Westfield State University
Policy concerning:

Section Administrative
number 0540
page 1 of 5

APPROVED: December 2010 REVIEWED:

# IDENTITY THEFT PREVENTION

## PURPOSE

Westfield State University (University) has adopted this initial Identity Theft Prevention Program (Program) in compliance with the Red Flag rules issued by the Federal Trade Commission pursuant to the Fair and Accurate Credit Transactions ACT (“FACTA”). The University is engaging in activities which are covered by the FACTA Red Flag rules. After consideration of the size and complexity of the University’s operations and account systems, and the nature and scope of the University’s activities, the Board has determined that this Program is appropriate for the University.

Under the Red Flag rules, the University is required to establish an “Identity Theft Prevention Program” with reasonable policies and procedures to detect, identify, and mitigate identity theft in its covered accounts. The University must incorporate relevant Red Flags into a Program to enable the University to detect and respond to potential identity theft. The University shall ensure that the Program is updated periodically to reflect changes in risks to customers or creditors or the University from identity theft.

## POLICY

- **RESPONSIBLE UNIVERSITY OFFICIAL**

  The President shall designate a senior University official to serve as Program Administrator. The Program Administrator shall exercise appropriate and effective oversight over the Program and shall report regularly to the President on the Program.

- **ADMINISTRATION AND MAINTENANCE**

  The Program Administrator is responsible for developing, implementing, and updating the Program throughout the University. The Program Administrator will be responsible for: coordinating appropriate training of University staff on the Program; advising on appropriate procedures to follow for identifying, preventing, and mitigating identity theft; determining which steps of prevention and mitigation should be taken under particular circumstances; serve as facilitator and advisor on incidences of identity theft and coordinate any reporting requirements, as necessary; and recommending to the President periodic changes to the Program.

  The Program will be periodically reviewed and updated to reflect changes in identity theft risks and technological changes. The Program Administrator will consider the University’s experiences with identity theft, changes in identity theft methods; changes in identity theft detection, mitigation and prevention methods; changes in types of accounts the University maintains; changes in the University’s business arrangements with other entities, and any changes in legal requirements in the area of identity theft. After considering these and other factors, the Program Administrator will determine whether changes to the Program are warranted.

  The Program Administrator shall confer with all appropriate University personnel and knowledgeable experts in the area of privacy issues as necessary to ensure compliance and maintenance of an effective program. The Program Administrator shall annually report to the President on the effectiveness of the Program. The Program Administrator shall present any recommended changes to the President for approval. The President’s approval shall be sufficient to make changes to the University’s Identity Theft Program.

- **DEFINITIONS**

Pursuant to the Red Flag regulations at 16 C. F. R. § 681.2, the following definitions shall apply to this Program:

*Identity Theft:*
A fraud committed using the identifying information of another person without authority.

*Red Flag:*
A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

*Covered accounts*:
1. Any account the University offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions.
2. Any other account the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from Identity Theft.

*Credit*:
The right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefore.

*Creditor:*
An entity that regularly extends, renews, or continues credit.

*Customer:*
Any person with a covered account with a creditor.

*Identifying information:*
Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including:
Name
Address
Telephone number
Social security number
Date of birth
Government issued driver's license or identification number
Alien registration number
Government passport number
Employer or taxpayer identification number
Unique electronic identification number
Computer's Internet Protocol address or routing code

- **IDENTIFICATION OF RED FLAGS**

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. The following are examples of relevant Red Flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

*A. 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 a customer or applicant;
- Notice or report from a credit agency of an active duty alert for an applicant; and

- Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

*B. Suspicious Documents*

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with existing customer information (such as is a person's signature on a check appears forged); and
- Application for service that appears to have been altered or forged.

*C. Suspicious Personal Identifying Information*

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- Social security number presented that is the same as one given by another customer;
- An address or phone number presented that is the same as that of another person;
- A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
- A person's identifying information is not consistent with the information that is on file for the customer.

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

- Change of address for an account followed by a request to change the account holder's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use (example: very high activity);
- Mail sent to the account holder is repeatedly returned as undeliverable;
- Notice to the University that a customer is not receiving mail sent by the University;
- Notice to the University that an account has unauthorized activity;
- Breach in the University's computer system security; and
- Unauthorized access to or use of customer account information.

*E. Alerts from Others*

- Notice to the University form a customer, identity theft victim, law enforcement or other person that is has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

- **DETECTING RED FLAGS**

The program is also designed to detect Red Flags relevant to each type of covered account as follows:

*A. New Accounts*
In Order to detect any of the Red Flags identified above associated with the opening of a new account, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

- Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;
- Verify the customer's identity (for instance, review a driver's license or other identification card);
- Independently contact the customer.

*B. Existing Accounts*
In order to detect any of the Red Flags identified above for existing accounts, University personnel will take the following steps to monitor transactions with an account:

- Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
- Verify the validity of requests to change billing addresses; and
- Verify changes in banking information given for billing and payment purposes.

- **RESPONDING TO RED FLAGS AND MITIGATING IDENTITY THEFT**

In the event University personnel detect any identified Red Flags, such personnel shall take prescribed steps to respond and mitigate identity theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to the following examples:

- Continue to monitor an account for evidence of identity theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account
- Reopen an account with a new number;
- Notify law enforcement; or
- Determine that no response is warranted under the particular circumstances.

- **STAFF TRAINING AND AWARENESS PROGRAM**

  An integral part of the Program entails initial and continual training and awareness of university staff to potential incidences of identity theft. To this end, University employees responsible for implementing the Program shall be trained under a university sponsored awareness and training program coordinated with departmental staff, the Office of Human Resources and the Program Administrator on the detection of Red Flags, and the responsive steps to be taken when a Red Flag activity is detected.

- **REPORTING**

  Appropriate staff and/or supervisors shall provide reports to the Program Administrator on incidents of identity theft and actions taken to mitigate any risks associated with Red Flag activity. A separate “Privacy Incident Report” form has been developed to facilitate and standardize this reporting. This reporting mechanism will be communicated to all responsible employees and will also be located on the University’s web site.

- **SERVICE PROVIDER ARRANGEMENTS**

  In the event the University engages a service provider to perform an activity in connection with one or more accounts, the University 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, by contract, that service providers review the University’s Program and report any Red Flags to the Program Administrator.

- **REPORTING RQUIREMENTS TO THE BOARD OF TRUSTEES**

  After initial approval of this policy by the Board of Trustees, the President will advise the Board on a periodic basis on the continued compliance of this policy and from time to time bring appropriate recommendations to the Board for their consideration, review and revisions to this policy, as necessary.

## REVIEW

This policy shall be reviewed annually be the Vice President, Administration and Finance.