Title: **Identity Theft Prevention & Red Flags Policy**	**Policy Category:** **Risk Management & Security**
Issuing Authority: **Administration & Finance**	**Responsibility:** **Administration & Finance**
Publication Date: **11/18/2022**	**Next Review Date:** **11/18/2025**

Policy Statement/Background:

The Federal Trade Commission (FTC) Red Flags Rule (16 C.F.R. Part 681), as pursuant to the Fair and Accurate Credit Transactions Act (FACTA) and Red Flag Program Clarification Act of 2010, requires financial institutions and creditors to execute policies, procedures, and plans to identify, detect and respond to and thwart those who attempt to steal and use identity information. Additionally, the Red Flags Rule requires Stony Brook University to develop, implement, and administer an identity theft program.

Scope

This policy applies to all University entities and employees, students, contractors, service providers, and volunteers who have access to Covered Account information. This policy is intended to compliment the Hospital's Identity Theft Prevention, Detection, and Mitigation: Red Flag Alert policy.

Policy:

The University has established an Identity Theft Prevention Program ("Program"). The Program is charged with detecting "Red Flags" of identity theft with respect to University Covered Accounts. The Program shall include reasonable policies and procedures in order to:

- Identify relevant Red Flags of identity theft that may occur in day-to-day operations, as it relates to Covered Accounts;
- Detect Red Flags that have been identified by the Program;

- Respond appropriately to Red Flags that are detected; &
- Detail how periodic updates to the Program will take place, in order to reflect changes in risks.

The Program is administered centrally by the Office of Administration & Finance. The Program's components include:

A. Identifying Relevant Red Flags

Departments will identify the Red Flags associated with their Covered Accounts, taking into consideration: the types of accounts offered or maintained; the methods provided to open and access accounts; and previous experiences with identity theft. The following types of notices, documents, personal information, and activities may be indicators or Red Flags that an individual's identity may be compromised:

- Suspicious documents
- Suspicious personal identifying information
- Unusual use of or suspicious activity related to a Covered Account
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts
- Alerts, notifications, or warnings from a consumer reporting agency
- Compromised systems

B. Detecting Red Flags

Departments should develop and implement procedures to detect Red Flags associated with opening new or accessing existing Covered Accounts, such as by:

- Monitoring account transactions for possible Red Flags; require certain identity information such as name, date of birth, residential or business address, driver’s license, or other photo identification
- Requiring multi-factor identification before conducting any transaction over the phone that relates to a Covered Account
- Requiring that online transactions come through a secure, password protected portal
- Thoroughly following-up on each billing inquiry, especially inquiries regarding services not received and/or billing errors
- Verifying the validity of a change of address request on an existing account and provide the customer with a means to promptly report an incorrect address

C. Responding to Red Flags

Departments should respond appropriately to detected Red Flags in order to prevent and mitigate identity theft. The response should be commensurate with the degree of risk posed.

Once potentially fraudulent activity is detected, employees must act quickly, as a rapid response can protect customers and the University from damages and loss. If Red Flags are detected, one or more of the following steps may be taken:

- Monitor the Covered Accounts for evidence of identity theft
- Request additional documentation to validate identity
- Contact the customer and verify if the activity is fraudulent
- Disable access or change passwords, security codes, or other security devices that permit access to a Covered Account (where appropriate)
- Close the Covered Account, and if needed reopen with a new account number
- Refuse to open a new Covered Account for the customer
- Notify the Office of Administration & Finance and/or the University Police Department
- Other responses as determined by the Department
- Determine that no response is warranted under the particular circumstances

D. Updating the Program

The Program and associated department Red Flags procedures will be periodically evaluated. The Office of Administration & Finance, in collaboration with other divisions, will monitor changes in legal requirements in the area of identity theft to determine if changes in the University's Program are warranted. Departments will review their Red Flags procedures annually and consider making revisions based on factors that may include:

- Experiences with identity theft incidents or identity theft attempts
- Changes in identity theft methods
- New procedures for detecting, mitigating, and preventing identity theft
- Changes in the types of Covered Accounts maintained by the Department
- Changes in business and service provider arrangements

Documentation reviews must be maintained at the Department level, in accordance with the University's Records Retention and Disposition Policy.

Definitions:

Covered Accounts: for the purposes of this policy, a Covered Account means: (i) an account that receives multiple payments or transactions, deferred payments, extensions of credit, loans, or which establishes a continuing relationship with an individual who has received services from the University (e.g., student accounts, tuition payment plans, non-hospital patient accounts, accounts associated with student lending activity, debit cards for use at off-campus vendors), and (ii) any other new or existing account that may pose a reasonably foreseeable risk to consumers or the institution from identity theft due to information retained and/or maintained by the institution. This includes single transaction, one-time payment accounts or records that may be vulnerable to identity theft because of the information collected and retained such as: date of birth, copies of checks, credit card numbers, social security number, and other personal identifying information.

Identity Theft: any use or attempt by an individual to use another person's identifying information (e.g.: name, social security number, date of birth, etc.) to obtain a thing of value to which the individual is not entitled to, including, but not limited to: money, credit, goods, or services such as education or medical care.

Red Flags: suspicious patterns or practices, or specific activities that indicate the possibility of identity theft.

Service Provider: contractor engaged by the University to perform an activity in connection with a Covered Account.

Contact:

Additional information about this policy is available here:

Jeffrey Mackey
Director for Finance Policy, Compliance and Internal/System Controls
Stony Brook Union, Suite 207-06
Stony Brook, NY 11794
(631) 632-9583
Financepolicyandcompliance@stonybrook.edu

Relevant Standards, Codes, Rules, Regulations, Statutes and Policies:

- Federal Trade Commission Red Flags Rule (16 CFR Part 681)
- Cyber Incident Response Policy
- Records Retention and Disposition Policy