The University of Memphis

POLICIES

BF4013 - Red Flag Policy

Issued: February 24, 2017

Responsible Official: Executive Vice President and Chief Operating and Financial Officer

Responsible Office: Business and Finance

Policy Statement

Background

The risk to the University of Memphis, its faculty, staff, students and other applicable constituents from data loss and identity theft is of significant concern to the University, and the University will make reasonable efforts to detect, prevent, and mitigate identity theft.

Purpose

The purpose of this policy is to assist employees in identifying, detecting and responding to patterns, practices and/or specific activities known as red flags that could indicate identify theft.

Contents

Definitions

- **Covered Account**
- **Identifying information**
- **Identity theft**
- **Red flag**

- **Procedures**

- **Identifying Red Flags**
- **Responding to Red Flags**
- **Protecting Personal Information**
- **Program Administration**

- **Links**
  - **Related Policies and Procedures**

	Definitions
Covered Account	1. Any account that involves or is designated to permit multiple payments or transactions; or 2. Any other account maintained by the University for which there is a reasonably foreseeable risk of identity theft to students, faculty, staff or other applicable constituents, or for which there is a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation or litigation risks.
Identifying information	Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to: 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, student identification number, computer Internet Protocol address or routing code, credit card number or other credit card information.
Identity theft	A fraud committed or attempted 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.

	Procedures
Identifying Red Flags	The University's Red Flag Plan addresses the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by: 1. Obtaining identifying information about, and verifying the identity of a person. For example, requiring persons

to show a valid photo ID or other proof of identity for any person conducting business with the University when opening a covered account and with existing accounts.
2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing accounts.

The following examples of red flags are potential indicators of fraud or identity theft. The risk factors for identifying relevant red flags include the types of covered accounts offered or maintained; the methods provided to open or access covered accounts; and, previous experience with identity theft. Any time a red flag or a situation closely resembling a red flag is apparent, it should be investigated for verification. Some examples are:

1. **Alerts, notifications or warnings from a credit or consumer reporting agency.**
2. **Suspicious documents.**
3. **Suspicious personal identifying information.**
4. **Unusual use of, or suspicious activity related to, the covered account.**

Responding to Red Flags

Once a red flag or potential red flag is detected, the employee must act quickly with consideration of the risk posed by the red flag. The employee detecting the red flag must gather all related documentation, write a description of the situation and present this information to the Program Administrator for determination. The Program Administrator will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

Protecting Personal Information

Employees should review on an annual basis the University's Red Flag Plan. University personnel are also encouraged to use good judgment in securing covered account information. Furthermore, employees should review AA3022 Privacy of Education Records, IT6005 Data Security Policy, the Tennessee Public Records Act, and other applicable laws and policies. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor. The Program Administrator may also be contacted for further advice.

Program Administration

Oversight and Appointment of the Institutional Program Administrator

Operational responsibility of the program at the University is delegated to a Program Administrator appointed by the President. The duties of the Program Administrator shall include but not be limited to the oversight, development, implementation and administration of the program; approval and implementation of needed changes to the program; and staff training. The Program Administrator is also responsible for ensuring that appropriate steps are taken for preventing and mitigating identity theft, for reviewing any staff reports regarding the detection of red flags, and for determining which steps should be taken in particular circumstances when red flags are suspected or detected.

The Program Administrator will compile an annual report concerning institutional compliance with and effectiveness of the program. This report should address service provider arrangements, the effectiveness of the program in addressing the risk and identifying red flags; significant incidents of red flags and the University's response; and, any recommendations for material changes to the program.

Staff Training

Staff training shall be conducted for all employees who may come into contact with covered accounts or identifying information, as determined by the Program Administrator.

Periodic Updates to the Program

At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable. Consideration will be given to the University's experiences with identity theft situations; changes in identity theft methods, detection methods or prevention methods; and, changes in the University's business arrangements with other entities.

Periodic reviews will include an assessment of which accounts are covered by the program. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate. Actions to take in the event that

fraudulent activity is suspected or discovered may also require revision to the program.

Overview of Service Provider Arrangements

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 designated to detect, prevent, and mitigate the risk of identity theft. In the event the University engages a service provider to perform an activity in connection with one or more covered accounts, the University will take 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.

Links

Related Policies and Procedures

Red Flag Plan

IT6005 - Data Security Policy

AA3022 - Privacy of Education Records (Compliance with FERPA)

HR5064 - Employee Personnel Records

Revision Dates

BF4013 - Revised March 28, 2018
UM1714 - Revised February 24, 2017
UM1714 - Issued: February 5, 2013

Subject Areas:

Academic	Finance	General	Human Resources	Information Technology	Research	Student Affairs
☐	☒	☒	☐	☐	☐	☐