NEVADA SYSTEM OF HIGHER EDUCATION
PROCEDURES AND GUIDELINES MANUAL

CHAPTER 13

IDENTITY THEFT PREVENTION PROGRAM (RED FLAG RULES)

CHAPTER 13

IDENTITY THEFT PREVENTION PROGRAM
(RED FLAG RULES)

Section 1. NSHE

I. POLICY AND PURPOSE

This policy is intended to meet the requirements of the FTC "Red Flag Rule." The Nevada System of Higher Education and its institutions have adopted this policy, except where separately approved institution specific policies have been approved. This policy, and any other approved institution specific policies, shall be included in the NSHE *Procedures and Guidelines Manual*. Oversight of this policy is through the chancellor's Office and institution presidents. After the initial approval of policies by the Board of Regents in June 2009, amendments may be approved by the chancellor. Institutions may also develop additional procedures with the approval of the institution president.

Identity theft is a fraud committed or attempted using the identifying information of another person without authority. It is the policy of NSHE to undertake reasonable measures to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account," and to establish a system for reporting a security incident.

II. BACKGROUND

Red Flag Rules

In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACT Act) which required the Federal Trade Commission (FTC) to issue regulations requiring "creditors" to adopt policies and procedures to prevent identify theft.

In 2007, the Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule. The rule requires "financial institutions" and "creditors" holding "covered accounts" to develop and implement a written identity theft prevention program designed to identify, detect and respond to "Red Flags." That regulation is scheduled to be enforceable on August 1, 2009.

III. DEFINITIONS

Covered Account – A covered account is a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition or fee installment payment plan.

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 Examples of activities that indicate a college or university is a "creditor" are:

- Participation in the Federal Perkins Loan program;
- Participation as a school lender in the Federal Family Education Loan Program;
- Offering institutional loans to students, faculty or staff;
- Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester.

Identifying Information – Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, routing code or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

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

Security Incident – A collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

IV. IDENTIFICATION OF RED FLAGS

Broad categories of "Red Flags" include the following:

- **Alerts** – alerts, notifications, or warnings from a consumer reporting agency including fraud alerts, credit freezes, or official notice of address discrepancies.
- **Suspicious Documents –** such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut up, re-assembled and photocopied.
- **Suspicious Personal Identifying Information** – such as discrepancies in address, Social Security Number, or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; personal information of others already on file; and/or failure to provide all required information.
- **Unusual Use or Suspicious Account Activity** –such as material changes in payment patterns, notification that the account holder is not receiving mailed statement, or that the account has unauthorized charges;
- **Notice from Others Indicating Possible Identify Theft** –such as the institution receiving notice from a victim of identity theft, law enforcement, or another account holder reports that a fraudulent account was opened.

V. DETECTION OF RED FLAGS

Employees shall undertake reasonable diligence to identify Red Flags in connection with the opening of covered accounts as well as existing covered accounts through such methods as:

- Obtaining and verifying identity;
- Authenticating customers; and
- Monitoring transactions.

A data security incident that results in unauthorized access to a customer's account record or a notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the university or to a fraudulent web site may heighten the risk of identity theft and should be considered Red Flags.

VI. RESPONSE TO RED FLAGS

Unless otherwise directed by the college or university, the detection of a Red Flag by an employee shall be reported to chief security officer for the institution. Based on the type of Red Flag, the appropriate administrator and the chief security officer will determine the appropriate response

VII. SECURITY INCIDENT REPORTING

An employee who believes that a security incident has occurred shall immediately notify their appropriate administrator and, unless otherwise directed by the institution, the chief security officer. After normal business hours, notification shall be made to the institution police or other responsible after hours administrator. Upon review of the incident, the responsible administrator shall determine what steps may be required to mitigate any issues that arise in the review. In addition, referral to law enforcement may be required.

VIII. TRAINING AND PROGRAM REVIEW

All employees who process any information related to a covered account shall receive training following appointment on the procedures outlined in this document. Refresher training may be provided annually.

Periodically the policy, procedure and training shall be reviewed to assess the need for changes or improvements.
(Added 6/09)

Section 2. UNR

In recognition that some university activities are subject to the provisions of the Fair and Accurate Credit Transactions Act (FACT Act) and its "Red Flag" rules as promulgated by the U.S. Federal Trade Commission, the university outlines the following program. This program complements existing policies, which can be found in various sections of the university's *Information Technology Policy Manual.*

Purpose

1. This document establishes the university's "Identity Theft Program" to detect, identify, and mitigate identity theft in the accounts covered under the Red Flags rules.
2. The university incorporates relevant Red Flags into a program to enable the university to detect and respond to potential identity theft.
3. The university ensures that the program is updated periodically to reflect changes in risks to customers or creditors or to the university from identity theft.

Definitions

1. Pursuant to the Red Flag regulations at 16 C.F.R. § 681.2, the following definitions apply to the Program:

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

    b. "Covered accounts"
        i. Any university account maintained primarily for a student or related to a loan administered by the university, which involves multiple payments or transactions.
        ii. Any university account for which there is a reasonably foreseeable risk from identify theft to customers.

    c. "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of identity theft."

    d. "Identifying information"
        i. Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to: 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, unique electronic identification number (including student ID), computer Internet Protocol addresses or routing codes.

    e. "Responsible university Official"
        i. The president shall designate a senior university official to serve as program administrator.
        ii. The program administrator shall exercise appropriate and effective oversight of the program and shall report regularly to the president on the program.

Program Administration and Maintenance

1. The program administrator is responsible for:
    a. Developing, implementing, and updating the university's program.
    b. Ensuring appropriate training of university staff on the program.
    c. Reviewing staff reports regarding the detection of Red Flags.
    d. Reviewing steps for identifying, preventing, and mitigating identity theft.

e. Determining which steps of prevention and mitigation should be taken in specific circumstances.
f. Reviewing, evaluating, and promulgating periodic changes to the program based on:
    i. Changes in identity theft risks, detection, mitigation, and prevention methods.
    ii. Technological advances.
    iii. university's experiences with identity theft.
    iv. Changes in types of accounts the university maintains.
    v. Changes in the university's business arrangements with other entities.
    vi. Changes in legal requirements in the area of identity theft.

Identification of Red Flags

1. The following are relevant Red Flags, in each of the listed categories for which employees should be aware and diligent in monitoring:
    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 a customer or applicant;
        iii. Notice or report from a credit agency of an active duty alert for an applicant; and
        iv. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

    b. Suspicious documents
        i. Identification document that appears to be forged, altered, or inauthentic;
        ii. Identification document on which a person's photograph or physical description is inconsistent with the person presenting the document;
        iii. Other document with information that is inconsistent with existing customer information (such as if a person's signature on a check appears forged); or
        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 customer provides (example: inconsistent birth dates);
        ii. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
        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 customer;
        vi. An address or phone number presented that is the same as that of another person;
        vii. A person fails to provide complete, personal identifying information on an application when reminded to do so (however, by law social security numbers may not be required in all instances); and

viii. A person’s identifying information is inconsistent with the information that is on file for the customer.

d. Suspicious account activity or unusual use of account
   i. Change of address for an account followed by a request to change the account holder's name;
   ii. Payments stop on an otherwise consistently up-to-date account;
   iii. Account used in a way that is inconsistent with prior use (example: very high activity);
   iv. Mail sent to the account holder is repeatedly returned as undeliverable;
   v. Notice to the university that a customer is not receiving mail sent by the university;
   vi. Notice to the university that an account has unauthorized activity;
   vii. Breach in the university’s computer system security; and
   viii. Unauthorized access to or use of customer account information.

e. Alerts from others
   i. Notice to the university from a customer, identity theft victim, law enforcement, or other person who has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Detecting Red Flags

1. New accounts
   a. university personnel will take the following steps to obtain and verify the identity of the person opening an account:
      i. Require personal identifying information such as name, date of birth, residential or business address, driver's license, or other identification;
      ii. Verify customer's identity (for instance, review a driver's license or other identification card); or
      iii. Independently contact the customer.

2. Existing accounts
      a. university personnel will take the following steps to monitor transactions with an account:
      b. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
      c. Verify the validity of requests to change billing addresses; and
      d. Verify changes in banking information given for billing and payment purposes.

Responding to Red Flags and Mitigating Identity Theft

1. In the event university personnel detect identified Red Flags, such personnel shall take all appropriate steps to respond and to mitigate identity theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to the following examples:
   a. Continue to monitor an account for evidence of identity theft;
   b. Contact the customer;
   c. Change any passwords or other security devices that permit access to accounts;
   d. Not open a new account;
   e. Close an existing account;
   f. Reopen an account with a new number;
   g. Notify law enforcement; or
   h. Determine that no response is warranted under the particular circumstances.

Staff Training and Reporting

1. university employees 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.

2. Appropriate staff shall provide reports to the program administrator on incidents of identity theft, the effectiveness of the program, and the university's compliance with the program.

Service Provider Arrangements

1. In the event the university engages a service provider to perform an activity in connection with one or more covered accounts, the university will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

   a. Require, by contract, that service providers have such policies and procedures in place; and
   b. Require, by contract, that any service providers review the university's program and report any Red Flags to the program administrator.

(Added 6/09)

Section 3. WNC

Western Nevada College (WNC) developed and implemented this Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. In recognition that some activities of WNC are subject to the provisions of this Rule as promulgated by the Commission, the college adopted the following policy. This policy complements, and is supported by existing department data security policies at the college.

I. Purpose

As required, WNC establishes an "Identity Theft Program" to detect, identify, and mitigate identity theft in the accounts covered under the Red Flag rules at the college.

a. The college will incorporate relevant Red Flags into a policy to enable the college to detect and respond to potential identity theft.
b. The college shall ensure that the policy is updated periodically to reflect changes in risks to customers or creditors or to the college from identity theft.

II. Definitions

Pursuant to the Red Flag regulations at 16 C.F.R. § 681.2, the following definitions apply to this policy:

a. "Identity theft" is a "fraud committed or attempted using the identifying information of another person without authority."
b. "Covered accounts"
    1. Any university account maintained primarily for a student or related to a loan administered by the university, which involves multiple payments or transactions.
    2. Any university account for which there is a reasonably foreseeable risk from identify theft to customers.
c. "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of identity theft."
d. "Identifying information": Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, but not limited to: 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, unique electronic identification number (including student ID), computer Internet Protocol addresses or routing codes.
e. Identification of a "Responsible University Official"
    1. The president designates the vice president of finance and administrative services as the Policy Administrator.
    2. The Policy Administrator shall exercise appropriate and effective oversight of the policy and shall report regularly to the president on the status of the policy.

III. Program Administration and Maintenance

a. The Policy Administrator is responsible for:
    1. Developing, implementing, and updating WNC's policy;
    2. Ensuring appropriate training of college staff on the policy;
    3. Reviewing staff reports regarding the detection of Red Flags;
    4. Reviewing steps for identifying, preventing, and mitigating identity theft;
    5. Determining appropriate prevention and mitigation steps to be taken in specific circumstances;
    6. Reviewing, evaluating, and promulgating periodic changes to the Policy based on:
        i. Changes in identity theft risks, detection, mitigation, and prevention methods
        ii. Technological advances
        iii. College's experiences with identity theft
        iv. Changes in types of accounts the college maintains
        v. Changes in the college's business arrangements with other entities
        vi. Changes in legal requirements related to identity theft.

IV. Identification of Red Flags

The following are relevant Red Flags in each of the listed categories for which employees should be aware and diligent in monitoring:

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 a customer or applicant;
    3. Notice or report from a credit agency of an active duty alert for an applicant; and
    4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.
b. Suspicious documents
    1. Identification document that appears to be forged, altered, or inauthentic;
    2. Identification document on which a person's photograph or physical description is inconsistent with the person presenting the document;
    3. Other document with information that is inconsistent with existing customer information (such as if a person's signature on a check appears forged); or
    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 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 credit report);
    3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social Security number presented that is the same as one given by another individual;
6. An address or phone number presented that is the same as that of another person;
7. A person fails to provide complete, personal identifying information on an application when reminded to do so (however, by law Social Security numbers may not be required in all instances); and
8. A person's identifying information is inconsistent with the information that is on file for the customer.

d. Suspicious account activity or unusual use of account
   1. Change of address for an account followed by a request to change the account holder's name;
   2. Payments stop on an otherwise consistently up-to-date account;
   3. Account used in a way that is inconsistent with prior use (example: very high activity);
   4. Mail sent to the account holder is repeatedly returned as undeliverable;
   5. Notice to the college that a customer is not receiving mail sent by the institution;
   6. Notice to the college that an account has unauthorized activity;
   7. Breach in the college's or NSHE's computer system security; and
   8. Unauthorized access to or use of customer account information.

e. Alerts from others
   1. Notice to the college from an individual, identity theft victim, law enforcement, or other person who has opened or is maintaining a fraudulent account for a person engaged in identity theft.

V. Detecting Red Flags

a. New accounts
   1. College personnel will take the following steps to obtain and verify the identity of the person opening an account:
      i. Require personal identifying information such as name, date of birth, residential or business address, driver's license, or other identification;
      ii. Verify customer's identity (for instance, review a driver's license or other identification card);
      iii. Independently contact the customer.

b. Existing accounts
   1. College personnel will take the following steps to monitor transactions with an account:
      i. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
      ii. Verify the validity of requests to change billing addresses; and
      iii. Verify changes in banking information given for billing and payment purposes.

VI. Responding to Red Flags and Mitigating Identity Theft

a. In the event college personnel detect identified Red Flags, such personnel shall take all appropriate steps to respond and to mitigate identity theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to the following examples:

1. Continue to monitor an account for evidence of Identity theft;
2. Contact the individual;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;
7. Notify public safety and/or law enforcement; or
8. Determine that no response is warranted under the particular circumstances.

VII. Staff Training and Reporting

a. College employees responsible for implementing the Policy shall be trained in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

b. Appropriate staff shall provide reports to the Policy Administrator on incidents of identity theft, the effectiveness of the Policy, and the college's compliance with the Policy.

VIII. Service Provider Arrangements

a. When the college engages a service provider to perform an activity in connection with one or more covered accounts, the college 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:

i. Require, by contract, that service providers have such policies and procedures in place; and

ii. Require, by contract, that any service providers review the college's Policy and report any Red Flags to the Policy Administrator.

(Added 6/09)