Northeastern University

Identity Theft Prevention Program

Effective May 1, 2009

Northeastern University
Identity Theft Prevention Program

Table of Contents

Section 1: Program Adoption

Northeastern University, hereinafter known as (“the University”), has developed this Identity Theft Prevention Program ("the Program") pursuant to the Federal Trade Commission Red Flags Rule that implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. This program was developed with consideration of the size and complexity of the University's operations and account systems, and the nature and scope of the University's activities. The University Board of Trustees approved this Program on May 1, 2009.

Section 2. Red Flags Rule Definitions Used in the Program

Term	**Red Flag Definition Used in the Program**
Identity Theft	A fraud or committed or attempted to be committed using identifying information of another person.
Red Flag	A pattern, practice, or specific activity or set of activities that indicates a potential, real or possible existence of Identity Theft.
Covered Account	An account or loan administered by the University.
Program Administrator	The individual designated with primary responsibility to oversee the Identity Theft Prevention program. See Section 6 below.
Identifying information	Any name or number that may be used, alone or in conjunction with any other information to positively identify a specific person, including, but not limited to name, address, 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 or student identification number.

Section 2A. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, the University is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. This program contains policies and procedures to:

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

- *Detect Red Flags incorporated into the Program.*

- *Provide that the Program is updated periodically to reflect changes in potential risks to students or to the safety of students from Identity Theft.*

Section 3: Identification of Red Flags

In order to identify relevant Red Flags, the University considers the types of information it requests, accepts, offers and maintains, the methods it uses to provide electronic access to information that could be used to commit Identity Theft; and previous experiences. The University identifies the following Red Flags in each of the listed categories:

Category	Red Flags
A. Notifications and Warnings from Credit Reporting Agencies	• Report of fraud accompanying a credit report. • Notice or report from a credit reporting agency of a credit freeze on an individuals credit report. • Notice or report from a credit reporting agency of an active duty alert for an individual. • Receipt of a notice of address discrepancy in response to a credit report request. • Indication from a credit report of activity inconsistent with an individual's usual patterns or activities.
B. Suspicious Documents and/or credentials	• Identification document that appears to be forged, tampered with, altered or inauthentic. • Identification document bearing a person's photograph or physical description that is inconsistent with the person presenting the document. • A document with information that is not consistent with existing information, and/or information held in University-owned or related/maintained systems of record • Any other form of communication or that appears to be forged, tampered with, altered or inauthentic

Section 3: Identification of Red Flags (continued)

Category	Red Flags
C. Suspicious Identifying Information	Identifying information presented that is inconsistent with other information provided by a student. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application). Identifying information presented that is the same as information shown on other applications, communications, or documents that are suspected or shown to be fraudulent Social security number presented that is the same as that given by another person. Identifying information presented that is consistent with fraudulent activity, including, but not exclusive to invalid phone number and/or fictitious billing address Any other inconsistency between known and presented identifying information
D. Suspicious Record Information	An address or phone number presented that is the same as that of another person, without an accompanying adequate and reasonable explanation. Failure of a person to provide complete personal identifying information on an application when asked to do so. A person's identifying information is not consistent with the information on file for that person

Section 3: Identification of Red Flags (continued)

Category	Red Flags
E. Suspicious Covered Account Activity or Unusual Use of Account	Change of address for an account followed by a request to change the student's name. Payments stop on an otherwise consistently up-to-date account. Account used in a way inconsistent with prior use or use pattern(s). Paper mail sent to a person is repeatedly returned as undeliverable. Notice to the University that a person is not receiving paper mail sent by the University. Notice to the University that an account has unauthorized activity; Breach in the University's computer system security Unauthorized access to and/or use of student account information.
F. Alerts from Others	Notice to the University from a student, alleged Identity Theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft

Section 4: Detecting Red Flags

Section 4A: Enrollment of a student

In order to detect Red Flags identified above associated with the **enrollment** of a student, University personnel or its agents will take the following steps to obtain and verify the identity of person(s) opening covered account(s)

Action(s) required when **opening a covered account**
• Require certain identifying information such as name, date of birth, academic records, home address or other identification. • Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification). • The student identification card shall be produced by the University subsequent to the above verification step.

Section 4B: Existing Covered Accounts

In order to detect any of the Red Flags identified above associated with an **existing Covered Account**, University personnel will take the following steps to monitor transactions on such an account:

Action(s) required to **monitor transactions on a covered account**
• Verify the identification of students when they request information, including, but not exclusive to in person, telephone, facsimile or email requests. • Verify the validity of requests to change billing addresses by mail or email and provide students a reasonable means of promptly reporting incorrect billing address changes • Verify changes in banking information given for billing and payment purposes.

Section 4C. Consumer (“Credit”) Report Requests

In order to detect any of the Red Flags identified above for an employment position for which a credit report is sought, University personnel or its agents will take the following steps to assist in identifying address discrepancies:

Action(s) required to **assist in identifying address discrepancies when credit or background report is sought**
• Require written verification from applicants that an address provided by the applicant is accurate at the time the request for a credit report is made to the consumer reporting agency • 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 University has reasonably confirmed is accurate.

Section 5: Reporting and Managing Red Fags

All suspected or real red flags shall be reported and managed using the process described below

Step	Action
1	A person suspecting or discovering a Red Flag notifies the Director of Information Security and Identity Services by phone at x7718 and at itsecurity@neu.edu. The reporter shall clearly identify in their oral and written communications that a Red Flag condition is believed to exist.
2	The Office of Information Security and Identity Services shall convene the Identity Theft Committee to investigate the red flag(s).
3	The University may contact the student or applicant or employee.
4	If applicable, the Office of Information Security and Identity Services may advise the student to change all passwords and other security tokens, devices or other factors that permit access to Covered Accounts.
5	The University shall take the following preventive and reactive steps: a) continue to monitor a Covered Account for evidence of Identity Theft b) will not open a new Covered Account c) may provide the student with a new student identification number (if applicable) d) may notify law enforcement and/or other government agencies (if applicable)
6	The Identity Theft Program Administrator and other members of the Identity Theft Committee complete and document their investigation.
7	As may be indicated, the student is informed of the outcome of the investigation and what further actions or assistance if any may be required of the student and/or the University.
8	The Program Administrator or their designate closes the case.

Section 6: Protecting Student Identifying Information

In an effort to prevent potential Identity Theft from occurring with respect to Covered Accounts, the University shall maintain the following practices with respect to its internal operating procedures to protect student identifying information:

Practices
• University-owned electronic experiences that solicit student identifying information must be reasonably secure, [or to provide clear notice if a particular experience is not secure.]
• Destroy and/or secure paper documents and computer files containing student account information when a decision has been made to no longer maintain such information, in consultation with the Office of Information Security and Identity Services.
• Office computers with access to Covered Account information must be password protected.
• Avoid use of social security numbers (See Northeastern Policy on Collection, Handling and Use of Social Security Number (SSN).
• Computer virus protection on University-owned computers must be installed and up to date.
• Collect and maintain only those items of student identifying information that are necessary for the conduct of University academic and/or business purposes.

Section 7: Program Administration and Oversight

Responsibility for developing, implementing and updating this Program lies with the **Identity Theft Committee** for the University. The Committee is headed by the Director of Information Security and Identity Services, also known as the Program Administrator. The following additional individuals make up the remainder of the Identity Theft Committee membership.

Identity Theft Committee

Program Administrator
Glenn C, Hill, Director of Information Security and Identity Services

Additional Members

Linda Allen, University Registrar, or her designate
Daniel Fennell, Associate Bursar, or his designate
Janet Faulkner, Senior Assistant University Counsel, or her designate (Advisory capacity)
D. Joseph Griffin, Director of Public Safety, or his designate
Seamus Harreys, Dean of Student Financial Services, or his designate
John McNally, Director, Compliance and Risk Services, or his designate

The Program Administrator is responsible for:

- *Appropriate training of University staff on the Program.*

- *Reviewing reports regarding the detection of Red Flags and steps for preventing and mitigating Identity Theft.*

- *Determining which steps of prevention and mitigation should be taken in particular circumstances.*

- *Updating and making appropriate changes to the Program in response to changing conditions.*

The additional members of the Identity Theft Committee are responsible for:

- *Participating and/or assisting in Red Flag case investigation and resolution.*

- *Assisting the Program Administrator in training, reporting and program change activities.*

Section 8. Staff Training and Reports

University 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 steps to be taken when a Red Flag is detected. University staff shall be trained as necessary to implement the Program.

University employees are required to notify the Program Administrator once they become aware of a real or suspected Red Flag, an incident of Identity Theft, or about a potential failure to comply with this Program.

On an annual basis, University staff responsible for development, implementation, and administration of the Program shall report to the Program Administrator on compliance with this Program. The report shall address such issues as:

- *effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening and maintenance of Covered Accounts*

- *compliance with the program by affiliates and outside service providers*

- *significant incidents involving identity theft and management's response, and recommendations for changes to the Program.*

The report shall be delivered to the Board of Trustees annually.

Section 9. Service Provider Arrangements

In the event the University engages a vendor or service provider to perform an activity in connection with one or more Covered Accounts, the University shall take the following steps to determine that the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft:

• ***Require by contract that service providers have such policies and procedures in place; and***

• ***Require by contract that service providers review the University's Program and report any Red Flags to the Program Administrator, and the representative of the University department who is responsible for the contract.***

Section 10. Nondisclosure of Specific Practices

Knowledge about specific Red Flag identification, detection, mitigation and prevention practices and measures shall be limited to the Identity Theft Committee who developed this Program and to those employees who need to implement those practices.

Any documents that may have been produced or are produced in order to develop or implement this program that list or describe specific practices are considered "Confidential" shall not be shared with other Northeastern employees who do not need to know, nor the public, to the extent consistent with law and regulation.

The Program Administrator shall inform the Identity Theft Committee and those employees with a need to know, which documents or specific practices shall be maintained in a confidential manner. Such documents shall be marked "NU CONFIDENTIAL", and shall be safeguarded using reasonable means.

Section 11. Program Updates

The Identity Theft Committee will periodically review and update this Program to reflect changes in risks to students and the University from Identity Theft. In doing so, the Committee will:

• ***Consider the University's experiences with personal identifying information.***

• ***Review changes and trends in Identity Theft motives, methods and operandi,***

• ***Analyze changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities.***

After considering these factors, the Program Administrator shall recommend to the Identity Theft Committee what changes to the Program, including the listing of Red Flags, may be warranted. If warranted, the Committee shall update and republish this Program, and the Program Administrator or their designate shall implement additional communications and/or training to those University employees who have responsibility for implementation under this Program.