



SUBJECT: Identity Theft Prevention	Effective Date: 6-24-09	Policy Number: 2-105
	Supersedes:	Page Of 1 9
	Responsible Authority: Vice President and General Counsel	

APPLICABILITY/ACCOUNTABILITY:

This policy applies to all UCF faculty members, Administrative and Professional staff, and University Support Personnel System employees.

POLICY STATEMENT:

The University of Central Florida maintains an Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

DEFINITIONS:

Identity theft. A fraud committed or attempted using the identifying information of another person without authority.

Red flag. A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Covered account. An account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. A covered account is also an account for which there is a foreseeable risk of identity theft.

Program administrator. The individual designated with primary responsibility for oversight of the identity theft prevention program.

Identifying information. Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, individual identification number, computer's Internet Protocol address, or routing code.

PROCEDURES:

I. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, the university is required to establish an identity theft prevention program tailored to its size, complexity, and the nature of its operation. This program must contain reasonable policies and procedures to:

- A. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the program.
- B. Detect red flags that have been incorporated into the program.
- C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.
- D. Ensure the program is updated periodically to reflect changes in risks to individuals or to the safety and soundness of the individuals from identity theft.

II. Identification of Red Flags

In order to identify relevant red flags, the university considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with identity theft. The university identifies the following red flags in each of the listed categories:

- A. Notifications and Warnings from Credit Reporting Agencies
 1. Report of fraud accompanying a credit report.
 2. Notice or report from a credit agency of a credit freeze on an applicant.
 3. Notice or report from a credit agency of an active duty alert for an applicant.
 4. Receipt of a notice of address discrepancy in response to a credit report request.
 5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.
- B. 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 identifying information.
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information provided (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 person.
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.
8. A person's identifying information is not consistent with the information that is on file for that person.

D. Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the person'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.
4. Mail sent to the individual is repeatedly returned as undeliverable.
5. Notice to the university that a person is not receiving mail sent by the university.
6. Notice to the university that an account has unauthorized activity.
7. Breach in the university's computer system security.
8. Unauthorized access to or use of student account information.

E. Alerts from Others

1. Notice to the university from a individual, identity theft victim, law enforcement official, or other person that the university has opened or is maintaining a fraudulent account for a person engaged in identity theft.

III. Detecting Red Flags

A. Enrollment

To detect any of the red flags identified above associated with the enrollment of an individual, 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.
2. Verify the person's identity at time of issuance of identification card (review of driver's license or other government-issued photo identification).

B. Existing Accounts

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 the individual if they request information (in person, via telephone, via facsimile, via email).
2. Verify the validity of requests to change billing addresses by mail or email and provide the individual a reasonable means of promptly reporting incorrect billing address changes.
3. Verify changes in banking information given for billing and payment purposes.

C. Consumer (Credit) Report Requests

To detect any of the red flags identified above for an employment or volunteer position for which a credit report is sought, university personnel will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency.
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the university has

2-105 Identity Theft Prevention 4

reasonably confirmed is accurate.

IV. Preventing and Mitigating Identity Theft

In the event that university personnel detect any identified red flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the red flag:

A. Prevent and Mitigate

1. Continue to monitor a covered account for evidence of identity theft.
2. Contact the individual (for which a credit report was run).
3. Change any passwords or other security devices that permit access to covered accounts.
4. Not open a new covered account.
5. Provide a new identification number.
6. Notify the program administrator for determination of the appropriate step(s) to take.
7. Notify law enforcement.
8. File or assist in filing a Suspicious Activities Report.
9. Determine that no response is warranted under the particular circumstances.

B. Protect Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the university will take the following steps with respect to its internal operating procedures to protect identifying information:

1. Ensure that its Web site is secure or provide clear notice that the Web site is not secure.
2. Subject to state record retention requirements, ensure complete and secure destruction of paper documents and computer files containing account information when a decision has been made to no longer maintain such information.
3. Ensure that office computers with access to covered account information are password protected.

4. Avoid use of social security numbers.
5. Ensure that computer virus protection is up to date.
6. Require and keep only the kinds of individual information that are necessary for university purposes.

C. Program Administration

1. Oversight

Responsibility for developing, implementing, and updating this program lies with an Identity Theft Committee for the university. The committee is headed by a program administrator who is the University Controller or designee and should include representation from affected units, such as:

- a. Finance and Accounting
- b. Student Financial Assistance
- c. General Counsel
- d. Information Technologies and Resources
- e. Admissions: Undergraduate Admissions, College of Graduate Studies, College of Medicine
- f. UCF Foundation
- g. Registrar's Office
- h. Business Services
- i. Human Resources

The program administrator will be responsible for ensuring availability of appropriate training on the program. University Audit will be responsible for reviewing any reports regarding the detection of red flags and ensuring that the action taken by management is effective in preventing and mitigating particular circumstances.

2. Staff Training and Reports

University staff responsible for implementing the program shall be trained in the detection of and responses to red flags. University staff shall be trained, as necessary, to effectively implement the program. University employees are expected to notify University Audit once they become aware of an incident of identity theft or of the university's failure to comply

2-105 Identity Theft Prevention 6

with this program (see UCF Policy 2-800 *Fraud Prevention and Detection*). At least annually or as otherwise requested by the program administrator, university staff responsible for development, implementation, and administration of the program shall report to the committee on compliance with this program. The report should address such issues as effectiveness of the policies and procedures 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, management responses, and recommendations for changes to the program.

3. Service Provider Arrangements

In the event the university engages a service provider in performing 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.

- a. Require, by contract, that service providers have such policies and procedures in place.
- b. Require, by contract, that service providers review the university's program and report any red flags to the program administrator or the university employee with primary oversight of the service provider relationship.

4. Non-disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific red flag identification, detection, mitigation, and prevention practices may need to be limited to the committee members who developed this program and to those employees who need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered confidential and should not be shared with other university employees or the public, unless required by applicable law. The program administrator shall identify those documents and practices which should be maintained in a confidential manner.

5. Program Updates

The committee will periodically review and update this program to reflect changes in risks to individuals and the soundness of the university from identity theft. In doing so, the committee will consider the university's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the university's business arrangements with other entities. After considering these factors, the program administrator will determine whether changes to the program, including the listing of red flags, are warranted. If warranted, the committee will update the program.

RELATED DOCUMENTS:

- Federal Trade Commission's Red Flags Rule, 16 C.F.R. 681
- Section 114 of the Fair and Accurate Credit Transactions Act, 15 U.S.C. 1681m(e)
- University Policy 2-800 *Fraud Prevention and Detection*:
<http://www.policies.ucf.edu/documents/2-800FraudPreventionandDetectionFINAL.pdf>

INITIATING AUTHORITY: Vice President and General Counsel

POLICY APPROVAL (For use by the Office of the President)	
Policy Number: 2-105	
Initiating Authority: <u><i>[Signature]</i></u>	Date: <u>7-30-09</u>
Policies and Procedures Review Committee Chair: <u><i>[Signature]</i></u>	Date: <u>7-15-09</u>
President or Designee: <u><i>[Signature]</i></u>	Date: <u>8/3/09</u>