TITLE: Identity Theft Prevention Program

ORIGINATOR: Vice President for Finance and Administration

APPROVAL DATE: February 8, 2010

EFFECTIVE DATE: February 8, 2010

PURPOSE: This policy outlines the requirements for complying with the Fair and Accurate Credit Transaction Act of 2003 to prevent, mitigate and respond to Identity Theft. This policy applies to all "Covered Accounts" and University departments which defer payments, allow multiple payments over time, or who utilize credit reports for employment or credit decisions.

REVIEWER: Comptroller

REVIEW DATE: November 2024 and every 5 years thereafter

OPERATING DETAILS:

DEFINITIONS:

A **covered account** is defined as a consumer account that involves multiple payments or transactions, such as a loan that is billed or payable monthly. Covered accounts include arrangements in which a "continuing relationship" is established by billing for previous services rendered. A covered account is also an account for which there is a foreseeable risk of identity theft. For the purpose of this program, covered accounts shall include, but not be limited to (1) Accounts Receivable Accounts and (2) Perkins Loan accounts. Within the scope of this policy, the Comptroller is charged with the responsibility to continuously monitor for the possibility that other accounts should be incorporated into this policy as covered accounts. Procedures will be modified as necessary, and appropriate University personnel notified of their responsibilities under the Program.

Identity Theft means a fraud committed using the identifying information of another person.

Red Flag means a pattern, practice, or specific activity that indicates the possible risk of identity theft. Institutions are to identify Red Flags in order to alert appropriate management, and to intervene against the possibility of such attempts.

POLICY:

It is the policy of Mississippi University for Women that specific steps will be taken to:

1. **Identify relevant red flags.** Appropriate university personnel as described in the scope statement above will identify specific red flag risks that may occur in their area of responsibility.

2. **Detect red flags.** Appropriate university personnel will define relevant procedures that would likely detect the occurrence of a red flag risk in their respective day-to-day operations.
3. **Prevent and mitigate identity theft.** Procedures are defined within this policy statement to describe the actions that will be taken to mitigate the harm.
4. **Update the Program.** Each area will continuously monitor their procedures to insure that risks have been identified and addressed. If a new risk should be discovered, steps will be taken to incorporate the new risk into procedural documentation in order to monitor for future occurrences.
5. Each University department that manages data associated with covered accounts is responsible for insuring their respective staffs are aware of the “Red Flags Program” and are trained to identify and detect red flag occurrences. Procedures will be on file in each department that manages this data.