

**Identity Theft Prevention**

**Program Procedures**

**Purpose**

Through the Identity Theft Prevention Program procedures outlined in this document, The University of Southern Mississippi intends to comply with the FTC Red Flags Rule identity theft detection and prevention guidelines. The purpose of University departments establishing effective identity theft prevention programs is to secure personal identifying information provided to the University by individual students, faculty, staff, or others, and thereby prevent its unauthorized and fraudulent use.

**Identification of Red Flags**

In order to identify relevant red flags, the University has considered the types of covered accounts offered and maintained, methods provided to open accounts, methods provided to access accounts, and previous experiences with identify theft. The University identifies the following red flags in each of the listed categories:

* Suspicious Documents

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing customer information (such as if a person’s signature on a check appears forged); and
4. An application for service that appears to have been altered or forged.

* Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates),
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application),
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent,
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address),
5. Social security number presented that is the same as one given by another student,
6. An address or phone number presented that is the same as that of another person,
7. A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law, social security numbers must not be required), and
8. A person’s identifying information is not consistent with the information that is on file for the student.

* Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the account holder's name,
2. Payments stop on an otherwise consistently up-to-date account,
3. Account used in a way that is not consistent with prior use (example: very high activity),
4. Mail sent to the student is repeatedly returned as undeliverable,
5. Notice to the University that a student is not receiving mail sent by the University,
6. Notice to the University that an account has an unauthorized activity,
7. Breach in the University’s computer system security, and
8. Unauthorized access to or use of the student’s account information.

* Alerts from Others

1. Notice to the University from a faculty, staff, or student, identity theft victim, law enforcement, or other person regarding possible identity theft in connection with covered accounts.

**Detecting Red Flags**

* Student Enrollment:

In order to detect any of the Red Flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the student’s identity at time of issuance of student identification card (review of driver’s license or other government-issued photo identification).

* Existing Accounts:

In order to detect any of the Red Flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email)
2. The identification should be scrutinized to verify that it has not been altered or forged
3. That the picture on the identification provided matches the appearance of the student presenting the identification.
4. That the information on the identification is consistent with other information on file at the University, particularly on the student’s account.
5. Not share any more information with a customer than is documented in the student system if there is a full FERPA restriction on the account. If additional information is requested, the student should be forwarded to the Registrar’s Office for assistance.

* Consumer Credit Report Requests

In the event credit reports are required for an employment position, University personnel will take the following steps to detect red flags to identify address discrepancies:

1. Require written address verification from any applicant at the time the request for the credit report is made to the consumer reporting agency, and
2. Verify that the credit report pertains to the applicant for whom the requested report was made in the event of an address discrepancy. Personnel should notify the consumer- reporting agency and provide the relevant address information.

**Response Actions**

* In the event the University detects any identified Red Flags, the University shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

1. Continue to monitoring a covered account for evidence of identity theft;
2. Report to management if an account is used in a manner not consistent with regular pattern of activity;
3. Call or email the student if mail addressed to the student is returned twice as undeliverable although transactions continue to be conducted with their account.
4. Investigate and verify the correctness of unauthorized charges or transactions assessed by Business Services in connection with a student’s account. If there are questions regarding the correctness of departmental charges, refer them on to the appropriate department for resolution;
5. Notify supervisor immediately if the University is notified by a student, a victim of identity theft, a law enforcement authority, or any other person that it has opened, discovered, or manipulated a fraudulent account for a person engaged in identity theft;
6. Determine that no response is warranted under the particular circumstances.

* Do not provide any information to an individual claiming to be the victim of identity theft without them providing evidence of a Police Case Number or an FTC affidavit of identity theft. If a student needs assistance of this type, the request must be in writing with detailed information requested as well as proof of positive identification and proof of claim of identity theft (police report or FTC affidavit).

1. Ensure that customers who call are not given information on an account if they cannot provide the EmpID or any other personal identifying item and student’s name. Be cautious about callers who attempt to get financial information without providing any substantive knowledge about the account.
2. Business Services staff should not respond to any questions from customers related to any medical type services. All calls of this type should be immediately referred to the department in question.

**Staff Training and Program Evaluation**

* University personnel responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected.

1. University personnel are expected to notify the Program Administrator once they become aware of an incident of identity theft.
2. At least annually, the Program Administrator shall report on compliance with the Program. The report will address such issues as effectiveness of the guidance in addressing the risk of identity theft in connection with the opening and maintenance of covered accounts, service provider arrangements, significant incidents involving identity theft, and recommendations for changes to the Program.
3. In accordance with the IT Security Policies, electronic breaches, regardless of the data type, must be reported to the IT Security Officer. Response to electronic breaches will be in line with the Security Incident Management policy. Depending on the nature of the breach, other areas of the University may be involved, as designated by the program administrator.

**Service Provider Arrangements**

* In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the University will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

1. Require, by contract, that the service provider has such policies and procedures in place;
2. Require, by contract, that the service provider review the University’s Program and report any red flags to the responsible Program Administrator or the University employee with primary oversight of the service provider relationship.