Procedure for Identity Theft Prevention Program

Effective Date of Procedure: November 1, 2009, revised October 19, 2010

OVERVIEW AND PURPOSE

In accordance with the Federal Trade Commission's (FTC) Red Flag Rule 16 CFR Part 681, which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACT Act), it is the policy of University of Mary Washington (UMW) to establish an identity theft prevention program to detect, prevent, and mitigate identity theft in connection with new and existing covered accounts.

UMW recognizes that some activities conducted by the University meet the definition of "creditor" and "financial institution" as defined by the Federal Trade Commission's (FTC) Red Flag Rules, which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACT Act). UMW is committed to conducting University business in compliance with federal law and after evaluating the nature and scope of the University's activities subject to the "FTC Red Flag Rules," the following program was developed.

UMW is committed to identifying Red Flags associated with identity theft and protecting its students, faculty, staff, and others who entrust their personal information with the University. The University complies with the FTC Red Flag Rule by developing an identity theft prevention program that includes:

(1) Identifying and detecting "red flags";
(2) Taking appropriate action when detection occurs to mitigate identity theft; and
(3) Updating the identity theft prevention program to reflect changes in risk.

UMW Acting Vice President for Administration and Finance and CFO and the Vice President for Information Technologies and CIO interpret this policy and shall designate the University Information Security Officer (ISO) to serve as the UMW Identity Theft Prevention Program Administrator. The Program Administrator will revise or eliminate any or all parts as necessary to meet the changing needs of UMW. Please direct policy questions to the Program Administrator.

SCOPE

- Accounting
- Admissions Office
- Business Services
- Cashiering
- Financial Aid Office
- Human Resources
- Department of Information Technology

- Payroll Office
- Registrar
- Student Accounts Office
- All employee's

PROCEDURE DETAIL

The purpose of the Program is to detect, prevent, and mitigate incidents of identity theft in connection with UMW covered accounts as defined under the FTC Red Flag Rules. UMW is committed to identifying Red Flags associated with identity theft and protecting its students, faculty, staff, and others who entrust their personal information with the University.

The Program

In the development of the Program, existing policies, procedures, and internal controls that would limit reasonably foreseeable risks to our students, faculty and staff from identity theft have been included. We have also identified and evaluated the covered accounts that meet the criteria specified by the FTC for inclusion as a "covered account."

UMW Covered Accounts

Each University department is responsible for determining whether they have oversight for a covered account and must share that information with the Program Administrator for inclusion in the Program. Identified covered accounts at UMW are as follows:

Student Installment Payment Plan Accounts *Responsible Office - Student Accounts*
A ten payment annual plan or five payment installment plan offered to enrolled students during the Fall or Spring semesters with an administrative fee assessed. In order to participate, the student or authorizer payer must sign up for the plan with an optional down payment.

Student Accounts with Refund Transactions *Responsible Office - Student Accounts*
Refunds due to overpayment on account as a result of personal payments, financial aid, and/or third party sponsor awards. A refund is processed as a check to the student's UMW on-campus mailbox address or parent's address (PLUS loan Borrower); or as a direct deposit to the student's bank account based on information submitted by the student on EagleNet. A refund may also be processed to a third party sponsor in the form of a check.

Student Accounts in Collection with Payment Arrangements *Responsible Office - Student Accounts*
Payment arrangements may be offered to non-enrolled students to collect a debt. A collection fee is assessed. Payment arrangements are generally set for the debt to be collected within six months.

Loan Accounts *Responsible Office - Financial Aid*
Federal Perkins Loans, Moisman Emergency Loans are collected in accordance to the terms of the promissory notes. An outside billing service provider, Campus Partners is used to ensure due

diligence for the above referenced loans with the exception of Moisman Loans.

EagleOne Card Prepaid Declining Stored - Value Accounts *Responsible Office - Business Services*

The EagleOne Card offers declining stored-value accounts, such as Eagle Dollars, Meal Plans, Flex Dollars, as part of the identification card. These accounts can be used at approved on campus and off campus merchant locations. Deposits can be made online with a credit card, depositing cash at Cashier's Office or by visiting the EagleOne Card Center.

Student Lockbox Payments *Responsible Office - Accounting*

Student tuition and fee payments may be made via BB&T Lockbox. Student invoices are available to the student and authorized payer in EaglePAY. Check or money order payments are accepted through the lockbox.

Service Provider Covered Accounts

UMW has contracted with BB&T for lockbox services to students making tuition and fee payments; General Revenue Corporation, Office of the Attorney General and Department of Taxation in the collection of past due loans, returned checks, and tuition and fee accounts; and Campus Partners as a billing service provider in the collection of campus based student loans.

Identification of Relevant Red Flags

Risk Factors

To identify potential red flags associated with covered accounts at UMW, the following will be considered:

- The types of covered accounts offered by UMW;
- The methods provided or employed to open a covered account;
- How students, faculty and staff can access covered accounts; and
- Any previous experiences with identity theft.

The following information sources are used in creation of covered accounts at UMW. Staff should evaluate this information and the methods used in collection of this information for "red flags."

- Common application (admissions/loan) with personally identifying information
- Transcripts
- Official standardized test scores
- Letters of recommendation
- Application for Virginia Domicile
- Loan Application/Promissory Note
- Direct Deposit Form
- New hire process

Sources of Red Flags

UMW staff should incorporate relevant Red Flags from the following sources:

- Incidents of identity theft experienced by UMW;

- Methods of identity theft identified by UMW that signal a change in risks; and
- Applicable guidance.

Categories of Red Flags
The University has identified the following Red Flags in each of the categories listed below:

Suspicious Documents
Receipt of suspicious documents (such as an identification card) that appear fraudulent, or are presented by a person who does not fit the photograph/description on the identification card; Presentation of other documentation that is inconsistent with existing information; and Application or other documentation appears to be forged or altered.

Suspicious Personal Identifying Information
Identifying information presented that was previously presented by another person; Identifying information that is inconsistent with other sources of information for the same person; Identifying information that was previously found to be fraudulent; and Failure to provide complete identifying information as requested.

Suspicious Covered Account Activity or Unusual Use of Account
The unusual use of, or other suspicious activity related to a UMW covered account; Unusual requests to make changes to account information; Attempts to redirect refund monies from the destination identified in the system of record; Attempts to involve the university in the verification of the identity of the account holder to an external entity; and Unauthorized access to or use of a students, faculty and staff's information or covered account.

Alerts From Others
Notice received from students, faculty and staff, victims of identity theft, law enforcement authorities or others regarding possible identity theft associated with a UMW covered account.

Detecting Red Flags
UMW staff should implement policies and procedures to address the detection of Red Flags associated with opening a covered account or accessing an existing covered account. The following procedures will be used in detecting Red Flags:

- Obtain and verify the identity of a students, faculty and staff opening a covered account;
- Authenticate students, faculty and staff when making changes to an existing covered account;
- Monitor transactions for possible Red Flags; and
- Verify the validity of a change of address request on an existing account and provide the students, faculty and staff with a means to promptly report an incorrect address.

Procedures to Mitigate Identity Theft

The Program includes the following University general and Student Accounts or Finance procedures to mitigate identity theft. Additional procedures should be developed as necessary to address specific covered accounts.

General Procedures:

a) Require certain identifying information such as name, birth date, academic records, home address, and other identification before creating a new account. Check for inconsistent or incomplete information and do not activate the account unless you receive complete information.

b) Verify the students, faculty and staff's identity at the time an identification card is issued (review driver's license, passport, or other government issued photo id).

c) Encourage students, faculty and staff to make changes of address through the appropriate password protected system or when applicable the Self Service Banner System. If requested in person, require picture identification;

d) Ensure that paper documents associated with or containing covered account information and students, faculty and staff personally identifiable information are maintained in a secure environment and are shredded when retention requirements expire.

e) Ensure that electronic files containing covered account information and students, faculty and staff personally identifiable information are secured in accordance with University information security requirements, and that access to such files is limited to those who need access to perform their job duties and that such files and records within them are securely destroyed when retention requirements expire.

f) Ensure that University websites used to access covered accounts meet University information security requirements.

g) Collect social security numbers only if required or authorized by federal or state law.

h) Require a student to identify himself/herself with picture identification and/or student number before providing him/her information about his/her student account.

Refund Processing Procedures:

i) Check refunds must be sent to the active address indicated in the Banner System, and the PLUS parent address collected on the application by the Financial Aid Office. Students/parents cannot request a check to be sent to a different address, the address in the system must be used.

j) Direct Deposit refunds must be sent to the account submitted. An email notification will be sent to the students, faculty and staff's UMW email address notifying him/her of the refund when the direct deposit is processed.

Response to Red Flag Detection

In determining the possible responses to Red Flags associated with UMW covered accounts, factors that may increase the risk of identity theft were considered. Based on these considerations, if red flags are detected, one or more of the following steps should be taken:

- Change passwords or disable access to covered accounts;
- Investigate transactions to covered accounts which include contacting the actual students, faculty and staff to notify the students, faculty and staff and verify if activity is fraudulent;
- Close the covered account;

- Reopen a covered account with a new account number after inactivating the existing account number;
- Do not open a new covered account for the students, faculty and staff;
- Notify the Program Administrator;
- Determine that no response is warranted under the particular circumstances.

Notification
When a red flag has been detected, all employees must immediately notify the Program Administrator by using one of the following methods:

- Escalating to the committee member representing the business area
- Calling the help desk at 540-654-2255.
- Via email to identitytheft@umw.edu

Oversight of the Program
The FTC Red Flag Rules require that provisions be made for the oversight, development, implementation, and administration of the Program. This requirement may be met by an entities board, appropriate committee of the board, or a designated employee at the level of senior management. The Acting Vice President for Administration and Finance and CFO and Vice President for Instructional Technology and CIO designate the University Information Security Officer to implement and oversee the UMW Identity Theft Prevention Program.

Reports
At least annually, the Program Administrator will require and review reports submitted by staff on the compliance of UMW with the Program. These reports should address and evaluate the following:

- Material matters related to the Program;
- Effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts;
- Service provider arrangements;
- Significant incidents of identity theft and managements response; and
- Recommendations for changes to the Program.

Updating the Program
The Program Administrator will update the Program periodically to reflect changes in risks to students, faculty and staff or to the safety and soundness of UMW based on the following factors:

- UMW experiences with identity theft;
- Changes in methods of identity theft;
- Changes in methods available to detect, prevent, and mitigate identity theft;
- Changes in the types of covered accounts maintained by UMW; and
- Changes in business arrangements such as alliances, joint ventures, or service provider agreements entered into by UMW.

Staff Training and Reporting

The Program Administrator will ensure that employees responsible for activities associated with the creation of covered accounts receive training on the detection of Red Flags and the appropriate response when a Red Flag is detected.

Oversight of Service Provider Arrangements
In instances where the University contracts for services provided in association with a covered account, UMW will require that the service provider has reasonable policies and procedures in place to detect, prevent, and mitigate the risk of identity theft. Additionally, documentation supporting the existence of policies and procedures or an identity theft prevention program shall be acquired and implemented into the Program.

Creation and Approvals

This procedure is issued by the Finance and Information Technology and approved by the Executive Vice President*;* November1, 2009.

Revision

0. By Assistant Vice President for Finance and Controller and Chief Security Officer, November 1, 2009
1. By Associate Vice President for Finance & Controller, October 19, 2010