency must ensure that it has reasonable policies and procedures in place to enable the office to form a reasonable belief that the consumer report the office has obtained relates to the consumer about whom it requested the report when the office receives a notice of address discrepancy. A notice of address discrepancy means that the office has received notice of a substantial difference between the address(es) for the consumer that the office provided to request the consumer report and the address(es) in the office's file on the consumer.

The office may reasonably confirm the accuracy of the consumer's address by:

1. Verifying the address with the consumer about whom it as requested the report;
2. Reviewing its own records (e.g., job applications, change of address notification forms, other customer account records) to verify the address of the consumer;
3. Verifying the address through third-party sources; or
4. Using other reasonable means.

The office must provide the consumer's address that it has reasonably confirmed to be accurate 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.

## **VII. TRAINING**

Staff training is required for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the University or its customers.

The Division or Department Head of each office that maintains a covered account under this Program is responsible for ensuring that appropriate identity theft training for all requisite employees, officials and contractors occurs at least annually.

As part of the training, all requisite employees, officials and contractors should be informed of the contents of the University's Identity Theft Program, and be provided with access to a copy of this document. In addition, all requisite employees, official and contractors should be trained how to identify Red Flags, and what to do should he/she detect a Red Flag or have similar concerns regarding an actual or potential fraud involving personal information.

## **VIII. OVERSIGHT OF THIRD PARTY SERVICE PROVIDERS**

It is the responsibility of the University to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Before the University may engage a service provider to perform an activity in connection with one or more of the University's covered accounts, the University must take the following steps to ensure the service provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risks of identity theft:

1. The University must require by contract that the service provider has such policies and procedures in place; and
2. The University must require by contract that the service provider is aware of the University's Identity Theft Program, and will report any Red Flags it identifies as soon as possible to the OACE.

## **IX. PROGRAM ADMINISTRATION**

Successful implementation of the Identity Theft Program ultimately is the responsibility of each office, the employees of each office that maintains accounts or databases covered by this Program, and the University community as a whole. As permitted by the Red Flags Rule regulations, responsibility for overseeing the administration of the Program has been delegated by the Board of Trustees to the Vice President and Chief Financial Officer of the University, with compliance monitoring responsibility to be performed by the OACE. On an annual basis, and as part of the University's Compliance Monitoring Plan, the OACE will confer with the University offices that maintain covered accounts under the Program to review each office's list of covered accounts, training and policies, procedures and practices as they relate to preventing, detecting and mitigating identity theft, and any positively identified Red Flags or similar

incidents documented by the offices who maintain covered account under this Program. The OACE will create an annual report, based upon its annual conferences with the University offices that maintain covered accounts, assessing the effectiveness of the University's Identity Theft Program as a whole. As part of the report, the OACE will make recommendations for updating or modifying the Program as appropriate. The annual report will be provided by the OACE to the Vice President and Chief Financial Officer for his review and presentation to the Executive Compliance Committees and the Joint Audit & Compliance Committee of the Board of Trustees (JACC).

## **X. UPDATING THE PROGRAM**

On an annual basis, as part of the University's Compliance Monitoring Plan, the Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable. This review will include an assessment of which accounts and/or databases are covered by the program, whether additional Red Flags need to be identified as part of the Program, whether training has been implemented, whether training has been effective. In addition, the review will include an assessment of whether mitigating steps included in the program remain appropriate, and/or whether additional steps need to be defined.

## **XI. APPROVAL BY THE BOARD OF TRUSTEES**

Under the Red Flags Regulations, implementation and oversight of the Identity Theft Program is the responsibility of the governing body or an appropriate committee of such governing body. Approval of the initial plan must be appropriately documented and maintained. After its initial approval of the Program, however, the governing body may delegate its responsibility to implement and oversee the Identity Theft Program. As the governing body of the University of Connecticut, the Board of Trustees, through its JACC, as of the date below, hereby approved the initial Identity Theft Program. Having made such initial approval, the Board of Trustees hereby delegates the responsibility for implementing, monitoring and overseeing the University's Identity Theft Program to the Vice President and Chief Financial Officer.

Approved by the Joint Audit & Compliance Committee of the Board of Trustees: April 2, 2009