

Policy on Identity Theft Prevention Program

Policy Number: *Number to be assigned later*
Effective Date of Policy: November 1, 2009

Overview

This policy implements an Identity Theft Prevention Program (the “Program”) at the University of Mary Washington, pursuant to the Federal Trade Commission’s Red Flags Rule under section 114 and 315 of the Fair and Accurate Credit Transactions Act, which amended the Fair Credit Reporting Act. This policy and its related procedures are determined to be appropriate to the size and complexity of the university’s operations and the nature and scope of its activities.

Purpose

The purpose of the Program is to detect and respond to identity theft attempts in order to prevent identity theft. This policy and related procedures are designed to identify relevant red flags and incorporate them into the Program; detect red flags that are part of the Program; respond appropriately to any red flags that are detected; and ensure the Program is updated periodically to address changing risks.

Policy Detail

I. SCOPE

This policy applies to all University of Mary Washington employees and service providers at all locations.

II. DEFINITIONS

Covered Account. The law defines this as a consumer account designed to permit multiple payments or transactions, and any other account for which there is a reasonably foreseeable risk of identity theft. This includes all student accounts for payment of tuition and fees including loans, all employee accounts for receipt of wages and reimbursed expenses, and EagleOne accounts.

Identity Theft. Identity theft is a fraud committed or attempted using the identifying information of another person without authority.

Identity Theft Committee (“Committee”). The Committee will be chaired by the Chief Information Security Officer, who will serve as the Program Administrator. Members of the committee may include representatives from Business Services, Finance, Human Resources, Information Technology, Office of Admissions, Office of Financial Aid, Office of the Registrar, and Office of Student Accounts. Other members may be appointed by the Program Administrator.

Program Administrator. The Program Administrator is the individual designated with primary responsibility for oversight of the program.

Red Flag. A red flag is a pattern, practice, or specific activity that could indicate identity theft.

Service Provider. A Service Provider is a third party who performs an activity in connection with one or more covered accounts.

IV. RESPONSIBILITIES

Committee. The Committee is responsible for ensuring appropriate training of university staff on the program, reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the Program. The Committee also is responsible for providing an annual report of Program activity to the President and Executive Cabinet.

Employees. Employees are expected to follow notification guidelines as outlined in the Procedure for Identity Theft Prevention.

Program Administrator. The Program Administrator is responsible for developing, implementing and updating the Program through his/her chairmanship of the Committee.

Purchasing. Purchasing is responsible for ensuring that contracts with service providers who perform an activity in connection with one or more covered accounts require that the service provider has policies and procedures in place to detect, prevent and mitigate the risk of identity theft.

V. COMPLIANCE

In order to identify relevant red flags, the university considers the types of covered accounts it offers or maintains, methods it provides to open or access its accounts, and its previous experiences with identity theft. The university will create appropriate procedures to respond to detection of red flags in order to prevent identity theft.

Approvals

The Executive Vice President and CFO, and the Vice President for Information Technology and CIP shall be responsible for the oversight of the Program and may delegate administration of the Program to other appropriate University officials. This policy was approved by the Board of Visitors on November 20, 2009.

Revision

0. By Assistant Vice President for Finance and Controller, October 27, 2009.