University System of New Hampshire

Identity Theft Prevention Program
(Red Flag Rule Program)

I. Background

On November 7, 2007, the Federal Trade Commission, in conjunction with several other federal agencies, promulgated a set of final regulations known as the "Red Flags Rule". The Red Flags Rule regulations require entities with accounts covered by the Red Flags Rule regulations, including universities, to develop and implement a written Identity Theft Prevention Program (hereinafter, the "Program" or the "Identity Theft Program") for combating identity theft in connection with certain accounts. The Program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft.

II. Scope

This policy applies to USNH and all its component institutions

III. Definitions

"*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"*
Each USNH institution will periodically determine whether it offers or maintains covered accounts. A covered account means:

1. An account offered or maintained, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account or savings account; AND
2. Any other account offered or maintained that poses a reasonably foreseeable risk to customers of identity theft, including financial, operational, compliance, reputation or litigation risks.

"Risk Assessment":

As part of identifying and determining covered accounts, USNH must conduct a risk assessment to determine whether it offers or maintains covered accounts as described above, taking into consideration:

1. The methods it provides to open its accounts;

2. The methods it provides to access its accounts; AND
3. Its previous experience with identity theft.

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

IV. 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:

a. Identify relevant Red Flags for new and existing covered accounts 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. Ensure the Program is updated annually to reflect changes in risks to students, employees, or other customers for Identity Theft and mitigating Red Flags controls are changed accordingly.

V. IDENTIFICATION OF RED FLAGS

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

i. Report of fraud accompanying a credit report.

ii. Notice or report from a credit agency of a credit freeze on an applicant.

iii. Notice or report from a credit agency of an active-duty alert for an applicant.

iv. Receipt of a notice of address discrepancy in response to a credit report request; and

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

b. Suspicious Documents

i. Identification document or card that appears to be forged, altered, or inauthentic.

ii. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.

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

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

c. Suspicious Personal Identifying Information

i. Identifying information presented that is inconsistent with other information the student, employee, or other customer provides (example: inconsistent birth dates); Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application).

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

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

iv. Identifying information presented that is consistent with fraudulent

activity (such as an invalid phone number or fictitious billing address).

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

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

vii. 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

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

ii. Stopping of payments on an otherwise consistently up to date account.

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

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

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

vi. Notice to the institution that an account has unauthorized activity.

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

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

e. Alerts from Others

i. 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

a.

VI. Detecting Red Flags

a. Student Enrollment

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

i. Require certain identifying information such as name, date of birth, academic records, home address, or other identification; and

ii. 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 working with covered accounts will take the following steps to monitor transactions on an account:

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

ii. Verify the validity of requests to change billing addresses by mail or e-mail and

iii. provide the student, employee, or other customer a reasonable means of promptly reporting incorrect billing address changes; and

iv. 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 working with covered accounts will take the following steps to assist in identifying address discrepancies:

i. 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

ii. 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.

VI. PREVENTING AND MITIGATING IDENTITY THEFT

In the event USNH personnel working with covered accounts 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

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

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

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

iv. Do not open a new Covered Account.

v. Provide the student with a new student identification number.

vi. Notify the RFR Committee campus representative for determination of the appropriate step(s) to take.

1. Reporting an incident (if applicable): Cybersecurity setup reporting cyber incidents, including detection of red flags at: https://td.unh.edu/TDClient/60/Portal/Requests/ServiceCatalog?CategoryID=47

vii. Determine if a Suspicious Activity Report (SAR) should be filed

viii. Notify law enforcement.

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

x. 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:

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

ii. 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.

iii. 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.

iv. Ensure that office computers with access to Covered Account information are password protected.

v. Avoid use of social security numbers whenever possible.

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

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

VII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Red Flag Rule Committee (RFRC). The Committee will include representatives from each member institution appointed by the institution's Chief Financial Officer (CFO) . 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.

Oversight of the Committee is provided by the Finance Executive Council (FINEC) chaired by the USNH Vice Chancellor and Treasurer/CAO. FINEC's membership includes the CFOs of each USNH institution and the Associate Vice Chancellor for Financial Affairs.

B. Staff Training and Reports

i. USNH staff responsible for implementing the Program shall be trained 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.

ii. USNH employees are expected to notify the Chief Security Officer once they become aware of an incident of identity theft or of USNH's failure to comply with this Program.

iii. At least annually or as otherwise requested, USNH staff responsible for development, implementation, and administration of the Program shall report to the RFRC campus representative 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. Such department or employee 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 RFRC will annually 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.

F: Additional Resources:

a. https://consumer.ftc.gov/articles/what-know-about-identity-theft
b. https://consumer.ftc.gov/features/identity-theft

University System of New Hampshire
Red Flags Rule Committee Charter

Background: On November 7, 2007, the Federal Trade Commission, in conjunction with several other federal agencies, promulgated a set of final regulations known as the "Red Flags Rule". The FTC requires entities with accounts covered by the Rule, including universities, to develop and implement a written Identity Theft Prevention Program (hereinafter, the "Program" or the "Identity Theft Program") for combating identity theft in connection with certain accounts. The Program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft.

Purpose: The Red Flags Rule Committee (RFRC) is a standing working group within the University System of New Hampshire (USNH). The Committee is advisory to the USNH Finance Executive Council and is charged with overseeing and coordinating the USNH Identity Theft Prevention program.

Membership and Structure: Membership of the committee will be the USNH Chief Information Security Officer or designee; at least one representative from each institution appointed by the CFO, and the USNH Manager of Policy and Risk; the Director of Internal Audit serves as an ex officio member of the committee. A representative from the USNH General Counsel's Office will provide advice and counsel to the committee. Other campus or USNH system staff may be invited to attend meetings as needed.

The Committee will function as a collaborative group and will be distinguished by consultation across all its members on agenda items; planning for matters and identification of responsible individuals to undertake tasks agreed to by the Committee; and other work products of the Committee.

Meetings: The Committee will have regular meetings sufficient to meet its objectives. Meetings may be held via video conferencing to reduce travel time and create operational efficiencies.

Objectives:

- The Committee will work to reduce the risk of identity theft and maintain compliance with the FTC Red Flags Rule through the following:
    - establish a written "Identity Theft Prevention Program"
    - conduct a risk assessment to identify new and existing accounts that are covered by the Red Flags Rule
    - identify Red Flags that are relevant to the types of accounts maintained by USNH and its component institutions and develop a program to detect those Red Flags
    - respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft

- ensure that USNH personnel working with covered accounts are trained on the Red Flags Rule procedures; and

- review and update the Identify Theft Program annually to reflect changes in risks to students, employees, or other customers for identity theft and augment Red Flags accordingly

- Be an effective and high functioning group that champions identity theft prevention and compliance with the Red Flags Rule across USNH.

- Recommend processes for monitoring, supporting, and ensuring any and all corrective actions are applied.

- Report any feedback, concerns, and identify needed resources to FINEC.

This Charter will be reviewed annually.