Eastern Kentucky University
Policy and Regulation Library

6.#.#P
Volume 6, Volume Title: Financial Affairs
Chapter #, Chapter Title
Section #, Name: **Identity Theft Prevention Policy**
Approval Authority: Board of Regents
Responsible Executive:
Responsible Office(s):
Effective: **Expires:**
Last Revised: **Next Review Date:**

Identity Theft Prevention Policy

Statement

The Federal Trade Commission and Federal banking agencies issued a regulation known as the Red Flag Rules as part of the Fair and Accurate Credit Transaction Act of 2003 intended to reduce the risk of identity theft. Under this regulation, Universities are required to establish an 'Identity Theft Prevention Program" to protect members of the University Community by reducing risk from identity theft fraud and to minimize potential damage to the University from fraudulent acts. The program includes policies and procedures to detect potential indications of identity theft, respond to potential or actual incidents of identity theft implement employee training and develop internal reports to mitigate risks associated with identity theft.

Entities Affected

All University students, faculty, staff, patients and other constituents including contractors serving in the University units having access to "identifying information" in a "covered account" as defined herein.

Background

No policy previously existed.

Policy Procedures

I. Identifying Red Flags

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, the methods it provides to open these accounts, the methods it provides to access its accounts

and its previous experiences with Identity Theft. The following are relevant Red Flags, in each of the listed categories, of which employees should be aware and for which employees should be diligently monitoring:

A. Suspicious Documents

- Documents provided for identification appear altered, forged, or inauthentic;
- The photograph or physical description on identification provided is not consistent with the appearance of the individual presenting the identification; or
- Other information on the identification provided is not consistent with information provided by the person presenting the identification or is not consistent with readily accessible information on file (such as a signature).

B. Suspicious Personal Identifying Information

- Identifying information provided is inconsistent when compared against external information sources used by the University. For example, the Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File;
- Identifying information provided by the individual is not consistent with other personal identifying information provided by the individual. For example, inconsistent birth dates;
- The individual fails to provide all required personal identifying information;
- Identifying information presented is the same as information shown on other applications that were found to be fraudulent;
- An address or phone number presented that is the same as that of another person;
- When using security questions (mother's maiden name, pet's name, etc.), the individual cannot provide authenticating information beyond that which generally would be available; or
- Personal identifying information provided is not consistent with personal identifying information that is on file with the University.

C. Suspicious Covered Account Activity or Unusual Use of Account

- Change of address for an account followed by a request to change the account holder's name;
- Payment stops on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use (example; very high activity);
- The University is notified of unauthorized charges or transactions in connection with an individual's Covered Account;
- The University receives notice from victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts held by the University;
- A breach in the University's computer system security; or
- Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Covered Account.

D. Alerts from Others

- Notice to the University from a customer, identity theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

E. Other Information Commonly Used in Identity Theft

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:

- payroll information, including but not limited to: paychecks, pay stubs, or flexible benefits plan check requests and associated paperwork;
- medical information for any employee or customer, including but not limited to: health care provider names and claims, insurance claims, prescriptions, and any related personal medical information; or
- other personal information belonging to students, faculty, staff, patients, and other constituents, including but not limited to: name, date of birth, address, phone numbers, maiden name, customer number, bank routing number, or account number.

II. Detecting Red Flags

A. New Covered Accounts

In order to detect Red Flags associated with the opening of a new covered account, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

- require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;
- verify the customer's identity (for instance, review a driver's license or other identification card);
- independently contact the customer.

B. Existing Covered Accounts

In order to detect Red Flags for an existing account, University employees should:

- verify the identification of person(s) who request information (in person, via facsimile, or via official EKU email accounts);
- verify the validity of requests to change billing addresses; and
- verify changes in banking information given for billing and payment purposes.

Any time a credit report is sought in connection with covered accounts, University employees should 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. In the event of notice of an address discrepancy in a credit report, University employees should verify whether the report pertains to the individual for whom the report was requested. If it is determined that the address provided by the credit reporting agency is inaccurate, University employees should report to the credit reporting agency an address that the University has confirmed is accurate.

III. Responding to Red Flags

Once a Red Flag, or potential Red Flag, is detected, University officials should act quickly to protect the University and its students, faculty, staff, patients, and other constituents from damages and loss. When fraudulent activity is detected, University officials shall act in accordance with the facts known. Actions may include one or more of the following:

- continue to monitor the account for evidence of identity theft;
- contact the individual;
- change any passwords, security codes, or other security devices that permit access to an account;
- not attempt to collect on a Covered Account or otherwise place into debt collection;
- not open a new Covered Account;
- notify and cooperate with appropriate law enforcement authorities;
- close a Covered Account and/or reopen a Covered Account with a new account number;
- determine that no response is warranted under the particular circumstances;
- cancel the transaction; and/or
- determine the extent of liability of the University.

IV. Program Administration

A. Delegation

The responsibility for developing, overseeing and updating this Identity Theft Prevention Program lies with the Vice President for Financial Affairs.

Operational responsibility for the Program, including implementation, ongoing administration, recommendation of needed changes, and implementation of needed changes, is delegated through the Vice President of Financial Affairs to the departments with Covered Accounts.

B. Employee training

Training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by the departments with Covered Accounts, that the employee may come into contact with Covered Accounts or personally identifiable information that may constitute a risk to the University or its students, faculty, staff, patients, and other constituents. Employees shall receive training, as necessary, in all elements of the Program. To ensure maximum effectiveness, employees shall continue to receive additional training as changes to the Program are made.

C. Oversight of Service Provider Arrangements

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. The University shall require, by contract, that service providers who perform an activity in connection with one or more Covered Accounts ensure that such activity shall be conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the Red Flag Rules and validated by appropriate due

diligence, may be considered to be meeting these requirements. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

D. Covered Accounts Identified by the University

Each unit identified by the University as having a Covered Account shall submit its most recent written **"Red Flag Compliance" Identity Theft Prevention Program** to the Vice President of Financial Affairs. Units identified by the University as having covered accounts are listed in *Appendix A,* which may be supplemented from time to time, as needed. The written **"Red Flag Compliance" Identity Theft Prevention Program** of each unit having a Covered Account(s) shall specifically identify the Covered Account(s), and describe the:

1. procedures to detect potential indications of identity theft with regard to new and existing accounts;

2. procedures to respond to potential or actual incidents of identity theft;

3. employee training and internal reports the unit uses to mitigate risks associated with identity theft; and

4. steps taken to ensure a service provider complies with identity theft standards, if any Covered Account data is shared with a service provider.

E. Reporting

Each unit identified as having a Covered Account(s) shall report the effectiveness of the unit's Program to the Vice President of Financial Affairs. The Vice President of Financial Affairs shall annually report to the President on the operations and effectiveness of the Program.

Specific incidents of identity theft shall be reported to the Office of Internal Audit in accordance with the University Fiscal Misconduct Policy.

V. Periodic Review and Updates to the Program

The Program shall be reviewed periodically as may be deemed prudent based on current law; changes in technology; the type of accounts established by the University; the University's experience with identity theft activities; changes in identity theft methods; changes in identity theft detection, mitigation, and prevention methods; changes in types of accounts the University maintains; changes in the University's business arrangements with other entities; and any changes in legal requirements in the area of identity theft. Periodic reviews shall include an assessment of which accounts are covered under the policy and changes to Red Flags. Appropriate action to be taken in the event that fraudulent activity is discovered also may require revision to reduce damage to the University and the individuals within the University community. The Vice President of Financial Affairs shall present any recommended changes to the President for approval.

Definitions

Identity theft- an attempted or committed fraud 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- 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, and other constituents that meets the following criteria is covered by this Program:

1. Accounts for which there is a reasonably foreseeable risk of identity theft; and

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.

Identifying information- means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to:

- 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
- student identification number,
- computer's Internet Protocol address, or routing code.

Responsibilities

Vice President for Financial Affairs	• Has administrative responsibility for developing, implementing, overseeing and updating the Program • Reports annually to the President on the operations and effectiveness of the Program. • Presents any recommended changes to Program to the President for approval
Office of Internal Audit	• Reviews reports of specific incidents of identity theft
Units having Covered Accounts or Having an effect on Covered Accounts	• Has operational responsibility of the Program • Determines training to be conducted for all employees for whom it is reasonably foreseeable, may come into contact with Covered

	Accounts or personally identifiable information that may constitute a risk to the University or its students, faculty, staff, patients, and other constituents
Students, faculty, staff, patients, and other constituents of the University	• Reports specific incidents of identity theft to the Office of Internal Audit

Violations of the Policy

Violations of this policy will be handled through normal University disciplinary processes.

Interpreting Authority

Vice President of Financial Affairs

Statutory or Regulatory References

"Red Flag Rules" Fair Credit Reporting Act 16 CFR 681.1

Relevant Links

- Fiscal Misconduct Policy: http://www.hr.eku.edu/Policy_and_Procedure/docs/Fiscal_Misconduct_Policy_Approved_11-8-2002.pdf
- Name and Address Change Policy (currently under review)

Policy Adoption Review and Approval

APPENDIX A

UNITS IDENTIFIED AS HAVING COVERED ACCOUNTS

1. Office of Financial Affairs
2. Student Accounting Services
3. Colonel 1 Card
4. Division of Financial Assistance
5. Bluegrass Community Health Center
6. The Office of the Registrar
7. The Office of Admissions
8. Alumni Relations
9. Human Resources
10. Speech, Language and Hearing Clinic
11. Psychology Clinic