**SECTION: General Information** **Number: 01.03.04**
**AREA: University-wide Business Management**

# SUBJECT: Identity Theft

I. PURPOSE AND SCOPE

In accordance with System Administrative Memorandum (SAM) 01.C.14, this document establishes the guidelines for an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with covered accounts and to provide continued administration of the Program in compliance with the Federal Trade Commission's (FTC) Red Flags Rule, which implements Sections 114 and 315 of the Fair and Accurate Credit Transaction Act of 2003.

II. POLICY

Departments with covered accounts will develop procedures tailored to the size, complexity and nature of its operation designed to detect, prevent and mitigate identity theft in accordance with this policy.

III. DEFINITIONS

A. Identity Theft – A fraud committed or attempted using the identifying information of another person without authority.

B. Red Flag – A pattern, practice, or specific activity that indicates the possible existence of identity theft.

C. Covered Account – An account that the university offers or maintains primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.

D. Program – For purpose of this MAPP, refers to the Identity Theft Prevention Program.

E. Program Administrator – The individual designated with primary responsibility for oversight of the Identity Theft Prevention Program.

F. 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, student identification number, computer's Internet Protocol address, or routing code.

IV. FULFILLING REQUIREMENTS FOR RED FLAGS RULE

The university has established this Program taking into consideration its size, complexity and the nature of its operation. The Program contains reasonable policies and procedures to:

A. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the Program;

B. Detect red flags that have been incorporated into the Program;

C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

D. Ensure the Program is updated periodically to reflect changes in risks to customers with covered accounts or to the safety and soundness of the covered accounts from identity theft.

V. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the university considered the types of covered accounts that it offers and maintains, methods it provides to open its covered accounts, methods it provides to access its covered accounts, and its previous experiences with identity theft. The university identified red flags in each of the following categories:

A. Notifications and Warnings from Credit Reporting Agencies

B. Suspicious Documents

C. Suspicious Personal Identifying Information

D. Suspicious Covered Account Activity or Unusual Use of Account

E. Alerts from Others

Note: Detailed information about the identification of red flags is not included in this MAPP for security reasons, but it is provided to those departments that are determined to have covered accounts.

VI. DETECTING RED FLAGS

A. New Covered Accounts

In order to detect red flags associated with the opening of a new covered account, department personnel responsible for issuing official university identification badges or opening and managing a covered account will verify the identity of the person obtaining the identification badge or opening the account by requiring certain identifying information such as name, telephone number, date of birth, home address, social security number (student ID for students), driver's license or other government-issued photo, and/or other identification depending on the operational unit's needs.

B. Existing Covered Accounts

In order to detect red flags for an existing covered account, university personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of a person if they request information whether in person, via telephone, facsimile, or e-mail;

2. Verify the validity of requests to change billing addresses by mail or e-mail and provide the person a reasonable means of promptly reporting incorrect billing address changes; and

3. Verify changes in banking information given for billing and payment purposes.

C. Consumer Credit Report Requests

In order to detect red flags for an employment or volunteer position for which a credit or background report is sought, university personnel will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report or background check is made; and

2. In the event that notice of an address discrepancy is received, verify that the credit report or background check pertains to the applicant for whom the requested report was made and report to the consumer reporting agency, if applicable, an address for the applicant that the university has reasonably confirmed is accurate.

## VII. PREVENTING AND MITIGATING IDENTITY THEFT

In the event university personnel detect any identified red flags, such personnel shall take one or more of the following steps, commensurate with the degree of risk posed by the red flag:

A. Prevent and Mitigate

1. Continue to monitor a covered account for evidence of identity theft;

2. Contact the customer or applicant (for which a credit report or background check was run);

3. Change any passwords or other security devices that permit access to covered accounts;

4. Not open a new covered account;

5. Close an account or provide the customer with a new account number;

6. Notify your immediate supervisor;

7. Notify the Program Administrator for determination of the appropriate step(s) to take;

8. Notify the UH Department of Public Safety (UHDPS);

9. File or assist in filing a suspicious activities report;

10. Not attempt or cease to collect, sell, or assign a covered account; or

11. Determine that no response is warranted under the particular circumstances.

B. Protect Student Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the university will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its web site is secure or provide clear notice that the web site is not secure;

2. Ensure complete and secure destruction of paper documents and computer files containing customer account information when a decision has been made to no longer maintain such information;

3. Ensure that office computers with access to covered account information are password protected;

4. Avoid use of social security numbers;

5. Ensure computer virus protection is up to date; and

6. Require and keep only the kinds of customer account information that are necessary for university purposes.

VIII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating the Program lies with the Program Administrator. The Program Administrator will be responsible for ensuring appropriate training of university staff on the Program, for reviewing any staff reports regarding the detection of red flags and the steps for preventing and mitigating identity theft, advising departments about which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program.

B. Staff Training

Information regarding the prevention, detection, and mitigation of identity theft will be included in an annual Red Flag Rules training for department representatives with covered accounts. In addition, each affected department must provide department-specific procedures for the prevention, detection, and mitigation of identity theft to the appropriate employees within the department, and any updates to those procedures, as needed.

C. Annual Reports

The Program Administrator will provide an annual report to the System Compliance Officer, which summarizes significant incidents involving identity theft and management's response, effectiveness of policies, and recommendations for material changes to the Program.

D. Service Provider Arrangements

In the event a department engages a service provider to perform an activity in connection with one or more covered accounts, the department 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 to perform its activities in compliance with Sections 114 and 315, as applicable, of the Fair and Accurate Credit Transaction Act of 2003; and

2. Require, by contract, that service providers report any suspected instances of actual or attempted identity theft to the department employee with primary oversight of the service provider relationship.

IX. REVIEW AND RESPONSIBILITY

Responsible Party: Associate Vice President for Finance

Review: Every five years

X. APPROVAL

*/Raymond Bartlett/*
Senior Vice President for Administration and Finance

*/Renu Khator/*
President

Date of President's Approval: July 30, 2021