

**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 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 identity 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 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 university's Identity Theft Prevention Program.
- 3.5. Program Administrator – The university individual designated with primary responsibility for oversight of the Program.

