SUBJECT: Red Flag Rule: Identity Theft Compliance for Colleges

In 2008, Congress enacted a law charging the Federal Trade Commission and other agencies with implementing regulations to reduce identity theft (see Attachment I). Despite a number of delays that were intended to allow organizations and institutions the ability to develop compliance procedures, a December 31, 2010 deadline has been announced for final implementation of the “Red Flag Rule.” As this date draws closer, SAC representatives are asked to review current institutional efforts in this area and be prepared to discuss questions/concerns being raised by campus personnel (see Attachment II for example of institutional response materials).

RECOMMENDED ACTION

Discussion.
FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule

At the request of several Members of Congress, the Federal Trade Commission is further delaying enforcement of the “Red Flags” Rule through December 31, 2010, while Congress considers legislation that would affect the scope of entities covered by the Rule. Today’s announcement and the release of an Enforcement Policy Statement do not affect other federal agencies’ enforcement of the original November 1, 2008 deadline for institutions subject to their oversight to be in compliance.

“Congress needs to fix the unintended consequences of the legislation establishing the Red Flags Rule – and to fix this problem quickly. We appreciate the efforts of Congressmen Barney Frank and John Adler for getting a clarifying measure passed in the House, and hope action in the Senate will be swift,” FTC Chairman Jon Leibowitz said. “As an agency we’re charged with enforcing the law, and endless extensions delay enforcement.”

The Rule was developed under the Fair and Accurate Credit Transactions Act, in which Congress directed the FTC and other agencies to develop regulations requiring “creditors” and “financial institutions” to address the risk of identity theft. The resulting Red Flags Rule requires all such entities that have “covered accounts” to develop and implement written identity theft prevention programs to help identify, detect, and respond to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft.

The Rule became effective on January 1, 2008, with full compliance for all covered entities originally required by November 1, 2008. The Commission has issued several Enforcement Policies delaying enforcement of the Rule. Most recently, the Commission announced in October 2009 that at the request of certain Members of Congress, it was delaying enforcement of the Rule until June 1, 2010, to allow Congress time to finalize legislation that would limit the scope of business covered by the Rule. Since then, the Commission has received another request from Members of Congress for another delay in enforcement of the Rule beyond June 1, 2010.

The Commission urges Congress to act quickly to pass legislation that will resolve any questions as to which entities are covered by the Rule and obviate the need for further enforcement delays. If Congress passes legislation limiting the scope of the Red Flags Rule with an effective date earlier than December 31, 2010, the Commission will begin enforcement as of that effective date.

In the interim, FTC staff has continued to provide guidance, both through materials posted on www.ftc.gov/redflagsrule, and in speeches and participation in seminars, conferences and other training events to numerous groups. The FTC also published a compliance guide for business, and created a template that enables low risk entities to create an identity theft program with an easy-to-use online form (www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm). The FTC staff also has published numerous general and industry-specific articles, released a video explaining the Rule, and continues to respond to inquiries from the public. To assist further with compliance, FTC staff has worked with a number of trade associations that have chosen to develop model policies or specialized guidance for their members.

As was the case previously, this enforcement delay is limited to the Red Flags Rule and does not extend to the rule regarding address discrepancies applicable to users of consumer reports (16 C.F.R.§641), or to the rule regarding changes of address applicable to card issuers (16 C.F.R.§881.2).

For questions regarding this Enforcement Policy, please contact Naomi Lefkovitz or Pavneet Singh, Bureau of Consumer Protection, 202-326-2252.

The Federal Trade Commission works for consumers to prevent fraudulent, deceptive, and unfair business practices and to provide information to help spot, stop, and avoid them. To file a complaint in English or Spanish, visit the FTC’s online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357). The FTC enters complaints into Consumer Sentinel, a secure, online database available to more than 1,800 civil and criminal law enforcement agencies in the U.S. and abroad. The FTC’s Web site provides free information on a variety of consumer topics.

MEDIA CONTACT:
Introduction

1.01 Oklahoma State University developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission’s ("FTC") Red Flags Rules ("Rules"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 16 C.F.R § 681.2. After consideration of the size and complexity of the University’s operations and account systems, and the nature and scope of the University’s activities, the University determined that this policy was appropriate and necessary for University compliance.

Background

2.01 Under the Rules, every financial institution and creditor [universities receiving certain federal grants as well as delaying payments and/or issuing debit cards must comply with these rules] is required to establish an Identity Theft Prevention Program tailored to the size, complexity, and nature of its operation.

Scope

3.01 Oklahoma State University is committed to supporting the intent of the Red Flags Rules and understands the importance to its constituents. Protecting individual privacy and the University from data loss and from identity theft is essential.

Purpose

4.01 The University strives to make reasonable efforts to detect, prevent, and mitigate identity theft. This policy and procedure is intended to help protect students, faculty, staff, and other constituents and the University from damages related to the fraudulent activity of identity theft. It is not intended to specify all the details of the Program or identify all possible instances for identity theft. This policy and procedure requires departments to maintain written procedures, identify specific "Red Flags," outline appropriate responses to "Red Flags" that are detected to mitigate identity theft, and establishes recommended employee training. This policy and procedure will be periodically reviewed by the University’s Identity Theft Committee ("Committee"), chaired by the Vice President of Administration and Finance’s designee, and will be updated to reflect changes in risks to faculty, staff, students, and affiliates at the University with respect to Red Flags and identity theft.
Identity Theft Program Adoption

5.01 Each University entity with access to personal identification and financial information is required to develop and implement reasonable internal written procedures to comply with the Red Flags Rules as well as other privacy requirements (e.g.; Gramm-Leach-Bliley, FERPA, HIPAA etc.). Departmental policies will be submitted to the Committee for review and will be subject to audits. The policies will identify red flags, ensure procedures are in place to prevent and detect opportunities, and determine a response to identity theft occurrences.

Definitions (As Defined in the Act)

6.01 Definitions

A. “Identity Theft” is a “fraud committed or attempted using the identifying information of another person without authority.”

B. “Red Flag” is a “pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”

C. “Covered Account” includes all bursar accounts or loans that are administered by the University. Additionally, it includes any other account for which there is a reasonably foreseeable risk of identity theft.

D. “Program Administrator” is the individual designated with primary responsibility for oversight of the Program. See Section 9.01.

E. “Identifying Information” is “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, student identification number, computer’s Internet Protocol address, or routing code.

Identification of Red Flags

7.01 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 specific Red Flags in each of the listed categories (individual departmental policies may contain additional Red Flags specific to their area):

A. Notifications and Warnings from Credit Reporting Agencies
   Red Flags
   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; or
5. Indication from a credit report of activity that is inconsistent with an applicant’s usual pattern or activity.

B. Suspicious Documents
Red Flags
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 account holder/student information; or
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information
Red Flags
1. Identifying information presented that is inconsistent with other information the account holder/student provides (example: inconsistent birth date);
2. Identifying information presented that is inconsistent with other sources of information (for instance, a permanent address not matching a permanent address on a loan application);
3. Identifying information presented that is the same as information shown on other documents 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 account holder/student;
6. A person fails to provide complete personal identifying information on a document when reminded to do so; or
7. A person’s identifying information is not consistent with information that is on file for the account holder/student.

D. Suspicious Covered Account Activity or Unusual Use of Account
Red Flags
1. Change of address for an account followed by a request to change the account holder/student’s name;
2. Account used in a way that is not consistent with prior use;
3. Mail sent to the account holder/student is repeatedly returned as undeliverable;
4. Notice to the University that an account holder/student is not receiving mail sent by the University;
5. Notice to the University that an account has unauthorized activity;
6. Breach in the University’s computer system security; or
7. Unauthorized access to or use of account holder/student account information.
E. Alerts from Others

Red Flags

1. Notice to the University by an account holder/student, 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.

7.02 Detecting Red Flags

A. 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 (individual departmental policies may contain additional Red Flags specific to their area):

Detect

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 or tribally issued photo identification).

B. 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 (individual departmental policies may contain additional verifications specific to their area):

Detect

1. Verify the identification of account holders/students if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing address by mail or email and provide the account holder/student a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

C. Consumer (“Credit”) Report Requests - In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel will take the following steps to assist in identifying address discrepancies:

Detect

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; and
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the application for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.
8.01 Preventing, Mitigating, and Response to Identity Theft
In the event University personnel detects 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 (individual departmental procedures may contain additional steps specific to their area):

A. Prevent and Mitigate
   1. Continue to monitor a covered account for evidence of identity theft.
   2. Contact the account holder/student or document provider (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 the account holder/student with a new campus identification number;
   6. Notify the Program Administrator for determination of the appropriate step(s) to take;
   7. Notify law enforcement;
   8. Notify the Security Compliance Officer, University Registrar, Controller, or Chief Human Resources Officer. EthicsPoint, the anonymous on-line reporting agency, may be used to provide this notification.
   9. File or assist in filing a Suspicious Activities Report (“SAR”); or
   10. Determine that no response is warranted under the particular circumstances.

B. Prevent Misuse of Account Holder/Student 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 account holder/student identifying information (individual departmental procedures may contain additional steps specific to their area):

   1. Ensure that websites are secure or provide clear notice that a website is not secure;
   2. Ensure complete and secure destruction of paper documents and computer files containing account holder/student 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 (See Electronic Use of Social Security Numbers, P&P 3-0322);
   5. Ensure computer virus protection is up-to-date; and
   6. Require and keep only the kinds of account holder/student information that is necessary for University purposes.

9.01 Identity Theft Program Administration
A. Oversight
   Responsibility for developing, implementing, and updating this program lies with the Committee for the University. The Committee is headed by a Program Administrator who is the Vice President for Administration and Finance of the
University or his/her designee. The remainder of the committee membership includes representatives from offices of Security Compliance, ID Card, Admissions, Registrar, Financial Aid, Bursar, University Health Services, Human Resources, and Housing. The Program Administrator will be responsible for ensuring appropriate training of University staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports
1. University staff 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. University staff shall be trained, as necessary, to effectively implement the Program. It is recommended that employees sign a document to be stored in their personnel file stating that they have been trained and understand this policy. Information will be tracked within OSU Training Services.

2. University employees are expected to notify the Program Administrator once they become aware of an incident of identity theft or of the University’s failure to comply with this program. 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 Program Administrator 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 and management’s response, and recommendations for changes to the Program.

C. 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 service providers have such policies and procedures in place; and
2. 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.

D. Non-disclosure of Specific Practices
For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flags identification, detection, mitigation and prevention practices may need to be limited to the Committee who developed this program and to those employees with a need to know. 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 employees or the public. The
Program Administrator shall inform the Committee and those employees with a need
to know the information of those documents or specific practices which should be
maintained in a confidential manner.

E. Program Updates
The Committee will annually review and update this document to reflect changes in
risks to account holders/students 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 revise this document
and will ensure ongoing support of the Red Flags regulation.

Approved by A&M Board of Regents: July 24, 2009