

# **THE UNIVERSITY OF MIAMI**

## **IDENTITY THEFT AND RED FLAG POLICY**

In compliance with Part 681 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003 and pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), the University of Miami Board of Trustees has adopted the following Identity Theft and Red Flag Policy as developed by the Office of Treasury Operations with support from the Office of the General Counsel, the Office of HIPAA Privacy and Security, and Internal Audit.

### **SECTION 1: BACKGROUND**

The risk to the University, and its students, faculty, staff, patients, and other constituents from data loss and identity theft is of significant concern to the University and it should make reasonable efforts to detect, prevent, and mitigate identify theft.

### **SECTION 2: PURPOSE**

The University adopts this Identity Theft Policy (the "Policy") in an effort to detect, prevent, and mitigate identify theft in connection with the opening of a "covered account" or any existing "covered account," as defined in Section 5.A. The Policy is further intended to help protect students, faculty, staff, patients, and other constituents and the University from damages related to the fraudulent activity of identity theft.

This Policy will:

1. Identify patterns, practices, or specific activities ("Red Flags") that indicate the possible existence of identity theft with regard to new or existing covered accounts;
2. Detect Red Flags that have been incorporated into the Policy;
3. Respond appropriately to any Red Flags that are detected under the Policy;
4. Ensure periodic updating of the Policy, including reviewing the accounts that are covered and the identified Red Flags that are part of the Policy; and
5. Promote compliance with state and federal laws and regulations regarding identity theft protection.

### **SECTION 3: SCOPE**

This Identity Theft and Red Flag Policy applies to students, faculty, staff, patients, research participants, donors, and other constituents at the University.

## **SECTION 4: IDENTITY THEFT PREVENTION**

This policy should be read in conjunction with the University's Data Classification Policy (A110) and the HIPAA Transmission Security Policy (HST 18.0). If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor.

### **4.A: Confidential Information for the Purpose of the University's Identify Theft and Red Flag Policy**

Confidential Information includes data covered by Federal and State legislation such as FERPA, HIPAA, and the Data Protection Act or is legally covered by contract and must be protected at all times. The disclosure of this information may seriously damage or negatively impact the University.

#### **4.A.1: Definition of Confidential Information**

Confidential Information includes, but is not limited to, the following items whether stored in electronic or printed format:

##### **4.A.1.a: Credit and debit card information, including:**

1. Credit and debit card number (in part or whole)
2. Credit and debit card expiration date
3. Cardholder name
4. Cardholder address

##### **4.A.1.b: Tax identification numbers, including:**

1. Social Security number
2. Business identification number
3. Employer identification number

##### **4.A.1.c: Payroll information, including among other information:**

1. Paychecks
2. Pay stubs

##### **4.A.1.d: Flexible benefits plan check requests and associated paperwork**

**4.A.1.e:** Medical information for students, faculty, staff, patients, research participants, donors, and other constituents, including but not limited to:

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personal medical information

**4.A.1.f:** Personal banking information for any employee, student, customer, patient or constituent, including but not limited to:

1. Password/Log-In information for online banking.
2. Bank account number.
3. Routing number.

**4.B.: Other Information Commonly Used in Identity Theft**

**4.B.1:** The following information, even though it may otherwise be considered public or proprietary, is often used in conjunction with Confidential Information to commit fraudulent activity such as identity theft:

1. Date of birth
2. Address
3. Phone numbers
4. Maiden name
5. Names
6. Customer number
7. Driver's License Number

**4.C: Hard Copy Distribution and Storage**

All University personnel shall comply with the following requirements:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Confidential Information must be locked when not in use.
2. Storage rooms containing documents with Confidential Information and record retention areas must be locked at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas must be cleared of all documents containing Confidential Information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas containing Confidential Information must be erased, removed, or shredded when not in use.
5. University records may only be destroyed in accordance with the University's records retention policy and applicable law.
6. Documents containing Confidential Information must be disposed of in a secure manner. A secure manner includes destroying the documents using a cross-cut shredder or disposing of documents in an authorized disposal container.

#### **4.D: Electronic Distribution and Storage**

All University employees shall comply with the following policies:

1. Non-University email systems, including but not limited to, Hotmail, Yahoo, Google shall not be used to send Confidential Information. When using approved University e-mail systems to send Confidential Information internally the preferred mode is to encrypt or password protect such information.
2. Any Confidential Information sent to recipients externally (i.e. to non University of Miami email accounts) should be encrypted and sent only to approved recipients. Additionally, a statement such as this should be included in the e-mail:

*"The information contained in this transmission may contain privileged and confidential information protected by federal and state privacy laws. It is intended only for the use of the person(s) named above. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution or duplication of this communication is strictly prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message."*

3. Encryption technologies should be employed when Confidential Information is being stored on mobile devices such as laptops, backup media, DVDs, CDs, external hard drives, and thumb drives, among others.
4. Confidential Information should be encrypted when internally transmitted over an electronic communications network.
5. All hardware/storage media that will be repurposed for use within the University must be sanitized adhering to United States Department of Defense standards for properly erasing media (DOD 5220.22-M). The DOD standard recommends the approach of overwriting all addressable media locations, a minimum of three times, with a character, its complement, then a random character and verifying the process. If hardware will be disposed of, or will be transferred to a third party outside of the University, all storage media must be rendered unusable, adhering to government standards which requires degaussing and/or complete physical destruction.

#### **4.E.: Application of Other Laws and University Policies**

University personnel should make reasonable efforts to secure Confidential Information to the proper extent. Furthermore, this section should be read and applied in conjunction applicable laws and University policies. If an employee is uncertain of the Red Flag implications of a certain piece of information, he/she should contact the Executive Director of Treasury, or a designee of the Executive Director of Treasury, as set forth in Section 8.A.2, or the University's Office of Vice President and General Counsel.

## **SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION EFFORTS**

### **5.A: Covered accounts**

For the purpose of the University's Identity Theft and Red Flag Policy, a "covered account" includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing account maintained by the University for its students, faculty, staff, patients, and other constituents that meets the following criteria is covered by this Policy:

1. Accounts for which there is a reasonably foreseeable risk of identity theft; or
2. Accounts for which there is a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

### **5.B: Red Flags**

**5.B.1:** The following Red Flags are potential indicators of fraud. Any time a Red Flag, or a situation closely resembling a Red Flag, is apparent, it should be investigated for verification.

1. **Alerts, notifications, or warnings from a consumer reporting agency.** Examples of these Red Flags include the following:
  - a. A fraud or active duty alert included with a consumer report;
  - b. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;
  - c. A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act; and
  - d. A consumer report that indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    - i. A recent and significant increase in the volume of inquiries;
    - ii. An unusual number of recently established credit relationships;
    - iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
    - iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

2. **Suspicious documents.** Examples of these Red Flags include the following:
  - a. Documents provided for identification that appear to have been altered or forged;
  - b. The photograph or physical description on the identification is not consistent with the appearance of the student, faculty, staff, patient, and other constituent presenting the identification;
  - c. Other information on the identification is not consistent with information provided by the person opening a new covered account or student, faculty, staff, patient, and other constituent presenting the identification;
  - d. Other information on the identification is not consistent with readily accessible information that is on file with the University; and
  - e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
  
3. **Suspicious personally identifying information.** Examples of these Red Flags include the following:
  - a. Personally identifying information provided is inconsistent when compared against external information sources used by the University;
  - b. Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University;
  - c. Personally identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University;
  - d. The SSN provided is the same as that submitted by another student, faculty, staff, patient or constituent;
  - e. The person opening the covered account fails to provide all required personally identifying information on an application or in response to notification that the application is incomplete;
  - f. Personally identifying information provided is not consistent with personal identifying information that is on file with the University; and
  - g. When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

4. **Unusual use of, or suspicious activity related to, the covered account.** Examples of these Red Flags include the following:
- a. Shortly following the notice of a change of address for a covered account, the University receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account;
  - b. A covered account is used in a manner that is not consistent with established patterns of activity on the account;
  - c. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors);
  - d. Mail sent to the student, faculty, staff, patient or other constituent is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account;
  - e. The University is notified that the student, faculty, staff, patient, or other constituent is not receiving paper account statements;
  - f. The University is notified of unauthorized charges or transactions in connection with a covered account;
  - g. The University receives notice from students, faculty, staff, patient, or other constituents, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University; and
  - h. The University is notified by a student, faculty, staff, patient, or other constituent, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

## **SECTION 6: RESPONDING TO RED FLAGS**

**6.A:** Once a Red Flag, or potential Red Flag, is detected, the University should endeavor to act quickly as a rapid appropriate response can protect students, faculty, staff, patients, and other constituents and the University from damages and loss.

**6.A.1:** The University should quickly gather all related documentation, write a description of the situation, and present this information to the University's Executive Director of Treasury, or a designee of the Executive Director of Treasury, as set forth in Section 8.A.2, for determination.

**6.A.2:** University's Executive Director of Treasury, or a designee of the Executive Director of Treasury, shall complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

**6.B:** If a transaction is determined to be fraudulent, appropriate actions should be taken immediately. Actions may include:

1. Canceling the transaction;
2. Notifying and cooperating with appropriate law enforcement;
3. Determining the extent of liability of the University; and
4. Notifying the student, faculty, staff, patient, or other constituent that fraud has been attempted.

## **SECTION 7: PERIODIC UPDATES TO THE IDENTITY THEFT AND RED FLAG POLICY**

**7.A:** At periodic intervals as deemed necessary by the University, the Policy should be re-evaluated to determine whether all aspects of the Policy are up to date and applicable in the current operational environment.

**7.B:** Periodic reviews will include an assessment of which accounts are covered by the Policy.

**7.C:** As part of the review, red flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate.

**7.D:** Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the University and its students, faculty, staff, patients, and other constituents.

## **SECTION 8: POLICY ADMINISTRATION**

### **8.A: Involvement of management**

**8.A.1:** Establishment of the Identity Theft and Red Flag Policy is the responsibility of the University's Board of Trustees. The Board's approval of the initial policy must be appropriately documented and maintained.

**8.A.2:** Operational responsibility of the Policy, including but not limited to the oversight, development, implementation, and administration of the Policy, approval of needed changes to the Policy, and implementation of needed changes to the Policy, is delegated to the University's Executive Director of Treasury, or a designee of the Executive Director of Treasury,.

## **8.B: Employee training**

**8.B.1:** Training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by the University's Executive Director of Treasury, or a designee of the Executive Director of Treasury, that the employee may come into contact with accounts or personally identifiable information that may constitute a risk to the University or its students, faculty, staff, patients, and other constituents.

**8.B.2:** The University's Human Resources offices, in conjunction with department administrators, are responsible for ensuring that identity theft training is conducted for all employees for whom it is required.

**8.B.3:** Employees shall receive annual training in all elements of the Identity Theft and Red Flag Policy.

**8.B.4:** To ensure maximum effectiveness, employees shall continue to receive additional training as changes to the Policy are made.

## **8.C: Oversight of service provider arrangements**

**8.C.1:** The University shall endeavor to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

**8.C.2:** A service provider that maintains its own identity theft prevention Policy, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

**8.C.2:** Any specific requirements should be specifically addressed in the appropriate contract arrangements.

### ***Additional University Policies pertaining to the protection of sensitive information:***

Data Classification Policy A110

[http://www6.miami.edu/UMH/CDA/UMH\\_Main/0,1770,21542-1;65641-3,00.html](http://www6.miami.edu/UMH/CDA/UMH_Main/0,1770,21542-1;65641-3,00.html)

HIPAA Transmission Security Policy (HST 18.0)