

# Indiana University

## Red Flag Rules Standard Operating Procedures

**SUBJECT:** Responsibilities & Administration of Identity Theft Prevention Program

**SOURCE:** The Office of the Treasurer

**ORIGINAL DATE OF ISSUE:** December 2011

**DATE OF LAST REVISION:** N/A

**SOP NO:** 1

**RATIONALE:** To provide guidelines pertaining to the roles and responsibilities related to the Identity Theft Prevention Program (“Program”).

**SOP:** Pursuant to the Federal Trade Commission’s (“FTC”) Red Flag Rules, which implements the Fair and Accurate Credit Transactions Act (the “FACT Act”), The Indiana University Board of Trustees have approved an Identity Theft Prevention Program. The University’s program is designed to :

1. Identify relevant Red Flags for new and existing Covered Accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure that the Program is updated periodically to reflect changes in risks to the account holders or to the safety and soundness of the creditor from Identity Theft.

The purpose of this standard operating procedure is to outline the roles & responsibilities associated with the Identity Theft Program.

### **IMPLEMENTATION OF THE PROGRAM**

1. A brief questionnaire will be sent to fiscal officers to help determine which departments or units may have Covered Accounts in addition to those already identified in the program.
2. Employees within departments or units that have Covered Accounts need to satisfy the following items:
  - Become familiar with this Standard Operating Procedure.
  - Read the Identity Theft Prevention “Red Flag Rule Program” approved by The Board of Trustees.
  - Complete Red Flag Rule training to prevent, mitigate, and detect Identity Theft. A [Red Flag Training Presentation](#) has been

created to guide you through the training.

3. Those department or units that have a Covered Account must develop and implement a written plan that identifies relevant Red Flags for their specific Covered Account. The document should also specify what controls the department has in place to detect and mitigate instances of Identity Theft, as well as the appropriate response when a Red Flag has been detected. A template of a matrix is available to capture the required information in [Attachment A- Departmental Red Flag Plan Blank Template](#). To assist the department or unit head, or the appropriate designated employee within that department or unit, with filling out the required matrix, a summary of possible Red Flags can be referenced in [Attachment B- Summary of Possible Red Flags](#). The department or unit head may also reference a completed version of the matrix in [Attachment D- Example of SLA Red Flag Plan](#).
4. Any department/unit who is involved in a case of Identity Theft should maintain a log of the incident(s). The log should contain the date, description of the incident, what Red Flags were involved, and what actions were taken to avoid a similar situation from occurring in the future. An example of a log can be referenced in [Attachment C- Incident Log Example](#).
5. The department/unit head or their designee of a Covered Account shall conduct an annual risk assessment. The assessment should consider prior experiences with Identity Theft; changes in the methods of Identity Theft; changes in the method of detection, prevention, and mitigation of Identity Theft; the Covered Accounts offered and administered by the University; and the potential Red Flags that may arise with respect to the Covered Accounts. The annual assessment should also consider any changes in risks to students and individual account holders and to the safety and soundness of the University from Identity Theft. If the department/unit determines changes to the plan are necessary, the matrix should be updated and shared with employees.
6. By February 15<sup>th</sup>, each department/unit head or their designee of a Covered Account will submit a [certification form](#) on an annual basis to the appropriate [campus representative](#) indicating:
  - a. They have completed their annual review of the controls in place to prevent, mitigate, and detect Identity Theft.
  - b. Their employee training has been completed.
  - c. The status of their Identity Theft Program, indicating either:
    - no changes have been made and a current copy of the template is being provided with the certification form; or
    - additional changes have been made and a new copy of the template is being provided with the certification form.
  - d. Documentation that either: i) that there were no instances of Identity Theft; or ii) that there were instances of Identity Theft and attaching a log of all known instances Identity Theft for the previous year.
  - e. Specify if their department or unit has a relationship with a Service Provider. If so, they need to indicate that they have a copy of the Red Flag Rules from a Third Party Contract and that the Third Party Provider has verified their compliance with the Indiana University Identity Theft Program.
7. The campus representatives will then forward the certification form to the

Indiana University Red Flag Coordinator by March 31<sup>st</sup>.

8. Annually, the Red Flag Rule Coordinator will compile the results of the certification and schedule a meeting to discuss any potential changes to the Program with the Red Flag Committee.
9. Annually, the Red Flag Rule Coordinator will provide a report to the President or his/her designee, regarding their compliance with the Program.

## **RESPONSIBILITIES**

Department heads with Covered Accounts are ultimately responsible for the administration, oversight, and annual review of their individual department/unit Identity Theft Prevention Plans.

Red Flag Rule Coordinator is the Director of Student Loan Administration. This individual is responsible for gathering the required information from the departments with Covered Accounts, conducting an annual meeting with the Red Flag Committee, and summarizing the findings for the President (or his/her designee).

Red Flag Committee is comprised of representatives from various campuses and administrative offices. This committee is responsible for evaluating any changes to the University's Identity Theft Prevention Program and reviewing the summary of the certification process on an annual basis. A list of these committee members can be found on The Office of the Treasurer webpage.

Employees within a Covered Account Area need to be familiar with the University Identity Theft Prevention Program adopted by the Board of Trustees, this procedure, and their individual department Identity Theft Prevention Plan. They are responsible for knowing the Red Flags associated with their Covered Account, following through on procedures to detect Red Flags, and communicating any Red Flags that are detected to management.

**“Account”** means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes. It includes (i) an extension of credit, such as the purchase of property or services involving a deferred payment, and (ii) a deposit account.

**“Covered Account”** means (i) an account that a creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions and (ii) any other account that the creditor offers to maintain for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from Identity Theft, including financial,

operational, compliance, reputation, or litigation risks.

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

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

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

**CROSS  
REFERENCE:**

**[Indiana Theft Prevention Program](#)**

**RESPONSIBLE  
ORGANIZATION:**

**The Office of the Treasurer**