Red Flags Program

Purpose

The purpose of this Red Flags Rules Program is to document the protocol adopted by the University of Memphis in compliance with the Red Flags Rules. Many offices at the University maintain files on employees and students, both in paper and electronic form with identity information. These files include, but are not limited to: admission information, financial aid information, student billing information, employee personal information, and academic and financial records. In addition, the University hires outside service providers to perform institutional functions which may contain identity information.

This program will indentify the areas of risk associated with identity theft on campus; will address the means whereby those risks will be identified; and will identify the methods of response to such Red Flags in order to mitigate the effects of identity theft.

Applying the Red Flags Rules to the University

Per the Federal Trade Commission guidelines, the University would be a low risk entity for identity theft because:

1. The University has privacy protocol and data security protocol in place
2. The University is a low priority target for identity theft or financial theft due to the nature of its transactions

Program Steps

Step 1 – Identify Relative Red Flags *(Red Flags of identity theft the University is likely to come across)*

A. Notice from a customer, a victim of identity theft, law enforcement agency, or some other entity that an account has been has been used fraudulently or opened for a person engaged in identity theft.

B. Suspicious documents – Examples include but are not limited to the following:
   - Documents provided for identification purposes that appear to have been altered, forged or are inauthentic.
   - The photograph or physical description on the identification document is not consistent with the appearance of the individual presenting the identification.
   - Information on the identification is not consistent with information provided by the person opening a new covered account or with the individual presenting the identification.
   - An application appears to have been altered, forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious personally identifying information – Examples include but are not limited to the following:

- Personal identifying information provided is inconsistent when compared against other sources of information used by the University, such as the Social Security Number (SSN) has not been issued or is listed in the Social Security Administrations Death Master File.
- Personal identifying information provided by the individual is not consistent with other information previously provided.
- Personal identifying information provided is associated with known fraudulent activity, such as addresses or phone numbers that have been previously submitted on fraudulent applications.
- Personal identifying information provided is of a type that is commonly associated with fraudulent activity. Examples are addresses submitted that are fictitious, a mail drop, or a prison, and phone numbers submitted that are invalid or are associated with a pager or answering service.
- The SSN provided is the same as that submitted by another person applying.
- The address or telephone number provided is the same or similar to the address or telephone number submitted by that of another person.
- The individual opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- When establishing security questions and answers, the person opening the covered account cannot provide authenticating information beyond that which would generally be available from a wallet or consumer report.

D. Suspicious covered account activity – Examples include but are not limited to the following:
   - Shortly following the notice of a change of address for a covered account, the University receives a request for a new, additional, or replacement card, or for the addition of authorized users on the account.
   - A covered account is used in a manner that is not consistent with established patterns of activity. Examples would be nonpayment when there is no history of late or missed payments or a material change in purchasing or usage patterns.
   - The activation or use of a covered account that has been inactive for a lengthy period of time. The type of account, expected pattern of usage, along with other relevant factors should be considered when evaluating the usage.
   - Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the individuals covered account.
   - Notification that the individual is not receiving paper account statements.
   - Notification of unauthorized charges or transactions in connection with an individual's covered account.
   - A breach of the University's computer system.

E. Notifications or warnings from credit reporting agencies.

Step 2 – Detecting Red Flags ***(Current procedures designed to detect red flags in day to day operations)***

A. Student Enrollment
   - Require specific identifying information such as name, date of birth, home address, or other identification; and

- Verify the student's identity at the time of issuance of the student identification card by reviewing the student's driver license or other approved government issued photo identification.

B. Existing covered accounts
   - Verify the identification of the student, faculty/staff member, or any other covered account holder if information is requested. Information requests may come in person, via phone, via fax, or via email.
   - Verify the validity of requests to change billing addresses by mail or email, and provide the covered account holder a reasonable means of promptly reporting incorrect billing address changes.
   - Verify the validity of changes in banking information given for billing and payment purposes.

C. Notifications from Consumer Credit Reporting Agencies
   - Require written confirmation from candidate that address provided on application is accurate at the time of the request for the credit report is made to the consumer reporting agency.
   - If, in the event that a notice of address discrepancy is received, verify that the credit report pertains to the candidate for whom the requested report was made and report back to the consumer reporting agency an address for the candidate that the Institution has reasonably confirmed is accurate.

Step 3 – Responding to Red Flags ***(Responses to prevent and mitigate identity theft)***

In the event a red flag or potential red flag is indentified, the Institution must act quickly to assess the risk posed by the red flag. All related documents should be gathered and a description of the situation should be summarized and reported to the Program Administrator. The Program Administrator, with assistance from appropriate University personnel, will determine whether the attempted transaction was fraudulent or authentic. At such time, the University may take the following steps as deemed appropriate:

- Determine that no response is warranted under the circumstances.
- Continue to monitor the covered account for evidence of identity theft.
- In the event of a credit warning, contact the candidate.
- Change any passwords or other security devices that permit access to covered accounts.
- Close and reopen the account.
- Cancel the transaction.
- Determine not to open a new covered account.
- Provide the student, faculty, or staff member with a new university identification number.
- Notify law enforcement.

Step 4 – Administering the Red Flag Program ***(Maintain program and educate staff)***

Program Oversight

The Red Flag Program is administered by the designated Program Administrator, currently the Director of Business Development, and members of the committee representing key units within the University. Because the program is evolving, the committee will meet periodically (a minimum of once per year) to review current processes, determine their effectiveness, and implement changes to the Red Flag Program as needed. The committee is comprised of representatives of the following units:

Academic Affairs
Advancement
Bursar's Office
Human Resources
Information Technology Services
Office of Admissions
Office of Financial Aid
Office of Legal Counsel
Registrar's Office
Student Affairs

The committee membership is also subject to change as needed if warranted by changes in the Red Flag program.

The Program Administrator is also responsible for ensuring that needed steps are taken to prevent and mitigate identity theft, review any staff reports regarding the detection of red flags, and for determining which steps should be taken in particular circumstances when red flags are suspected or detected. The Program Administrator is also responsible for providing an annual report to the University President concerning institutional compliance with the program and its overall effectiveness. The annual report should also include red flag arrangements with service providers, the effectiveness of the program in addressing the risk of identity theft, any significant incidents of identity theft and the University's response, and any recommendations for any material changes to the program.

Staff Training

Training will be provided to all University employees for whom it is reasonably foreseeable that the employee may come into contact with covered accounts or other indentifying information.

Service Providers

The University will require by contract that the service provider either: 1.) have policies and procedures in place to comply with the Red Flag Rule; or 2.) review the institutional policy and report any red flags to the Program Administrator.

Program Updates

The committee will meet periodically to review and re-evaluate the program to determine whether all aspects of the program are up to date and applicable. Consideration will be given the University's experiences with identity theft situations, changes in identity theft methods (both detection methods and prevention methods), and changes in the University's business arrangements with other entities. These reviews will also include an assessment of which accounts are covered by the program. Also, red flags may be revised, replaced, or eliminated with new red flags defined as appropriate.

Additional Measures

Best Practices for the Safeguard of Personally Identifiable Information

In order to limit the risk of identity theft, employees should take the following steps with respect to covered accounts:

- Lock file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with covered account information when not in use.
- Lock storage rooms containing documents with covered account information and record retention areas at the end of each workday or when unsupervised.
- Clear desks, workstations, work areas, printers, fax machines, and common shared work areas of all documents containing covered account information when not in use.
- Review and adhere to recommended security best practices as indentified in the University's campus data security policy. Link is provided below.
- Documents or computer files containing covered account information will be destroyed in a secure manner following established University policies.
- Ensure you share information only in the course of authorized University business.
- Turn your computer monitor away from the view of others who may enter your office or workspace.
- Do not leave you computer unattended when logged into the system.
- Avoid the use of social security numbers. Use the students "U" number.
- Utilize encryption devices when transmitting covered account information.
- Shred documents that are to be disposed of which contain personally identifiable information.
- Use common sense when working with personal identifying data. If an employee is uncertain of the sensitivity of a particular piece of information they should contact their supervisor.

Additional Resources & Policies

In order to supplement the Red Flag Program, employees are encouraged to be knowledgeable of additional laws and policies that relate to employee and student privacy. These include but are not limited to the following:

Federal Trade Commission Red Flag Program–
https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule

Family Education Rights and Privacy Act (FERPA) -
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

University of Memphis FERPA Policy -
https://memphis.policytech.com/dotNet/documents/?docid=481&public=true

University of Memphis Campus Data Security –
https://memphis.policytech.com/dotNet/documents/?docid=451&public=true