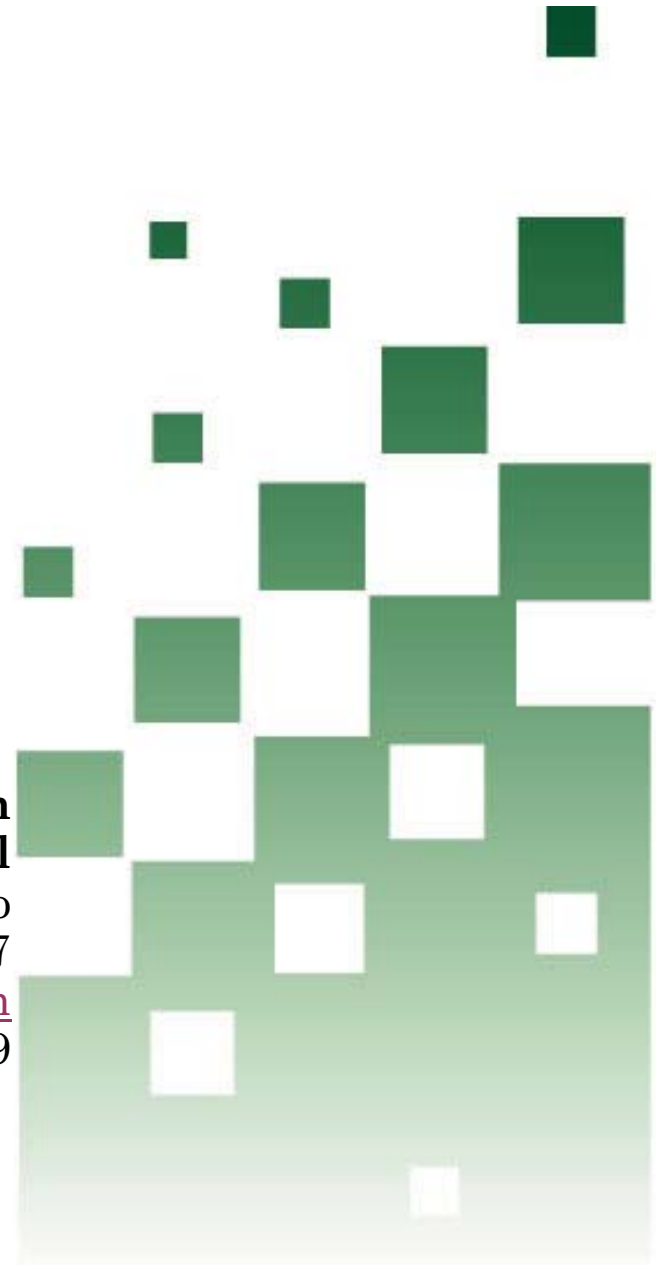




**RED FLAGS RULE:
Steps to Achieve Compliance
and
Protect, Students, Parents
and Universities
from Identity Theft**

Benita Kahn
Vorys Legal Counsel
Columbus, Ohio
(614) 464-6487
bakahn@vorys.com
January 2009



What is Identity Theft?

- ◆ Fraud committed or attempted by using identifying information of another person without authority
- ◆ It can include social security numbers, birth dates, driver's license information, account numbers
- ◆ Students and parents are victimized due to time and expenses incurred to correct their personal information
- ◆ Universities/colleges are victimized when they cannot collect the amount owed for goods and services



FTC's Red Flags Regulations

- ◆ Fair and Accurate Credit Transactions Act of 2003 (FACTA) required regulations from FTC to mitigate incidents of identity theft
- ◆ Final Rules published November 2007 include 3 duties
 - Address discrepancy notification - 16 CFR 681.1
 - Red Flags Program - detection, prevention and mitigation of identity theft – 16 CFR 681.2
 - Card Issuers regarding changes of address – 16 CFR 681.3

FTC's Red Flags Regulations

- ◆ Mandatory compliance by **November 1, 2008**
 - Address Discrepancy
 - Card Issuers

Red Flags Program

- **May 1, 2009**
October 22nd FTC announced it would suspend enforcement of Red Flags Policy Rule until this date



Red Flags Program

What is a Red Flag?

A suspicious circumstance that should prompt the university or college to be alert for possible identity theft





Red Flags Program

- ◆ **FTC's Stated Purpose of the Red Flags Program Rule**
 - To detect and stop identity thieves using someone else's identifying information at your institution to commit fraud.
 - Distinct from data security

Red Flags Program

How Do You Know if the Red Flags Program Rule Applies to your University

1. Is your university/college a “creditor”?
2. Is your university/college subject to enforcement under the FCRA by the FTC?
3. Does your university/college have “covered accounts”?



Red Flags Program

Is your university/college a “creditor”?

- ◆ Any person who regularly extends, renews or continues credit
 - Includes the right granted by the creditor to purchase services and defer payment for those services
- ◆ Any person who arranges for the extension, renewal or continuation of credit
- ◆ Any assignee of a creditor if they participate in the decision



Red Flags Program

Is your university/college subject to enforcement under the FCRA by the FTC?

- ◆ The FTC has the authority to enforce against any person that violates the FCRA *“irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act”*
- ◆ Therefore, the FTC can enforce FCRA violations against non-profit entities

Red Flags Program

Do you have “covered accounts”?

First, what is an account?

A continuing relationship established by a person with a creditor to obtain a product or service for personal, household or business purposes.

- Specifically includes extension of credit for property or services that involves deferred payments



Red Flags Program

Do you have “covered accounts”?

Second, what is a “covered account”?

- ◆ A consumer account designed to permit multiple payments and transactions

or

- ◆ Any other account for which there is a reasonably foreseeable risk from identity theft

Red Flags Program

What are the Program Requirements?

- ◆ Conduct periodic assessment to determine if you have covered accounts
- ◆ Implement a written Identity Theft Prevention Program to detect, prevent and mitigate identity theft in connection with:
 - Opening of a covered account
 - Any existing covered account
- ◆ Program must be appropriate to size and complexity of creditor and nature and scope of activities surrounding covered accounts
 - Must be consistently applied



Red Flags Program

Steps to Compliance

- ◆ Creating Program
 1. Identify Covered Accounts
 2. Identify Relevant Red Flags
 3. Detect Red Flags
- ◆ Administering Program
 1. Obtain approval of Program
 2. Oversee Program
 3. Train Employees
 4. Oversee Service Providers
 5. Provide Reports and Update Program

Red Flags Program

Detail on identifying Red Flags

- ◆ An alert is received (fraud/active duty)
- ◆ Consumer report indicates activity inconsistent with usual pattern
- ◆ Documents appear to be altered or destroyed and reassembled
- ◆ SSN is same as SSN provided by others or is invalid
- ◆ Account that is inactive for relatively long period is used



Red Flags Program

Detail on preventing and mitigating identity theft through your Program

- ◆ Monitor covered accounts
- ◆ Evaluate if red flag detected needs further review
- ◆ Contact student/parent if necessary
- ◆ Change passwords and security codes
- ◆ Create new account with new numbers
- ◆ Decline to open account or close existing
- ◆ Don't attempt to collect on account
- ◆ Notify law enforcement

Red Flags Program

Administering the Program

- ◆ Once created, Program must be approved by Board or appropriate Committee of Board prior to implementation
- ◆ Ongoing responsibility required by Board, appropriate Committee of the Board or a designated senior management



Red Flags Program

Administering the Program

- ◆ Oversight requires assigning responsibility to individual(s) with authority to review and revise Program
- ◆ Oversight should include factors of need to update
 - Actual instances of identity theft
 - Changes in methods of identity theft
 - Changes in types of covered accounts maintained
 - Changes in business arrangements (joint ventures)
- ◆ Annual written report should include:
 - effectiveness of Program and procedures
 - service provider arrangements
 - significant incidents, if any
 - recommendation for material changes

Red Flags Enforcement

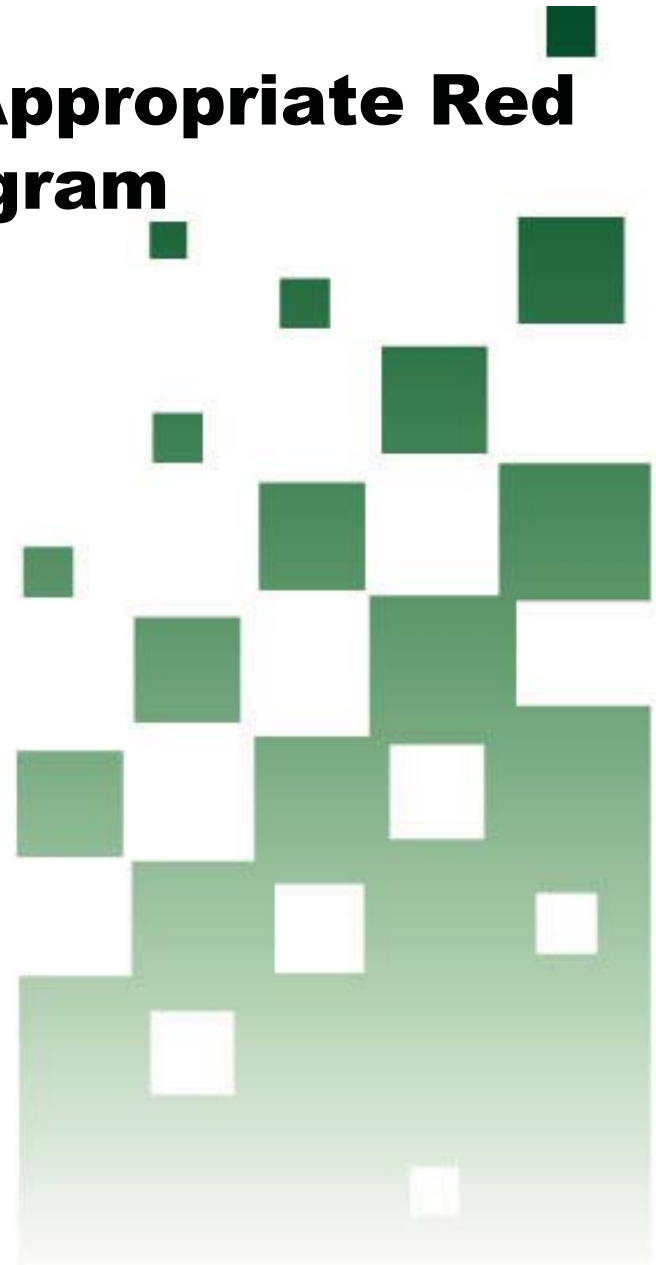
- ◆ Administrative enforcement under Section 621 of FCRA
- ◆ No private right of action
- ◆ State Attorneys General
- ◆ Civil penalties, but no criminal penalties



How to Develop an Appropriate Red Flags Program

GENERAL RULE:

Each university or college that is a “creditor” with covered accounts must *develop and implement* a Written Identity Theft Program that is appropriate to the size and complexity of the university or college.



Seven Steps to Compliance

1. Analyze the size and complexity of your university or college and your “covered accounts.”
2. Determine the existing policies that control foreseeable risks of identity theft.
3. Develop a list of “red flags” (risk factors) and how to detect.



Seven Steps to Compliance

4. Establish the procedures that should be followed when a red flag is detected.

5. Train your Employees.

6. Determine how the plan will be continually administered and regularly updated to reflect changes in risk.

7. Managing outside service providers.



Step One: ANALYZE the size and complexity of your university or college and your covered accounts

CONSIDER:

- Size and type of university or college operations
- Size of university or college account systems
- Previous experience with identity theft
- Methods available for opening university or college accounts
- Methods available for accessing university or college accounts

Step One: ANALYZE the size and complexity of your university or college and your covered accounts

CONSIDER the *nature* and *scope* of university or college activities:

- Federal Perkins Loan Program
- Small institutional loan program
- Tuition payment plans
- Accounts where there is foreseeable risk, including reputation and litigation risks to the university

Step Two: Determine existing policies that control foreseeable risks of identity theft

CONSIDER:

- Controls over parents' access to students non-directory information (grades, academic standing)
- Mechanisms that allow payment of tuition by parents or parties other than the student
- Previous experiences with identity theft
- Policies to comply with FERPA
- Student health programs and HIPAA compliance in place



Step Three: Develop a list of Red Flags (risk factors)

CONSIDER:

- Address discrepancies
- Suspicious documents
- Inconsistent photo identification or personal identifying information
- Personal information inconsistent with other information on file
- Notifications from outside sources regarding possible identity theft or fraudulent activity

Step Four: Employee Training

CONSIDER:

- ◆ Who is responsible for training
- ◆ Group(s) of personnel to be trained
- ◆ General training for larger group and specific training for those more closely involved



Step Five: Establish Consistent Procedures for Responding to Red Flags

CONSIDER:

- Who receives notice of the Red Flag?
- How should the individual who receives notice respond?
 - Investigate that particular incident
 - Determine if the detected incident is indicative of a larger breach
- What steps should be taken if an identity theft event is discovered?
 - How do we escalate
 - Notify student or employee
 - Change passwords
 - Contact law enforcement

Step Six: Develop A Plan to Continually Administer and Regularly Update

CONSIDER how the program will be administered:

- Assign specific employees to administer the program
- Schedule report to the Board of Directors (Board of Regents) or a designated committee at least annually
- Oversee any outside service providers that perform activities in connection with the university's covered accounts (billing and collection agencies).

CONSIDER the changing risk environment:

- Changes in methods of identity theft
- Changes in prevention techniques
- Changes in the business arrangements of the university or college (mergers, new programs)

Step Seven: Managing Outside Service Providers

GENERAL RULE:

A university or college that engages an outside service provider to perform activities in connection with its covered accounts must take steps to ensure that the outside service provider complies with the Red Flag Rules.



Step Seven: Managing Outside Service Providers

Consider

Including in your Program a description of

- the activities performed by the outside service provider
- the steps that your university or college has taken to minimize the outside service provider's access to personal information
- the steps your university or college has taken to ensure that the outside service provider complies with the Red Flag Rules



Step Seven: Managing Outside Service Providers

CONTRACTUALLY OBLIGATE

- All outside service providers to develop and implement policies and procedures designed to prevent, detect, and mitigate the risk of identity theft

How to Develop an Appropriate Red Flags Program

Example of Policy:

Step 1 – state the policy

Example - University will request, to extent feasible, sufficient personally identifying information when signing up for multiple payment program to match with other information retained by the university

Step 2 – state purpose for policy

Example – to detect attempts at identity theft

Step 3 – state specific means to comply

Example – staff will be alert to discrepancies between retained PII and PII provided to sign up for multiple payment program and notify manager of discrepancies

Compliance With Address Discrepancy

- ◆ Do you use Consumer Reports?
(example - background checks)
- ◆ Notice of Address Discrepancy must first be received from national credit reporting agency
- ◆ Implement reasonable procedures for reasonable belief the notice is about the same person
- ◆ Reasonable procedures to furnish address once reasonably confirmed



Compliance Checklist for Address Discrepancy

Once Notice of Address Discrepancy is received, must only take next steps if:

- (1) user forms a reasonable belief that the consumer report relates to the consumer about whom the user requested the report,
- (2) user establishes a continuing relationship with the individual, and
- (3) user regularly and in ordinary course of business furnishes information to the consumer reporting agency from which the notice was received

Compliance Checklist for Address Discrepancy

- ◆ Consumer Reports used
- ◆ Notice of Address Discrepancy received
- ◆ Is the consumer report (notice) about the same employee/applicant that you have on file? If yes, continue.
- ◆ Is the individual a current employee? If yes, continue.
- ◆ Do you regularly furnish information to the consumer reporting agency that sent the Notice of Address Discrepancy? If yes, continue.
- ◆ Look to the employee's personnel file to confirm the most recent address.
- ◆ Send the confirmed address to the consumer reporting agency with the information you regularly furnish during the reporting period in which the employee was hired, or, if the Notice of Address Discrepancy came after that period passed, the reporting period in which you confirmed the accuracy of the employee's address.



Card Issuers and Change of Address

Card issuers must adopt policies to address receipt of notice of change of address at same time or shortly thereafter (within 30 days) a request is made for a card replacement

- Must still be a “creditor”
- “credit card” includes any card or other credit device used to obtain services on credit – 15 U.S.C. 1602(k)



Card Issuers and Change of Address

- ◆ Card Issuer must implement “reasonable policies and procedures” to assess validity of change of address if received at same time (or shortly thereafter) as card replacement
- ◆ May not issue card until either:
 - Assesses validity of change of address under policies and procedures adopted, or
 - Complies with following
 - notify cardholder at former address
 - by any other means of communication previously agreed to be used
 - provide reasonable means for cardholder to report incorrect address changes



**RED FLAGS RULE:
Steps to Achieve Compliance
and
Protect, Students, Parents
and Universities
from Identity Theft**

Benita Kahn
Vorys Legal Counsel
Columbus, Ohio
(614) 464-6487
bakahn@vorys.com
January 2009

