UNIVERSITY OF HOUSTON SYSTEM
ADMINISTRATIVE MEMORANDUM

SECTION: General Administration **NUMBER: 01.C.14**

AREA: Risk Management

SUBJECT: Identity Theft

---

1. PURPOSE

This policy establishes an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with a covered account 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.

2. POLICY

Each component university shall develop policies and procedures to implement an Identity Theft Prevention Program tailored to its size, complexity and nature of its operation designed to detect, prevent and mitigate identity theft in accordance with Sections 114 and 315 of the Fair and Accurate Credit Transaction Act of 2003.

3. DEFINITIONS

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

3.2. Red Flag – A pattern, practice, or specific activity that indicates the possible existence of identity theft. Examples of Red Flags include: alerts, notifications or warnings from a consumer reporting agency, suspicious documents, suspicious personal identifying information, unusual use of or suspicious activity related to the covered account or notice from customers, victims of identify theft, law enforcement authorities or other persons regarding possible identify theft in connection with covered accounts held by the institution.

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

3.4. Program – For purpose of this SAM, this refers to the component university's Identity Theft Prevention Program.

3.5. Program Administrator – The component university individual designated with primary responsibility for oversight of the Program.

4. PROCEDURAL REQUIREMENTS

Each component university's Program must contain reasonable policies and procedures to:

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

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

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

4.4. 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;

4.5. Provide annual staff training on the prevention, detection, and mitigation of identity theft;

4.6. Provide annual updates on the Program to the System Compliance Officer; and

4.7. Contractually require service providers of covered accounts to perform their activities in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

5. REVIEW AND RESPONSIBILITY

Responsible Party: Associate Vice Chancellor for Finance

Review: Every two years on or before June 1

6. APPROVAL

Approved: ~~Carl P. Carlucci~~
~~Executive~~ Interim Vice Chancellor for Administration and Finance

~~Renu Khator~~
Chancellor

Date: ~~November 5, 2012~~

REVISION LOG

Revision Number	Approval Date	Description of Changes
1	01/13/2010	Initial version
2	11/05/2012	Applied revised SAM template and added new Revision Log. No additional changes were required via the Subject Matter Expert (SME)
3	TBD	