Policy Name:
Identity Theft Fraud Prevention Program (Red Flag Rules)

Policy:
The University of Maryland, Baltimore will comply with the Identity Theft Fraud Prevention Program mandated by the Federal Trade Commission’s Fair and Accurate Credit Transactions Act (FACT Act), which amended the Fair Credit Reporting Act (FCRA), also known as the Red Flags Rule regulation under sections 114 and 315 of the FACT Act. This mandate requires financial institutions and creditors that hold covered accounts to develop and implement an identity theft prevention program for new and existing accounts. Institutions of higher education, whose fiscal operations fall within the Red Flags Rule, are mandated to identify, detect, prevent and mitigate instances of identity theft.

Definitions and Terms:
A. “Red Flags Rule Identity Theft Fraud Prevention Program”: The administrative, technical, or physical safeguards the University uses to identify, detect, prevent and mitigate instances of identity theft, as required under the Federal Trade Commission’s FACT Act and the Red Flags Rule regulations.

B. “Financial Institution”: A state/national bank, savings & loan association, mutual savings bank, state/federal credit union or any other entity that directly or indirectly holds a transaction account belonging to a customer.

C. “Creditor”: Federal law defines a creditor as an entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Where non-profit and government entities defer payment for goods or services, they are considered creditors. The federal law also includes any entity that defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month. For example, the University falls within the definition of creditor by participation [i] in the Federal Perkins Loan Program, [ii] in offering institutional loans to students, faculty or staff and [iii] in offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester.

D. “Covered Accounts”: A consumer account that involves multiple payments or transactions, such as a loan that is billed or payable monthly. This would include any type of account or payment plan that involves multiple transactions or multiple payments in arrears, including payroll deduction accounts. A covered account is also any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. Examples include small business accounts, sole proprietorship accounts, or single transaction consumer...
administration and Finance

accounts that may be vulnerable to identity theft.

E. “Red Flag”: A pattern, practice or specific activity that could indicate identity theft.

F. “Collection Unit”: Any University department or unit that administers covered accounts. Collection units will be identified through procedures established under this Policy, and include, but are not limited to Student Accounting, Auxiliary Enterprises, Office of Student Financial Assistance and Education, URecFit and Department of Parking Services.

G. “Program Officer”: The University’s VP for Admin & Finance, or designee, that is responsible for coordinating and overseeing the Identity Theft Fraud Prevention Program.

Purpose:
To ensure compliance with the Federal mandate that requires financial institutions and creditors that hold covered accounts to develop and implement a program for new and existing accounts that would identify, detect, prevent and mitigate instances of identity theft.

Scope:
Any department or unit on Campus that is responsible for a covered account, as defined in D above.

Restrictions and Exclusions:
N/A

Responsibilities:
1. The Program Officer shall perform his/her duties in conjunction with representatives from offices identified as Collection Units, including, but not limited to Student Accounting, Auxiliary Enterprises, Office of Student Financial Assistance and Education, URecFit and Department of Parking Services.

2. Each Collection Unit shall develop identity theft prevention procedures to implement under this Identity Theft Prevention Program.

Related/Impacted Policies:
N/A

Procedures:
As required by federal law, the University’s Identity Theft Prevention Program has the following four components:

(i) Identification of relevant “red flags” and incorporating them into the Program;

(ii) Detection of red flags that the Program incorporates;

(iii) Prevention and mitigation of identity theft by responding appropriately to detected red flags; and
(iv) Evaluation and adjustment of the Program periodically to reflect changes in risks, including periodic evaluation and adjustment of the Program based upon the results of testing and monitoring as well as changes in operations or operating systems.

A. Identification of Relevant Red Flags. The University shall consider the following risk factors in identifying relevant red flags for covered accounts:

(i) Types of covered accounts it offers or maintains;
(ii) Methods it provides to open its covered accounts;
(iii) Methods it provides to access its covered accounts; and
(iv) Its previous experiences with identity theft.

The University shall incorporate relevant red flags from sources, such as:

(i) Incidents of identity theft that the University has experienced;
(ii) Methods of identity theft that the University has identified that reflect changes in identity theft risks; and
(iii) Applicable supervisory guidance.

The University's Identity Theft Prevention Program shall include red flags from the following categories:

(i) Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
(ii) The presentation of suspicious documents;
(iii) The presentation of suspicious personal identifying information, such as a suspicious address change;
(iv) The unusual use of, or suspicious activity related to, a covered account; and
(v) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University.

B. Detection of Red Flags. Policies and procedures shall be established to address the detection of Red Flags in connection with the opening of covered accounts and the maintenance of existing covered accounts. This shall be done by obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules codified in 31 U.S. C. 5318(l) (31 CFR 103.121); and authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

C. Prevention and Mitigation of Identity Theft. The Program shall provide for appropriate responses to the Red Flags the University has detected that are commensurate with the degree of risk posed. The Program will consider aggravating factors that may heighten the risk of identity theft.
Such factors include, but are not limited to, a data security incident that results in unauthorized access to a customer’s account records or notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the Institution.

D. Oversight of Service Provider Arrangements. UMB will ensure that service providers of covered accounts conduct business in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

E. Evaluation and Adjustment of the Program. On an annual basis, the Program Officer, working with the Collection Units and responsible units and offices, shall evaluate and adjust the Program to reflect changes in risks to customers or to the safety and soundness of the University from identity theft, based on factors such as:

(i) University experience with identity theft;
(ii) Changes in methods of identity theft;
(iv) Changes in methods to detect, prevent, and mitigate identity theft;
(v) Changes in the types of accounts that the University offers or maintains; and
(vi) Changes in the business arrangements of the University, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Following the evaluation process, the Collection Units shall modify their respective identity theft prevention procedures as necessary to implement identified revisions in the Identity Theft Prevention Program.

Signature_______________________________________Date____________
Kathleen M. Byington
Vice President Administration and Finance