University System of New Hampshire

Identity Theft Prevention Program

Approved by the USNH Board of Trustees on April 30, 2009

I. PROGRAM ADOPTION

The University System of New Hampshire (USNH) developed its Identity Theft Prevention Program (Program) pursuant to the Federal Trade Commission's (FTC) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size and complexity of USNH's operations, systems, and accounts, and the nature and scope of USNH activities, the USNH Board of Trustees determined that this Program was appropriate for USNH, and approved it on April 30, 2009.

II. DEFINITIONS AND PROGRAM

A. Red Flags Rule Definitions Used in this Program[1]

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

A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

A "Covered Account" includes all student, employee, or other customer accounts, multiple transactions, or loans that are administered by USNH.

"Program Administrator" is the individual designated with primary responsibility for oversight of the program. See Section VI below.

"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, passwords, or personal account numbers.

B. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, USNH is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity, and the nature of its operation, containing reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;

2. Detect Red Flags that have been incorporated into the Program;

[1] This program and its definitions are based on a model provided by the National Association of College and University Business Officers.

3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

4. Ensure the Program is updated periodically to reflect changes in risks to students, employees, or other customers for Identity Theft and mitigating Red Flags controls are changed accordingly.

III. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, each USNH institution shall have its Information Security Working Group consider 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.

Each USNH institution identifies where the following Red Flags may occur in relation to its accounts and related operations:

A. Notifications and Warnings from Credit Reporting Agencies

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; and

5. Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

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 identifying information that is not consistent with existing student, employee, or other customer information; and

4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. Identifying information presented that is inconsistent with other information the student, employee, or other customer provides (example: inconsistent birth dates);

2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);

3. Identifying information presented that is inconsistent with the information that is on file for the student, employee, or other customer.

4. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

5. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

6. Social security number presented that is the same as one given by another student, employee or other customer;

7. An address or phone number presented that is the same as that of another person; and

8. Failure of a person to provide complete personal identifying information on an application when reminded to do so.

D. Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the person's name;

2. Stopping of payments on an otherwise consistently up-to-date account;

3. Use of an account in a way that is not consistent with prior use;

4. Repeated return as undeliverable of mail sent to the student, employee, or other customer;

5. Notice to the institution that a student, employee, or other customer is not receiving mail sent by the institution;

6. Notice to the institution that an account has unauthorized activity;

7. Breach in the institution's computer system security; and

8. Unauthorized access to or use of student, employee, or other customer account information.

E. Alerts from Others

1. Notice to USNH institutions from a student, identity theft victim, law enforcement, or other person that USNH has opened or is maintaining a fraudulent account for a person engaged in identity theft.

IV. <u>DETECTING RED FLAGS</u>

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, USNH personnel will take the following steps to obtain and verify the identity of the person opening the account:

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 photo identification).

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, USNH personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students, employees, or other customers if they request information (in person, via telephone, via facsimile, or via e-mail);

2. Verify the validity of requests to change billing addresses by mail or e-mail and provide the student, employee, or other customer 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 or Covered Accounts for which a credit or background report is sought, USNH personnel will take the following steps to assist in identifying address discrepancies:

1. Verify with 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 applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the USNH has reasonably confirmed is accurate.

V. <u>PREVENTING AND MITIGATING IDENTITY THEFT</u>

In the event USNH personnel detect 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:

A. Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of identity theft;

2. Contact the student or applicant (for which a credit report was run);

3. Change any passwords or other security devices that permit access to Covered Accounts;

4. Do not open a new Covered Account;

5. Provide the student with a new student identification number;

6. Notify the Program Administrator for determination of the appropriate step(s) to take;

7. Notify law enforcement;

8. Notify the New Hampshire Attorney General's Office under RSA 359-C; or

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

B. Protect Student and Other Customer Identifying Information

In order to further prevent the likelihood of identity theft occurring with respect to Covered Accounts, USNH will take the following steps with respect to its internal operating procedures to protect student and other customer identifying information:

1. Ensure that its websites are secure or provide clear notice that the websites are not secure;

2. Ensure that printed materials containing identifying information are secured in sealed envelopes for transmitting via campus mail or between offices and that mail-drops and mailrooms for pick-up of the envelopes are also secured.

3. Ensure complete and secure destruction of paper documents and computer files containing student or other customer account information when a decision has been made to no longer maintain such information;

4. Ensure that office computers with access to Covered Account information are password-protected;

5. Avoid use of social security numbers whenever possible;

6. Ensure computer virus protection is up to date; and

7. Require and keep only the kinds of student or other customer information necessary for USNH purposes.

VI. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the USNH Information Security Committee (Committee). Among its other responsibilities, the Committee is responsible for promoting policies for protecting personally identifiable information; ensuring appropriate training of USNH staff on the Program and related policies; 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. The USNH Executive Director of Information Technology serves as the Committee's Chair and as the Program Administrator on behalf of the Committee.

Oversight of the Committee is provided by the USNH Information Technology Policy Advisory Committee (ITPAC), chaired by the USNH Vice Chancellor and Treasurer. ITPAC's membership includes the chief financial officers and the chief information officers of USNH and each of its institutions. See Appendix A for the USNH Governance Chart for the Identity Theft Prevention Program.

B. Staff Training and Reports

USNH staff responsible for implementing the Program shall be trained 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. USNH staff shall be trained, as necessary, to effectively implement the Program. USNH employees are expected to notify the Program Administrator once they become aware of an incident of identity theft or of USNH's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, USNH 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 USNH engages a service provider to perform an activity in connection with one or more Covered Accounts, USNH 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 USNH's Program and report any Red Flags to the Program Administrator or USNH 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 Flag 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 them. 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 USNH 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 periodically review and update this Program to reflect changes in risks to students, employees, and other customers and the soundness of USNH controls to detect and prevent identity theft. In doing so, the Committee will consider the USNH's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in USNH's business arrangements with other entities. After considering these factors, the Committee will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Committee will update the Program.

APPENDIX A

USNH GOVERNANCE CHART FOR IMPLEMENTATION OF FTC RED FLAGS RULES PERTAINING TO IDENTITY FRAUD