Red Flag Identity Theft Training

December 12, 2011

INDIANA UNIVERSITY

Red Flag Rules Overview

The Red Flag Rules, found at 16 Code of Federal Regulation (CFR) § 681.2, require a creditor to periodically determine, by conducting a risk assessment, whether it offers or maintains covered accounts. Once the existence of a covered account has been identified, the department/unit is required to develop and implement a written plan designed to:

- Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Board approved program;
- Detect Red Flags that have been incorporated into the Board approved program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
- Ensure that the Board approved 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.

Goals of the Training Session

The goal of this training is to familiarize employees with terminology associated with the Red Flag Rules; categories of Red Flags; methods of detection, prevention, and mitigation that you may want to consider when developing your written plan; and, the appropriate response when a Red Flag is detected.

Terminology

- **“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.

- **“Active Duty Alert”** allows a member of the military who is away from their usual duty station, to flag their credit report to help minimize the risk of identity theft while they are deployed. When a business sees the alert on the credit report, it must verify your identity before credit can be issued.

Terminology Continued

- **“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.

Terminology Continued

"**Creditor**" refers to a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit.

Examples of creditor like activities within the University:

- Student Loan Activities (i.e. Federal Perkins Loan Program, Health Professions Loan Program, Nursing Loan Program, Institutional Loan Programs)
- Short Term Loans processed by the Bursar, IU Foundation, or International Services
- Bursar/Student Accounts
- Patient Accounts (i.e. Optometry, Dentistry, Health Services)
- Stored Value Cards
- Deferred Payments (after goods or services are received)
- Installment Payments

Terminology Continued

- **“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.

Categories of Red Flags

- Alerts, notifications or warnings from a consumer reporting agency
- Suspicious Documents
- Suspicious Personal Identifying Information
- Unusual Use of, or Suspicious Activity Related to, the Covered Account
- Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by University

Alerts, notifications or warnings from a consumer reporting agency:

- Receipt of a fraud or Active Duty Alert accompanying a consumer credit report
- Receipt of a notice of credit freeze provided in response to a request for a consumer report
- Receipt of a notice of address discrepancy from a credit reporting agency
- Receipt of a consumer report which indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of the account holder (e.g. recent and significant increase in number of inquiries; unusual number of recently established credit relationships; a material change in the use of credit)

Suspicious Documents

- Documents presented for the purpose of personal identification are incomplete or appear to have been altered, forged or inauthentic
- The photographic and/or physical description on the personal identification is inconsistent with the appearance of the individual presenting the document
- Other information contained on the personal identification is inconsistent with information provided by the individual opening a new covered account or when presenting the personal identification for verification
- Other information contained on the personal identification is inconsistent with readily accessible information on file with the University
- An application received by the University appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled

Suspicious Personal Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the University (e.g. discrepancies in addresses)
- Personal identifying information provided is inconsistent when compared against internal information held by University, such as discrepancies in addresses, phone numbers, and other personal identifying information
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University, such as fictitious and/or duplicated phone numbers, addresses or social security number (SSN)

Suspicious Personal Identifying Information Continued

- Personal identifying information provided is fictitious and/or the same or very similar to that submitted by others opening an account or holding existing accounts, such as addresses, telephone numbers, bank accounts, and SSN
- The student or individual opening a covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete
- Challenge questions, used by University to allow students and individuals to access their covered accounts, are answered incorrectly

Unusual Use of, or Suspicious Activity Related to, the Covered Account

- Shortly following a change of address to a covered account, or a request to change the address, University receives a request to change the account holder's name, a request for the addition of authorized users on the account, or other suspect request
- A covered account that has been inactive for a reasonably lengthy amount of time is used in an unusual manner
- Mail sent to the account holder is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account
- The University is notified that the student or individual is not receiving paper account statements and those statements are not being returned as undeliverable
- The University is notified of unauthorized changes or transactions in connection with a student's or individual's covered account

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by University

- University is notified by a student or individual account holder, a victim of Identity Theft, a law enforcement entity, or any other person that it has opened a fraudulent account for a person engaged in Identity Theft

Detection of Red Flags

- Appropriate personal identifying information (e.g., photo identification, date of birth, academic status, address, etc.) shall be obtained from the student or individual account holder, prior to issuing a new or replacement ID card, opening a covered account, or allowing access to a covered account.

- When certain changes to a covered account are made online, students and individuals holding covered accounts shall receive notification to confirm the change was valid and to provide instruction in the event the change is invalid.

- Suspicious changes made to covered accounts that relate to an account holders identity, administration of the account, and billing and payment information shall be verified.

Prevention & Mitigation of Identity Theft

University personnel involved in the administration of covered accounts will take the following steps, where appropriate, to prevent and mitigate instances of identity theft.

- Monitor a covered account for evidence of Identity Theft;
- Contact student(s) and/or individual account holder(s) if they suspect inappropriate activity;
- Request additional documentation from the student and/or individual account holder to verify identity;
- Change passwords, security codes and other security devices permitting access to the covered account;
- Reopen a covered account with a new account number;
- Decline to open a new covered account;
- Close an existing covered account;
- Notify law enforcement;
- Determine that no response is warranted under the particular circumstances;
- Attempt to identify the cause and source of the Red Flag; and
- Take appropriate steps to modify the applicable process to prevent similar activity in the future.

Response to Red Flags

- The detection of a Red Flag by an employee should be reported to the Director of the area.
- Based on the type of Red Flag, the Director will work with the employee and other University personnel to determine the appropriate response.
- Red Flags should also be recorded into a log and submitted to the campus and Red Flag Coordinator on a regular basis. The log should contain the date, description of the incident, which Red Flags were involved, and what actions were taken to avoid a similar situation from occurring in the future.

Service Providers

- If and when the University engages a service provider to perform an activity in connection with a covered account, the University remains responsible for the compliance with the Red Flag Rules.

- It is the responsibility of the department/unit ,directly engaged with the service provider, to ensure the activity conducted is in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.