IDENTITY THEFT PREVENTION PROGRAM FOR CONSUMER ACCOUNTS

PURPOSE:

In November 2007, final rules implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 were issued by the Federal Trade Commission ("FTC"), the federal bank regulatory agencies, and the National Credit Union Administration ("NCUA"). A joint notice of final rulemaking was published in the Federal Register (72 FR 63718) finalizing *the Identity Theft Red Flags Rule* ("the Rule"). The Rule was issued with the underlying goal of detecting, preventing, and mitigating identity theft "in connection with the opening of certain accounts or existing accounts," referred to as "*covered accounts*." 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. Red Flags are defined by the Rule as those events which should alert an organization that there is a risk of identity theft against a covered account. Institutions are to identify Red Flags in order to alert appropriate management, and to intervene against the possibility of such attempts.

SCOPE:

This program will apply to all university personnel who set-up, modify, or process transactions in covered accounts. 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 Controller and Treasurer's Office 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.

POLICY:

It is the policy of Mississippi State University 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.

PROCEDURE:

Identification and Detection of Red Flags:

- Verify identity of person requesting service, or in the case of Perkins Loan, the person signing the promissory note. Compare picture ID, or use alternative means of identification (e.g. driver's license).
- Examine documentation presented to insure it is not altered or forged
- Observe documentation presented, and note any inconsistencies with data already available in the University database
- Examine personal identifying information provided for inconsistencies with information on record
- Verify personal identifying information provided to insure it is not actually associated with another person, or customer
- Observe account activity for transactions that are inconsistent with established patterns
- Investigate postal mail that is repeatedly returned as undeliverable even though activity continues on the account
- Investigate any notices received regarding unauthorized transactions on the account

Program Administration

- 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.
- While each red flag occurrence would not necessarily be a case of identity theft, each case should be examined carefully by the department to determine the level of risk. Any occurrence determined to be of high risk should be reported to the Controller and Treasurer's Office. The Controller and Treasurer's Office will review the case specifics and make a determination for appropriate corrective action. These actions might include involving the Police Department and/or the Office of Internal Audit if some form of investigation, or prosecution, is warranted.

- Each department should continuously review their operations in order to identify new types of red flag occurrences that have not been previously identified within this policy. Any new red flag occurrences should be reported to the Controller and Treasurer's Office.

REVIEW:

This policy will be reviewed as needed by the University Controller and Treasurer with any modifications submitted to the Vice President for Finance and Administration.

RECOMMENDED BY:

/s/ Kevin Edelblute — 05-06-09
Kevin Edelblute — Date
Controller and Treasurer

/s/ Wayne Bland — 05-06-09
Wayne Bland — Date
Associate Vice President for Finance and Administration

/s/ Michael J. McGrevey — 05-18-09
Michael J. McGrevey — Date
Vice President for Finance and Administration

REVIEWED BY:

/s/ Don Zant — 05-19-09
Don Zant — Date
Director of Internal Audit

/s/ Charles L. Guest — 05-26-09
Charles L. Guest — Date
General Counsel

APPROVED BY:

/s/ Mark E. Keenum — 06-03-09
Mark E. Keenum — Date
President