IOWA STATE UNIVERSITY IDENTITY THEFT PREVENTION PROGRAM

Iowa State University of Science and Technology

Ames, Iowa

June 10-11, 2009

Action Requested: Approve the proposed Identity Theft Prevention Program as part of the Fair and Accurate Credit Transactions Act of 2003 (FACTA).

Background Information

On November 9, 2007, the Federal Trade Commission published final rules implementing part of the Fair and Accurate Credit Transactions Act of2003 (FACTA) regarding the duties of creditors, card issuers and users of consumer reports with respect to the prevention of identity theft. Compliance with these rules is required by August 1, 2009. The FTC regulations, known as the Red Flag Rules are organized into three parts including:

1. Duties of users of consumer reports regarding address discrepancies.
2. Duties of creditors regarding the detection, prevention and mitigation of identity theft.
3. Duties of card issuers regarding changes of address.

A task force led by university legal counsel determined Iowa State University was a “creditor” as defined by the Red Flag Rules, since we regularly extend, renew, or continue credit for student and employee accounts involving student loans, institutional loans and payment for services received over time. Therefore, the duties of creditors regarding the detection, prevention and mitigation of identity theft contained in the Red Flag Rules apply to Iowa State University. It was also determined that, in certain cases, a university department does receive a consumer report from a credit reporting agency, and therefore is subject to the duties of users of consumer reports regarding address discrepancies. However, the task force also determined that the ISU card is not a debit or credit card but is a "stored value" card that cannot be processed through the regular financial debit/credit card network unless a student chooses to add the optional services from our third party servicer, US Bank. For that reason, ISU is not responsible for the Red Flag Rules regarding the duties of card issuers regarding changes of address and our contractual service provider, currently US Bank, would be responsible for compliance with the Red Flag Rule.

As the FTC Red Flag Rule requires that Iowa State University must "obtain approval of the initial written program from its board of directors we are requesting authorization to move forward with the program proposed in the attached document. Its purpose is to establish an identity theft prevention program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide continued administration of the program. The identity theft prevention program includes reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts ISU offers or maintains and incorporate those red flags into the program.
2. Detect red flags that have been incorporated into the program,
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft, and,
4. Assure the program is updated periodically to reflect changes and risks involving possible identity theft and fraud.

Iowa State University of Science and Technology

IDENTITY THEFT PREVENTION PROGRAM

1. PURPOSE

The purpose of this program is for Iowa State University of Science and Technology (hereinafter "ISU") to establish an Identity Theft Prevention Program (hereinafter "Program") designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

A. Identify relevant Red Flags for covered accounts ISU offers or maintains 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; and

D. Assure the Program is updated periodically to reflect changes in risks involving possible identity theft and fraud.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

2. DEFINITIONS

A. **Covered Account** – A covered account is a consumer account used by customers of ISU primarily for personal, family, or household purposes that is designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by the customer (borrower) periodically over time. At ISU, a covered account includes the following:

1. Participation in the following Federal student loan programs: Perkins Loan, Health Profession Student Loan and Loans for Disadvantaged Students;
2. Participation in institutional loans to students, faculty or staff;
3. Participation in a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester;
4. Participation in a plan for payment for services received over time rather than requiring full payment upon receipt of services;
5. Participation in other services provided by third party service providers that satisfy the definition of a covered account.

B. **Creditor –** A creditor is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit. ISU is a creditor under the Federal Trade Commission (FTC) Identity Theft Red Flags Rule, 16 CFR 681.2.

C. **Customer** – A customer is a person or entity that has a covered account with ISU. Customer includes students, faculty, staff and persons or entities doing business with ISU.

D. **Identity Theft** – Identity theft is a fraud committed or attempted using the identifying personal information of another person.

E. **Personal Information** – Specific items of personal information identified in Iowa Code Section 715C.1(11). This information includes an individual's name in combination with any one or more of the following data elements:

- Social Security number,
- Driver's license number,
- Health insurance information,
- Medical information, or
- Financial account number (such as a credit card number, debit card number or bank account number) or an ISU issued university identification number (UID) when the numbers are in combination with any required security code, access code, or password that would permit access to an individual's financial account or the ISU AccessPlus account for an individual.

When the name or the data elements are encrypted, redacted or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable, they are not included in the definition of personal information.

F. **Red Flag –** A Red Flag is a pattern, practice or specific activity that indicates the possible existence of identity theft or fraud.

G. **Service Provider –** A service provider is a third party that is contracted to provide outsourced operations directly to ISU customers that are related to a covered account.

3. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags within its covered accounts, ISU 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. Any time a Red Flag, or a situation closely resembling a Red Flag, is detected, it should be evaluated by ISU personnel for verification of the person or entity involved and implementation of an appropriate response pursuant to Section 5 of this program.

ISU identifies the following Red Flags in each of the listed categories:

A. Alerts received by ISU from a Credit Reporting Agency

1. Receipt of any alerts, notifications, or warnings from a national consumer credit reporting agency including a fraud alert, active duty alert, credit freeze, or notice of an unusual pattern of activity relating to a customer.

2. Receipt of an official notice of address discrepancy from a consumer reporting agency as defined in 15 USC 1681c(h)(l) and 16 CFR 681.2. See Section 6 for Specific Address Discrepancy Procedure.

B. Suspicious Documents

1. Presentation by a customer of an application for service, identification document or card that appears to be forged, altered or inauthentic.

2. Presentation by a customer of an application for service, identification document or card on which a person's image or physical description is not consistent with the person presenting the document; or where the photo ID does not resemble its owner.

3. Presentation by a customer of an application for service or identification document which appears to have been cut up, reassembled and/or photocopied.

4. Failure of the customer to have available for review their ISUCard or other government issued photo identification document to assist in verification of the identity of the customer.

C. Suspicious Personal Identifying Information

1. Presentation of a university identification number, social security number, or tax identification number that is the same as one given by another customer.

2. Presentation of identifying information that is not consistent with the information on file with ISU for the customer such as university identification number, social security number, or tax identification number.

3. Failure to provide complete personal identifying information on an application document when reminded to do so.

D. Unusual Use or Suspicious Account Activity

1. Receipt of a request to change demographic or personal information without appropriate documentation.
2. Receipt of a request to mail something to an address not listed in customer's file.
3. Receipt of notification that the customer is not receiving statements or other communications.
4. Receipt of notification that the covered account has unauthorized charges or transactions.
5. Notification of exceeding try limits attempting to login to a student AccessPlus account.
6. Notification of exceeding try limits attempting to login to a student E-mail account

E. Notice from Others Indicating Possible Identify Theft

Receiving notice from the customer, a victim of identity theft, law enforcement, the U. S. Department of Education, a financial institution, an insurance company, a credit card company, or another account holder regarding reports that a fraudulent account was opened or possible identity theft in connection with a covered account.

4. DETECTING RED FLAGS

In order to detect any of the Red Flags identified in Section 3 above that are associated with the opening of a covered account for a customer or for monitoring transactions on an existing covered account, ISU personnel will take one or more of the following steps to obtain and verify the identity of the person opening a covered account or using an existing covered account in accordance with the written operational policies of the unit that manages the covered account:

A. Require certain identifying information such as name; date of birth; residential, business or in-session university address; or other identification in conjunction with a signature and/or other communication with the person or entity whose covered account is involved;

B. Presentation of an ISUCard or government issued photo identification document and determining that:

1. The image on the identification document matches the appearance of the customer presenting

the identification; and

2. The identification document has not been altered, forged or the paperwork does not have the appearance of having been destroyed and reassembled.

C. Verify any changes made electronically to financial information contained in a covered account by e-mailing customers to alert them to changes made to their account.

5. PREVENTING AND MITIGATING IDENTITY THEFT

In the event ISU personnel detect any identified Red Flags, such personnel shall respond depending on the degree of risk posed by the Red Flag. The appropriate responses to the relevant Red Flags can include any one or more of the following:

A. Deny access to the covered account until other information is available to eliminate the Red Flag;

B. Contact the customer to advise that a fraud has been attempted on their covered account;

C. Change any passwords, security codes or other security devices that permit access to a covered account;

D. Notify law enforcement; or

E. Determine that no response is warranted under the particular circumstances.

6. SPECIFIC ADDRESS DISCREPANCY PROCEDURE

The FTC has also issued a special rule regarding the receipt of an official notice of address discrepancy from a consumer credit reporting agency pursuant to 15 USC 1681c(h)(l) and 16 CFR 681.2. This Address Discrepancy Rule applies to any ISU employee or department that has requested a criminal background check or consumer credit report from a consumer credit reporting agency, such as HireRight, TransUnion, Experian and Equifax, whether or not the request involves a covered account as defined by this program.

Upon receipt of an official notice of address discrepancy from a consumer credit reporting agency, ISU personnel will take the following steps to assist in verifying any address discrepancies and forming a reasonable belief that the criminal background check or consumer credit report relates to the person about whom the ISU personnel has requested the report:

A. Investigate the accuracy of the address information provided by the applicant, volunteer or other person about whom the criminal background check or consumer credit report was requested by comparing address information included in the report received from the consumer reporting agency and verifying address information directly with the person about whom the report was requested.

B. Require written verification from any applicant, volunteer or other person about whom the criminal background check or consumer credit report was requested that the address provided to ISU is accurate.

C. Report the results of any investigation to the Program Administrator.

D. The Program Administrator shall notify the credit reporting agency of any newly confirmed address information regarding the person about whom the Address Discrepancy Notice was received.

7. PROGRAM ADMINISTRATION

A. Oversight by an Identity Theft Prevention Committee

Responsibility for developing, implementing and updating this Program lies with the Vice President for Business and Finance. An Identity Theft Prevention Committee is a five-member committee that is chaired by a Program Administrator. The Program Administrator shall be the Director of the ISU Accounts Receivable Office. The other members shall be employees appointed by the Vice President for Business and Finance, and at least one member shall represent the Student Financial Aid Office, at least one member shall represent the Information Technology Services Office, and other members shall be from units that have covered accounts. The Program Administrator will be responsible for:

1. Assuring appropriate training of ISU staff on the Program;
2. Reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft;
3. Determining which steps of prevention and mitigation should be taken in particular circumstances when necessary; and
4. Considering periodic changes to the Program.

B. Staff Training and Reports

ISU 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. ISU staff shall be trained, as necessary, to effectively implement the Program. ISU employees are expected to notify the Program Administrator once they become aware of an incident of identity theft or of ISU's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, ISU 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. Identity Theft Prevention Program Updates

The Committee will periodically review and update this Program to reflect changes in risks to customers and the soundness of the ISU Identity Theft Prevention Program. In doing so, the Committee will consider ISU's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in ISU'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.

8. SERVICE PROVIDERS

A. ISU remains responsible for compliance with the Red Flag Rules even if it outsources operations regarding covered accounts to a third party service provider. In the event ISU engages a service provider to perform an activity in connection with one or more covered accounts, ISU 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 in place reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities;

2. Require, by contract, that service providers review the ISU's Program and timely report any Red Flags to the Program Administrator or the University employee with primary oversight of the service provider relationship; and

3. Require, by contract, that the service provider is responsible for implementing appropriate steps to prevent or mitigate identify theft.

B. 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.

9. 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 President, Vice President for Business and Finance, the Program Administrator and to those employees with a need to know them for purposes of carrying out their responsibilities under the Program. Although this program is a public document and may be posted on the ISU Policy Library, 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 ISU employees or the public as a security plan and protocol pursuant to Iowa Code Sections 22.7(52) and 22.8 and the ISU Policy regarding Public Records Exemption for Security Related Information. 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.

10. OTHER RESOURCES

Iowa Open Records Act – Iowa Code Chapter 22
Iowa Personal Information Security Breach Protection – Iowa Code Chapter 715C
FERPA (Family Educational Rights & Privacy Act) - Notification of Rights
Health Information Privacy and Security (HIPAA)
Identification (ID) Card (ISUCard)
Social Security Number Protection
Student Records
Employee Records
Public Records Exemption for Security Related Information
IT Security
IT Security Incident Reporting
Code of Computer Ethics and Acceptable Use