# FCR 13

Office of the President
September 15, 2009

Members, Board of Trustees:

APPROVAL FOR PROPOSED ADMINISTRATIVE REGULATION: UNIVERSITY OF KENTUCKY IDENTITY THEFT PROGRAM ("RED FLAGS RULE")

Recommendation: that the Board of Trustees approve Administrative Regulation (AR) 8:8, Identity Theft Program ("Red Flags Rule"); delegate to the President the authority to amend the Administrative Regulation in the future; and delegate, through the President, to the Executive Vice President for Finance and Administration the operational responsibility for the program, including but not limited to: oversight, development, implementation, and continuing administration. The proposed AR is attached as Exhibit A.

Background: As part of the Fair and Accurate Credit Transactions (FACT) Act of 2003, the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) issued regulations (the Red Flags Rules) requiring financial institutions and creditors to develop and implement written identity theft prevention programs. The programs must be in place by November 1, 2009, and must provide for the identification, detection, and response to patterns, practices, or specific activities - known as "red flags" – that could indicate identity theft. The programs also must include provisions defining the oversight and ongoing administration of the program.

AR 8:8 establishes the University's written identity theft prevention program in compliance with these federal regulations. The University engages in activities which are subject to the federal Red Flag Rules, such as operating tuition payment installment plans, allowing students to carry balances on accounts, and maintaining health care patient accounts. Therefore, the Board of Trustees is required to develop and implement an identity theft program in compliance with the federal regulations.

In order to have the flexibility to amend the regulation rapidly to correspond to additional regulatory guidance, it is recommended that the Board of Trustees delegate to the President the authority to amend the AR and to the Executive Vice President for Finance and Administration the responsibility for program administration. The President shall report any material amendments to the Board.

---

Action taken: ☑ Approved ❑ Disapproved ❑ Other _____

# IDENTITY THEFT PREVENTION PROGRAM
# (APPROVED BY THE BOARD OF TRUSTEES)

## I. Introduction

The Federal Trade Commission (FTC) and the federal banking agencies issued regulations (the "Red Flags Rules"), as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003, requiring financial institutions and creditors to develop and implement written identity theft prevention programs.

This Administrative Regulation establishes the University's identity theft prevention program (the "Program") in accordance with the federal regulations. The Program is designed to: detect, prevent, and mitigate identity theft in connection with new or existing covered accounts; help protect students, faculty, staff, other constituents, and the University from damages related to the fraudulent activity of identity theft; provide for continued administration of the Program; and promote compliance with state and federal laws and regulations regarding identity theft protection.

## II. Definitions

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

B. A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

C. 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 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.

D. "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, patient account number, health insurance number, student identification number, computer's Internet Protocol address, credit card number, or routing code.

III. Red Flags

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

A. Suspicious Documents

1. Documents provided for identification appear altered, forged, or inauthentic;

2. The photograph or physical description on identification provided is not consistent with the appearance of the individual presenting the identification; or

3. 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

1. Personal 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;

2. Personal identifying information provided by the individual is not consistent with other personal identifying information provided by the individual. For example, there is a lack of correlation between the SSN range and date of birth;

3. The individual fails to provide all required personal identifying information;

4. 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

5. Personal identifying information provided is not consistent with personal identifying information that is on file with the University.

C. Unusual Use of, or Suspicious Activity Related to, a Covered Account

1. The University is notified of unauthorized charges or transactions in connection with an individual's Covered Account;

2. 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;

3. A breach in the University's computer system security; or

4. Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Covered Account.

D. 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:

1. Payroll information, including but not limited to: paychecks, pay stubs, or flexible benefits plan check requests and associated paperwork;

2. 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

3. 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, credit card number, or account number.

VII. Detecting Red Flags

A. New Covered Accounts

In order to detect Red Flags, University employees should verify the identity of the person(s) opening a new account by requiring certain identifying information such as name, date of birth, academic records, residential or business address, or other identification as appropriate; and by verifying the person's identity (for instance, review of driver's license or other government-issued photo identification card).

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 telephone, via facsimile, or via email); and verify the validity of requests to change billing addresses and 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.

VIII. Responding to Red Flags

Once a Red Flag, or potential Red Flag, is detected, University officials should act quickly to protect students, faculty, staff, patients, and other constituents and the University 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:

- 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.

X. Program Administration

A. Delegation

Establishment of the initial Identity Theft Prevention Program is the responsibility of the University's Board of Trustees. Thereafter, the President is authorized to make amendments to this regulation, upon recommendation by the Executive Vice President

for Finance and Administration, and as will conform to current law and to reflect risks to covered accounts.

Operational responsibility for the Program, including but not limited to oversight, development, implementation, ongoing administration, recommendation of needed changes, and implementation of needed changes, is delegated through the President to the Executive Vice President for Finance and Administration, or designee.

B. Employee training

Training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by the Executive Vice President for Finance and Administration, or designee, 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. Human Resources, in coordination with other appropriate units, is responsible for providing training for all employees for whom it is required. 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 Office of the Treasurer. 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. Policies and procedures to detect potential indications of identity theft with regard to new and existing accounts;

2. Policies and 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.

D. Reporting

Each unit identified as having a Covered Account(s) shall report incidents of identity theft and the effectiveness of the unit's Program to the Executive Vice President for Finance and Administration, or designee. In addition, units having Covered Account(s) in clinical areas shall also report incidents related to health information privacy or security to the appropriate UKHealthCare unit (e.g., Corporate Compliance/Privacy, IT Security). The Executive Vice President for Finance and Administration shall annually report to the President on the operations and effectiveness of the Program.

IX. 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 Executive Vice President for Finance and Administration shall present any recommended changes to the President for approval.

XI. Securing Identifying Information

A. Hard Copy

All identifying information concerning Covered Accounts shall be secured by the following means:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Identifying Information must be locked when not in use.

2. Storage rooms containing documents with Identifying 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 Identifying Information when not in use.

4. Whiteboards, dry-erase boards, writing tablets, etc. containing Identifying Information and located in common shared work areas must be erased, removed, or shredded when not in use. Whiteboards, dry-erase board, etc., located in clinical areas shall also adhere to University privacy policies with regard to patient information.

5. University records may only be destroyed in accordance with the University's records retention policy and applicable law.

6. Documents containing Identifying Information must be destroyed in a secure manner, and in accordance with applicable University policy and procedure.

B. Electronic

All University employees are expected to be familiar with and follow the University's *Policy Governing Access to and Use of University Information Technology Resources* (AR 10:1) (http://www.uky.edu/Regs/files/ar/ar064.pdf) and other applicable electronic data security policies (http://www.uky.edu/UKIT/policies.htm).

## XII. Application of Other Laws and University Policies

University personnel should make reasonable efforts to secure identifying information. Furthermore, this regulation should be applied in conjunction with the Family Education Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Kentucky Open Records Act, and other applicable laws and University policies. If an employee is uncertain of the confidentiality of a particular piece of information, he or she should contact the University's Office of Legal Counsel, or for clinical areas the Office of Corporate Compliance/Privacy.

References:

- Fair and Accurate Credit Transactions (FACT) Act of 2003
- Red Flag Rules (16 C.F.R. 681 – Federal Trade Commission)
- Family Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Kentucky Revised Statutes, Chapter 61 (Kentucky Open Records Act)
- *AR II-1.7-2, Policy Governing Access to and Use of University Information Technology Resources*

- University Information Technology Security Policies

## APPENDIX "A"

University of Kentucky units identified as having covered accounts:

1. Student Billing Services/Student Financial Aid – Student Accounts and Loan Accounts
2. Dining and Plus Account Office – Plus Accounts
3. Hospital – Hospital Patient Accounts
4. University Health Service – Student Health Patient Accounts
5. College of Dentistry – Dentistry Patient Accounts
6. Central Kentucky Management Services, Inc. (CKMS) – Active Patient Accounts and Bad Debt Accounts
7. Kentucky Medical Services Foundation (KMSF) – KMSF Patient Accounts