

NSHE Identity Theft Red Flag Policy and Procedure

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 as approved by the Chancellor’s Office and the Board of Regents. This policy shall be included in the NSHE Procedures and Guidelines Manual. Oversight of this policy is through the Chancellor’s Office and institution presidents, and amendments may be approved by the Chancellor. This policy is effective as to all NSHE institutions, but the institutions may expand the policy and further identify 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 became enforceable on May 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 off 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.

(Effective April 2009)

DRAFT