Identity Theft Red Flag Policy

Purpose

Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA), also known as the *Red Flag Rule*, require institutions to develop and implement a written identify theft prevention program which is under the oversight of the institutions' governing boards or senior employees. The purpose of this policy is to establish guidelines for management and staff to use in establishing and maintaining policies and procedures in order to comply with FACTA guidelines on detecting, preventing, and mitigating identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the policy. This policy is in addition to any other information security policies currently in effect at the University of Mary.

Nomenclature

- **Identify theft.** A fraud committed or attempted using the identifying information of another person without authority.
- **Account.** A continuing relationship established by an individual with the University of Mary for the purpose of obtaining a product or service for personal, educational, or business purposes. The University of Mary shall determine which accounts are *covered* per FACTA guidelines.
- **Covered account.** A financial account designed to permit multiple payments or transactions whose purpose can be personal, educational or business and is offered or maintained by the University of Mary. Covered accounts include accounts established under the Federal Perkins Loan Program, Federal Nursing Loan Program; Federal Family Education Loan Program, or other Title IV programs; student account, loan, grant, or scholarship information; M-Card accounts; credit/debit card processing; financial aid information; business accounts; payroll account information; and any other account that University of Mary offers or maintains for which there is a reasonably foreseeable risk to the accountholder or to the safety and soundness of University of Mary from identity theft, including financial, operational, compliance, reputation, or litigation risks.
- ***Red flag.*** Relevant warning signs of possible identity theft. Examples may include unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents.
- ***Service provider.*** A third party who provides service to the University of Mary.
- ***Need to Know:*** Authorization is given to a user for whom access to the information must be necessary for the conduct of one's official duties and job functions as approved by the employee's supervisor.

Red Flag Activities

Certain “red flag” activities are associated with a likelihood of fraud. In the event that any of the following activities are detected on a University of Mary account, the employee detecting the activity shall make a red flag report to his or her immediate supervisor for investigation. These red flag activities include the following.

- A fraud alert included with a consumer report
- Notice of a credit freeze in response to a request for a consumer report
- A consumer reporting agency providing a notice of address discrepancy
- Unusual credit activity, such as an increased number of accounts or inquiries
- Documents provided for identification appearing altered or forged
- Photograph on ID inconsistent with appearance of accountholder
- Information on ID inconsistent with information provided by person opening account
- Information on ID, such as signature, inconsistent with information on file
- Application appearing forged or altered or destroyed and reassembled
- Information on ID not matching any address in the consumer report, social security number has not been issued or appears on the Social Security Administrator’s Death Master File, a file of information associated with social security numbers of those who are deceased.
- Lack of correlation between social security number range and date of birth
- Personal identifying information associated with known fraud activity
- Suspicious address supplied, such as a mail drop or prison, or phone numbers associated with pagers or answering service
- Social security number provided matches that submitted by another person registering or opening an account or other accountholders
- An address or phone number matching that supplied by a large number of applicants
- The person registering or opening the account unable to supply identifying information in response to notification that the application is incomplete
- Personal information inconsistent with information already on file
- Person opening account or accountholder unable to correctly answer challenge questions
- Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account
- Accountholder indicates that they are not receiving paper account statements
- Accountholder notifies that there are unauthorized charges or transactions on accountholder’s account
- Institution notified that it has registered or opened a fraudulent account for a person engaged in identity theft

Responding to Red Flags

Any employee detecting red flags shall report the activity to his or her supervisor as soon a possible. Employees shall report actual and potential red flags and any potential evidence of identify theft. The supervisor must make appropriate and timely inquiries to determine the validity of the red flag(s).

In the event that the supervisor determines that identify theft has occurred, the supervisor must submit a formal report of the matter and submit it his or her department head, who shall take action to mitigate the effect of the action on the victim of identity theft fraud. Appropriate actions will be determined by the department head, taking into account the factors such as the type of transaction, the availability of contact information for the victim of the fraud, and any relationships with the victim of the fraud.

The following list includes some examples of appropriate action, but is not intended to be exhaustive.

1. Deny access to the covered account until other information is available to eliminate the red flag;
2. contact the student;
3. notify the accountholder and/or victim that fraud has been attempted or that it has occurred;
4. cancel the registration or transaction;
5. not opening a new account;
6. closing the account in question;
7. notify law enforcement;
8. notify the vice president for financial affairs;
9. change any passwords, security codes or other security devices that permit access to a covered account; or
10. monitor the account or database for evidence of identity theft.
11. In some circumstances, no action may be required after a thorough investigation of the matter.

The department head shall make a formal report of the incident to the vice president for financial affairs. The report shall describe the appropriate action taken, actions taken to mitigate the impact of the effects of the actual or potential identity theft, and include a plan to address additional actions the department has identified to improve the systems with the department to handle or prevent similar situations in the future.

Oversight of the Program

The initial Identity Theft Red Flag Program shall be approved by the university's board of trustees. Operational oversight lies with the vice president for financial affairs and his/her designees. Oversight shall include policy administration, ensuring appropriate training of staff on the policy, reviewing staff reports regarding the detection of red flags, reviewing the steps for preventing and

mitigating identity theft, and determining which steps of prevention and mitigation should be taken in particular circumstances.

Updating the Policy

This policy will be periodically reviewed and updated to reflect changes in risks to students and the university from identity theft. At least once per year, the vice president for financial affairs will consider the university's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the university maintains, and changes in the university's business arrangements. After considering these factors, the vice president for financial affairs will determine whether changes to the policy, including the listing of red flags, are warranted. If warranted, the vice president for financial affairs will bring proposed changes to the policy forward to the university's senior management team for further consideration and approval by the president.

Oversight of Service Provider Arrangements

The university shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. The University of Mary shall require service provider, by contract, to have policies and procedures to detect relevant red flags that may arise in the performance of the service provider's activities and either report the red flags to the University of Mary's vice president for financial affairs or take appropriate steps to prevent or mitigate identity theft.

Approved
September 18, 2009 by the University of Mary's Board of Trustees