

## IMMACULATA RED FLAG RULE PROGRAM

### EFFECTIVE DATE:

- Authority** This Program was approved by the Board of Directors of Immaculata University (hereinafter "IU").
- Program Statement** The risk to IU and its Customers from Identity Theft is of significant concern and pursuant to this Program IU will make responsible efforts to detect, prevent and mitigate Identity Theft associated with Covered Accounts.
- Program Purpose** This Program is intended to work in conjunction with the IU Administrative Data Security Program, the GLBA Required Information Security Program, the IU Confidentiality of Student Records Program, the IU HIPAA Program and other related policies.
- Summary** This Program creates reasonable procedures to (1) identify risks that signify potentially fraudulent activity within new or existing Covered Accounts; (2) detect risks when they occur in Covered Accounts; (3) respond to risks if fraudulent activity has occurred and act if fraud has been attempted or committed; and (4) update the Program periodically to reflect changes in risks to Customers, Covered Accounts and previous experience with Identity Theft.

Section headings are:

1. PROGRAM SCOPE AND APPLICABILITY
2. DEFINITIONS
3. RESPONSIBILITY OF PROGRAM OFFICER
4. ELEMENTS OF THE PROGRAM
5. PROGRAM ADMINISTRATION

### I. PROGRAM SCOPE AND APPLICABILITY

This Program is to be administered by IU through the Program Officer and it applies to all employees of IU that are involved in affected businesses processes and/or Service Providers providing services to IU relating to the Covered Accounts.

### II. DEFINITIONS

**"Identity Theft"** means fraud committed or attempted using the identifying information of another person without authority.

**"Covered Account"** means an account that a financial institution or Creditor offers or maintains, primarily for personal, family, or household purposes, that

involves or is designed to permit multiple payments or transactions; and any other account that the 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.

**“Creditor”** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original Creditor who participates in the decision to extend, renew, or continue credit.

**“Customer”** is a person with a Covered Account at IU.

**“Program Officer”** is the person appointed by the President who is responsible for the management and administration of the Program, the IU GLBA Required Information Security Policy and the IU IT Security Incident Response Plan.

**“Red Flag”** means a pattern, practice or specific activity that indicates the possible existence of Identity Theft.

**“Red Flag Rules”** are rules issued by the Federal Trade Commission (“FTC”) on November 7, 2007 regarding Identity Theft. These rules implement Sections 114 and 115 of the Fair and Accurate Credit Transactions Act and require certain policies and procedures be developed that are designed to detect, prevent and mitigate Identity Theft.

**“Service Provider”** means a person that provides a service directly to the financial institution or Creditor.

### **III. RESPONSIBILITY OF PROGRAM OFFICER**

The Program Officer shall be responsible for implementing this Program and shall have the authority to create procedures and additional policies to effectively and reasonably fulfill the requirements outlined in this Program.

### **IV. ELEMENTS OF THE PROGRAM**

#### **A. Identification of Red Flags**

When appropriate, IU will consider the following risk factors when identifying Red Flags:

1. Alerts, notifications or warnings from credit reporting agencies;
2. The presentation of suspicious documents;
3. Notices from Customers, law enforcement authorities, or other persons regarding possible Identity Theft in

connection with Covered Accounts; and

4. Unusual use of, or suspicious activity related to, a Covered Account.

## **B. Detecting Red Flags**

IU will attempt to detect Red Flags in connection with the opening of Covered Accounts and existing Covered Accounts by:

1. Obtaining identifying information about, and verifying the identity of, a person opening a Covered Account;
2. Authenticating Customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing Covered Accounts; and
3. Rejecting any application for a service or transaction that appears to have been altered or forged.

## **C. Responding to Fraudulent Activity**

All potentially fraudulent activity must be reported to the Program Officer. When appropriate, IU shall take the following steps to prevent Identity Theft :

1. The Program Officer and relevant personnel will gather all related documentation.
2. The Program Officer and relevant personnel will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic and will respond appropriately.
3. Additional responses may include: terminating a transaction, changing passwords, security codes, or other security devices that permit access to a Covered Account, not opening a Covered Account, closing an existing Covered Account, notifying and cooperating with appropriate law enforcement and/or determining that no response is warranted under the particular circumstances.

## **D. Periodic Updates to Program**

At periodic intervals established pursuant to this Program, or as required, the Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current business environment. Periodic reviews will include, at a minimum, an assessment of:

1. The types of Covered Accounts offered or maintained;
2. The methods provided to open Covered Accounts;
3. The methods provided to access Covered Accounts;
4. Previous experience with Identity Theft;
5. Red Flags as identified above and the need to define new Red Flags; and
6. Response procedures defined above and their efficacy to reduce damage to the university and its Customers.

## **V. PROGRAM ADMINISTRATION**

### **A. Oversight of the Program**

Oversight of the Program will lie with the Program Officer. The Program Officer will be responsible for appointing personnel to assist with Program implementation, administering the Program, reviewing reports prepared by staff regarding compliance with Red Flag Rules and approving material changes to the Program as necessary to address changing Identity Theft risks.

### **B. Reports**

The Program Officer shall provide updates to the Board and the President on the progress of the Program. This report should address such issues as: the effectiveness of the Program and procedures in addressing the risk of Identity Theft in connection with Covered Accounts; Service Provider arrangements; significant incidents involving Identity Theft and management's response and recommendations for material changes to the Program.

### **C. Training**

The Program Officer will train all employees and officials for whom it is reasonably foreseeable that they may come into contact with Covered Accounts that may constitute a risk to IU or Customers. Training will also be provided as changes to the Program are made. Training will include operating procedures for identifying and detecting Identity Theft as well as responding to Identity Theft.

### **D. Oversight of Third Party Service Provider Arrangements**

IU is responsible for ensuring that the activities of Service Providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. When appropriate, contractual arrangements with Service Providers, including Service Providers that are entities outsourced for the provision of hosting services, should specifically require the Service Provider to maintain its own Identity Theft prevention Program consistent with the guidance of the Red Flag Rules.