Contact: Thomas Evans

IDENTITY THEFT PREVENTION PROGRAMS

Actions Requested: Approve the proposed Identity Theft Prevention Programs of Iowa State University, University of Iowa/University of Iowa Hospitals and Clinics and University of Northern Iowa as part of the Fair and Accurate Credit Transactions Act of 2003 (FACTA).

Executive Summary: On November 9, 2007, the Federal Trade Commission published final rules implementing part of the Fair and Accurate Credit Transactions Act of 2003 (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.

The universities are considered a “creditor” as defined by the Red Flag Rules, since they 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 the universities. The universities also periodically receive a consumer report from a credit reporting agency, and therefore are subject to the duties of users of consumer reports regarding address discrepancies. Student cards, however, are not a debit or credit card but a "stored value" card that cannot be processed through the regular financial debit/credit card network unless a student chooses to add optional services from the university’s third party servicer. For that reason, the universities are not responsible for the Red Flag Rules regarding the duties of card issuers regarding changes of address. Instead the university’s contractual service provider would be responsible for compliance with the Red Flag Rule.

The purpose of each program 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 programs include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts the universities offer or maintain 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.

The FTC Red Flag Rule requires that the universities must "obtain approval of the initial written program from its board of directors.” As such the universities are requesting approval of their respective programs as proposed in Appendix A, B, B-1 & C.

Appendix A

IOWA STATE UNIVERSITY
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

Appendix B

UNIVERSITY OF IOWA
IDENTITY THEFT PREVENTION PROGRAM

Subject: **Identity Theft detection, prevention, and mitigation**

Purpose: To establish an Identify Theft Prevention Program designed to detect, prevent, and mitigate identify theft in connection with opening a covered account or an existing covered account at the University of Iowa.

Definitions:

Account: A continuing relationship established as a result of becoming a student, accepting employment or obtaining goods or service which includes an extension of credit involving a deferred payment.

Covered Account: Accounts allowed by the University of Iowa are primarily for students, faculty and staff and allow multiple payments or transactions; and any other accounts the University of Iowa maintains for which there is a foreseeable risk to customers or to the safety and soundness of the University of Iowa from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Red Flag: A pattern, practice or specific activity that indicates the possible existence of identity theft.

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.

Identifying Information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

Policy:

A. University of Iowa Identification of Covered Accounts

1. Student – Accounts opened as part of being a registered student.
2. Faculty and Staff – Accounts opened as a result of accepting employment
3. Non-Student – Accounts opened as a result of obtaining goods or services.

B. Establishment of an identify Theft Prevention Program

1. The University of Iowa establishes its program through the implementation of this policy. The Program is designed to detect, prevent, and mitigate identify theft in connection with the opening of a covered account or any existing covered account.

C. Elements of the Program

1. The University of Iowa will identify relevant Red Flags for covered accounts that the University of Iowa offers or maintains and will incorporate those Red Flags into the Program.
2. The University of Iowa will put process and procedures in place to detect Red Flags that have been incorporated into the Program.
3. The University of Iowa will respond appropriately to any Red Flags that are detected in order to prevent and mitigate identity theft.
4. The University of Iowa will ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the University of Iowa systems and services from identity theft.

D. Administration of the Program

1. The initial program shall be approved by the University of Iowa Provost and Vice-President for Finance and Operations.
2. Program oversight shall be the responsibility of the Vice President for Finance and Operations and responsibility for the implementation of the program shall be assigned to the Controller of the University of Iowa.
3. At least annually, the Controller shall report to the Vice President for Finance and Operations on the University of Iowa's compliance with the detection, prevention, and mitigation of identity theft.

E. **Service Provider Arrangements**

1. When the University of Iowa engages a service provider for an activity in connection with one or more covered accounts, The University of Iowa will require the service provider by contract to have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider's activities, and to report the Red Flags to the University of Iowa, as well as to take appropriate steps to prevent or mitigate identity theft.

F. Identification of Red Flags

1. When identifying relevant Red Flags, the University of Iowa will consider, as appropriate, the types of covered accounts it offers or maintains, the methods it provides to open its covered accounts, the methods it provides to access its covered accounts, and its previous experiences with identity theft.

G. Identified Potential Red Flags and Corresponding Policies
(See Attachment G - Identified Potential Red Flags and Corresponding Response Policies, next page)

Attachment G - Identified Potential Red Flags and Corresponding Response Policies

Red Flag	Response Policy			
Documents provided for identification appearing altered or forged	1) Refuse Service	2) Notify University Police	3) Retain altered or forged card if University ID card	
Photograph on ID inconsistent with appearance of customer	1) Request additional form of Photo ID to resolve inconsistency	2) If not resolved with additional form or additional form not provided - refuse service	3) Notify University Police	
Photograph on UNIV ID inconsistent with appearance of customer	1) Request additional form of Photo ID to resolve inconsistency	2) If not resolved with additional form or not provided, refuse service	3) Notify University Police	4)Retain Univ ID
Information on ID inconsistent with information provided by person opening account	1) Ask account holder to provide additional information to resolve inconsistency.	2) refuse service if not resolved		
Information on ID such as signature, inconsistent with information on file at financial institution	1) Ask account holder to provide additional information to resolve inconsistency.	2) refuse service if not resolved		

Information on ID not matching any address in the consumer report, Social Security number has not been issued or appears on the Social Security Administration's Death master File, a file of information associated with Social security numbers of those who are deceased.	1) Notification of a social security number not matching can be received by either Social Security Office or Department of Education	2) Request additional information to resolve why there is no match	3) Resolution required or refuse service	4) If service refused, report to University Police
Lack of Correlation between Social Security number range and date of birth	1) Notification of a social security number not matching can be received by either Social Security Office or Department of Education	2) Request additional information to resolve why there is no match	3) Resolution required or refuse service	4) If service refused, report to University Police
Personal Identifying information associated with known Fraud activity	1) Follow University Police procedures and policies			
Social Security numbers provided matching that submitted by another person opening an account or other customers	1) Ask for additional information to resolve	2) Refuse service until resolved		

personal information inconsistent with information already on file at financial institution or creditor. (i.e. address)	1) Request additional information to resolve	2) Refuse service	3) Verify with National Database (i.e. credit bureaus) to resolve inconsistency.	
Person opening account or customer unable to correctly answer challenge questions.	1) Refuse service			
Most of available credit used for cash advances, jewelry or electronic, plus customer fails to make first payment.	1) Student ID cards not allow to purchase electronic gaming systems. In the Apple Store, purchases limited to $200.	2) Students or staff not making payments, account will become past due and further charging is suspended until account is current.		
Drastic change in payment patterns, use of available credit or spending patterns	1) Detection from reports by IMU Business Office for accounts with excessive spending, itemized receipts are pulled	2) Customer is contacted to verify purchases are legitimate and card not stolen	3) If any suspicion of fraud as a result of receipt examination, suspend charging ability on card.	4) Report to University Police
Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account.	1) Contact Customer to determine correct address	2) If unable to determine correct address, suspend activity on account until resolved	3) When possible, verify address through credit bureau and/or review account activity for departmental help in verifying correct address.	

Financial institution or creditor notified that customer is not received paper account statements	1) Student and Staffs bills will be delivered electronically beginning 2/1/09	2) If paper bill still mailed, verify customer, verify address.	
Financial institution or creditor notified of unauthorized charges or transactions on customer's account	1) Report to University Police for investigation	2) Advise department that submitted charge to billing system	3) Suspend charging ability on account
Information discovered from a background check not consistent with information already onn file.	1) Applicant is given report to respond or provide additional documentation.	2) If applicant says incorrect, vendor is asked to run report again using additional identifiers.	3) If information is verified with applicant to be correct, reviewed by Dean of College so a decision can be made on what action should be taken regarding the applicant.

Appendix B-1

UNIVERSITY OF IOWA HOSPITALS AND CLINICS
IDENTITY THEFT PREVENTION PROGRAM

PURPOSE: To establish an Identity Theft Prevention Program (the "Program") designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account at the University of Iowa Hospitals & Clinics ("UIHC"), which includes addressing issues associated with patient misidentification due to identity theft that could result in the inclusion of information in a medical record that relates to more than one person, as well as issues associated with unauthorized charging to staff/faculty/student accounts.

DEFINITIONS:

Account: A continuing relationship established by a person with UIHC to obtain a product or service for personal, family, or household purposes, which includes an extension of credit, such as the purchase of property or services involving a deferred payment.

Covered Account: 1) An account that the UIHC offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. 2) Any other account that the UIHC offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the UIHC from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.

Identifying Information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

Medical Identity Theft: A fraud committed or attempted using the identifying information of another person without authority in order to obtain medical care.

Service Provider: A person or entity that provides a service directly to the UIHC that involves a covered account.

POLICY:

A. Establishment of Identity Theft Prevention Program (the "Program")

1. Upon consideration of the Guidelines published in 72 Fed. Reg. 63718 (Nov. 9, 2007) the Red Flag Rules Appendix A, UIHC establishes this Program to detect, prevent, and mitigate identify theft in connection with the opening or maintenance of a covered account and has identified its covered accounts and Red Flags as stated herein.

B. Identification of Covered Accounts

1. UIHC has determined that it offers and maintains the following covered accounts:

   a. Patient Account: Account opened at the time of becoming a registered patient.

   b. Faculty/Staff/House Staff Account: Account opened upon requesting and receiving a UIHC ID badge with charging capabilities.

   c. Student Account: Account opened by a health profession student (e.g. medical/pharmacy/nursing student) upon requesting and receiving a UIHC ID with charging capabilities or opened by a non-health profession student upon requesting and receiving hospital charging capabilities through an existing UI student ID.

C. Elements of the Program

1. UIHC will identify relevant Red Flags for the covered accounts that UIHC offers or maintains and will incorporate those Red Flags into the Program.

2. UIHC will detect the identified Red Flags that have been incorporated into the Program.

3. UIHC will respond appropriately to any Red Flags that are detected to reasonably prevent and mitigate identity theft.

4. UIHC will update the Program (including the Red Flags determined to be relevant) periodically to reflect changes in risks to customers and to the safety and soundness of UIHC from identity theft.

D. Administration of the Program

1. Program oversight shall be the responsibility of the Associate Vice President for Finance & Chief Financial Officer ("AVP for Finance & CFO").

2. Responsibility for the development, implementation, and administration of the Program shall be assigned to the Joint Office of Patient Financial Services ("JOPFS").

a. At least annually, the Director of the JOPFS shall report to the AVP for Finance & CFO on UIHC's compliance with the detection, prevention, and mitigation of identity theft.

i. The annual report should address material matters related to the Program such as the effectiveness of the policies/procedures of UIHC in addressing the risk of identity theft; service provider arrangements; significant incidents involving identity theft and management's response thereto; and recommendations for material changes to the Program.

b. The JOPFS Director shall ensure that a risk assessment is conducted periodically or as needed when there are material changes in the types of covered accounts offered and maintained by UIHC or in the risks to such covered accounts so that necessary modifications are made to the Program.

c. To monitor compliance issues and evaluate the need for any changes to the Program based on changes in the types of covered accounts offered and maintained, changes in the risks of identity theft, and actual reported incidents of identity theft, the JOPFS Director shall consult with the Joint Office for Compliance ("JOC").

d. The JOPFS Director shall ensure that UIHC faculty/staff for whom it is reasonably foreseeable that they may come into contact with covered accounts are trained, as necessary, to effectively implement the Program.

e. The JOPFS Director shall exercise appropriate and effective oversight of service provider arrangements associated with covered accounts.

i. When UIHC engages a service provider to perform an activity in connection with one or more covered accounts, UIHC will require the service provider by contract to have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider's activities, and to report the Red Flags to UIHC, as well as to take appropriate steps to prevent or mitigate identity theft.

3. The JOC shall maintain a record of reported incidents of attempted and/or successful identity theft activities and the action taken to address such incidents.

PROCEDURE:

A. Patient Identification

1. UIHC Registration staff should follow department protocols/policies for verifying the identity of patients during the registration process.

2. All other UIHC staff should follow their respective department/clinic protocols/policies for verifying the identity of patients as necessary and when appropriate (e.g. upon clinic check-in).

B. Identification of Red Flags

1. Faculty/staff should identify and report incidents involving the following Red Flags and any other suspicious activities involving covered accounts directly to the **Joint Office for Compliance at (38)4-8282**. The JOC shall then contact the JOPFS Director, the Safety & Security Director, and any affected department to notify them of the incident or suspicious activity for the determination of an appropriate response.

2. The UIHC adopts the following Red Flags to alert faculty/staff to possible instances of identity theft.

   a. PRESENTATION OF SUSPICIOUS DOCUMENTS, including, but not limited to:

      i. Documents provided for identification appear to have been altered or forged.

      ii. The photograph or physical description on the identification is not consistent with the appearance of the person presenting the identification.

      iii. Other information on the identification is not consistent with information provided by the person opening a new covered account or presenting the identification.

      iv. Other information on the identification is not consistent with readily accessible information that is already on file with UIHC, such as clear identifying characteristics (e.g. age, gender, race/ethnicity, etc.).

   b. PRESENTATION OF SUSPICIOUS PERSONAL IDENTIFYING INFORMATION, including, but not limited to:

      i. The Social Security Number provided is the same as that of another person with a covered account. [Note: Social Security Number should only be collected when necessary (e.g. Medicare/Medicaid patients)]

      ii. Personal identifying information provided is not consistent with personal identifying information that is already on file with UIHC (e.g. date of birth, Social Security Number, etc.).

      iii. Medical history/treatment as stated in the patient's medical record is suspiciously and/or significantly inconsistent with the physical examination of the patient or with the medical history as reported by the patient.

      iv. A patient who has an insurance number, but never produces an insurance card or other physical documentation of insurance.

c. UNUSUAL USE OF, OR SUSPICIOUS ACTIVITY RELATED TO, THE COVERED ACCOUNT, including, but not limited to:

i. A covered account (e.g. faculty/staff/student ID charge account) is used in a manner that is not consistent with established patterns of activity on the account. For example, nonpayment when there is no history of late or missed payments (e.g. in the case of part-time/temporary employees with no payroll deduction that receive billing statements for cafeteria/book store charges or students that are billed via U-Bill) or there is a material change in purchasing or spending patterns.

ii. Mail sent to the person responsible for the covered account is repeatedly returned as undeliverable although transactions continue to be conducted in connection with the covered account.

iii. UIHC is notified that the person responsible for the covered account is not receiving paper account statements.

iv. UIHC is notified of unauthorized charges or transactions in connection with a covered account.

v. A complaint or concern is received from a patient based on the patient's receipt of a bill for another individual, a bill for a product or service that the patient denies receiving, a bill from a health care provider that never treated the patient, or an explanation of benefits for health services never received by the patient.

d. NOTICE OF POTENTIAL IDENTITY THEFT

i. UIHC is notified by a person responsible for a covered account, a victim of identity theft, a law enforcement authority, or any other person that identity theft may have occurred with regard to a covered account.

C. Medical Records

1. In the event medical identity theft is confirmed, the JOPFS Director and Health Information Management (HIM) Director shall take reasonable steps to correct payment records and medical records, as appropriate, for victims of medical identity theft.

2. For confirmed cases of medical identity theft, the JOC will follow UIHC's policies/protocols regarding the handling of patient privacy matters when applicable.

D. Preventing and Mitigating Identity Theft

1. Upon detecting or being notified of a Red Flag, the JOPFS Director and the Safety & Security Director, in consultation with the affected department(s), will determine the appropriate response, which shall be commensurate with the degree of risk posed.

2. Appropriate responses may include, but are not limited to, the following:

   a. Initiation of an internal investigation;

   b. Monitoring a covered account for evidence of identity theft;

   c. Contacting the person responsible for the covered account (e.g. patient, employee, student, etc.);

   d. Contacting the third-party payor involved;

   e. Changing any passwords, security codes, or other security devices that permit access to a covered account (e.g. electronic medical record passwords);

   f. Reopening a covered account with a new account number;

   g. Closing an existing covered account;

   h. Not opening a new covered account;

   i. Not collecting or continuing to collect on the debt of a victim of identity theft or not reporting the debt on the victim's credit report;

   j. Notifying law enforcement;

   k. Correcting medical, payment, and other records of identity theft victims;

   l. Flagging records (e.g. electronic medical records) that have been or may be affected by identity theft;

   m. Mitigating, to the extent reasonably practicable, any harmful effect known to UIHC as a result of identity theft; and

   n. Determining that no response is warranted under the particular circumstances.

3. Once a Red Flag situation has been appropriately addressed, the JOPFS Director and/or the Safety & Security Director shall report the specific action taken and resolution, if any, to the JOC to be included in the UIHC's log of identify theft incidents.

Appendix C

UNIVERSITY OF NORTHERN IOWA
IDENTITY THEFT PREVENTION PROGRAM

Subject: **Identity Theft detection, prevention, and mitigation**

Purpose: To establish an Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft in connection with opening a covered account or an existing covered account at the University of Northern Iowa.

This Program is established pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

Definitions: **Account:** A continuing relationship established as a result of becoming a student, accepting employment, or obtaining goods or service which includes an extension of credit involving a deferred payment.

Covered Account: Accounts allowed by the University of Northern Iowa which are primarily for students, faculty, and staff and allow multiple payments or transactions; and any other accounts the University of Northern Iowa maintains for which there is a foreseeable risk to customers or to the safety and soundness of the University of Northern Iowa from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Red Flag: A pattern, practice or specific activity that indicates the possible existence of identity theft.

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.

Identifying Information: Any name or number used (alone or in conjunction with any other information) to identify a specific person.

Policy:

H. University of Northern Iowa Identification of Covered Accounts

1. Student – Accounts opened as part of being a registered student.
2. Faculty and Staff – Accounts opened as a result of accepting employment
3. Non-Student – Accounts opened as a result of obtaining goods or services.

I. Establishment of an identity Theft Prevention Program

1. The University of Northern Iowa establishes its program through the implementation of this policy. The Program is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

J. Elements of the Program

1. The University of Northern Iowa will identify relevant Red Flags for covered accounts that the University offers or maintains and will incorporate those Red Flags into the Program.
2. The University of Northern Iowa will put process and procedures in place to detect Red Flags that have been incorporated into the Program.
3. The University of Northern Iowa will respond appropriately to any Red Flags that are detected in order to prevent and mitigate identity theft.
4. The University of Northern Iowa will ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the University systems and services from identity theft.

K. Administration of the Program

1. The initial program shall be approved by the Board of Regents, State of Iowa.
2. Program oversight shall be the responsibility of the Director, Office of Business Operations and responsibility for the implementation of the program shall be assigned to the Bursar, Cashier Coordinator, and other designee(s) as necessary and appropriate. University staff will be trained as necessary to effectively implement the Program.
3. At least annually, the Bursar, Cashier Coordinator, and any other designee(s) shall report to the Director, Office of Business Operations on the University of Northern Iowa's compliance with the detection, prevention, and mitigation of identity theft.

L. **Service Provider Arrangements**

1. When the University of Northern Iowa engages a service provider in connection with one or more covered accounts, the University will require the service provider by contract to have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider's activities, and to report the Red Flags to the University of Northern Iowa, as well as to take appropriate steps to prevent or mitigate identity theft.

M. Identification of Red Flags

1. When identifying relevant Red Flags, the University of Northern Iowa will consider, as appropriate, the types of covered accounts it offers or

maintains, the methods it provides to open its covered accounts, the methods it provides to access its covered accounts, and its previous experiences with identity theft.

N. Detection of Red Flags

1. To detect Red Flags, the University of Northern Iowa will take the following steps to obtain information and verify the identity of the person opening a covered account or using an existing covered account, consistent with the applicable University procedures:

    i. obtain indentifying information and verify identity of a person opening a covered account; and
    ii. monitor transactions and verify validity of change of address requests for existing covered accounts.

O. Identified Potential Red Flags and Corresponding Responses/Procedures

1. The attachment to this section is to be updated periodically, to reflect changes in risks to students and customers and to the safety and soundness of the University systems and services from identity theft.

    (See Attachment O - Identified Potential Red Flags and Corresponding Response Policies, next page)

Attachment O - Identified Potential Red Flags and Corresponding Response Policies

Red Flag	**Response Policy**		
UNI notified of unauthorized charges or transactions on customer's account	1) Notify University Police	2) Suspend charging ability	3) Advise UNI departments to cease submitting charges for that account
Documents provided for identification appear to have been altered or forged	1) Refuse Service	2) Notify University Police	3) Retain altered or forged documents
Photograph on UNI ID card is not consistent with the appearance of the customer presenting the identification	1) Request additional form of Photo ID to resolve inconsistency - if not resolved with additional form of Photo ID, or additional form not provided, refuse service	2) Notify University Police	3) Retain UNI ID card
Customer unable to correctly answer challenge questions.	1) Refuse service		
Information is discovered that is not consistent with information already on file	1) Contact customer to provide additional documentation to resolve discrepancy	2) If any suspicion of fraud remains, notify University Police	
Personal identifying information associated with known Fraud activity	1) Follow University Police procedures and policies		
Social Security Number provided matches that of another person	1) Request additional information to resolve SSN discrepancy	2) Resolution required or refuse service	3) If service refused, report to University Police
Social Security Number provided has not been issued or appears on the Social Security Administration's Death master File	1) Request additional information to resolve SSN discrepancy	2) Resolution required or refuse service	3) If service refused, report to University Police
Lack of Correlation between Social Security Number range and date of birth	1) Request additional information to resolve SSN discrepancy	2) Resolution required or refuse service	3) If service refused, report to University Police
Personal information provided inconsistent with information already on file (e.g. address)	1) Request additional information to resolve	2) Resolution required or refuse service	
Excessive spending on discretionary items or drastic change in purchasing patterns	1) Contact customer to verify purchases are legitimate and i.d. card is not stolen	2) If any suspicion of fraud remains, suspend charging ability	3) If any suspicion of fraud remains, notify University Police

Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account	1) Contact customer to determine correct address	2) If unable to determine correct address, suspend charging ability until resolved	