Title: Identity Theft Prevention Policy
Effective Date: June 14, 2017
Issuing Authority: New York University Chief Financial Officer
Responsible Officer: New York University Chief Financial Officer

Purpose of this Policy

The U.S. Congress has provided protection for consumers from identity theft by enacting the Fair and Accurate Credit Transactions Act (“FACTA”) and the Fair Credit Reporting Act (“FCRA”). FACTA directed the Federal Trade Commission (“FTC”) to issue regulations, now generally referred to as the “Red Flags Rule” (the “Rule”), which require financial institutions and creditors to adopt policies and procedures that protect consumers from identity theft. “Red Flags” are defined by the Rules as patterns, practices, or activities that indicate the possibility of identity theft.

As set forth in the “Definitions” section below, New York University (“NYU” or the “University”) is a “creditor” under the Rule because it advances funds to or on behalf of persons in connection with its participation in federal student loan programs and in making housing loans to faculty and staff. NYU has “covered accounts” relating to these activities under the Rule and is therefore required to establish an Identity Theft Prevention Program. Accordingly, NYU adopts this Policy to: Identify, prevent and mitigate identity theft in compliance with the Rule; approve and establish an Identity Theft Prevention Program, attached to this Policy as Appendix A (the “Program”); and appoint a Program Administrator who has primary responsibility for oversight of the Program.

Policy

It is the policy of NYU to comply with the requirements of the Rule. Accordingly, NYU has developed a Program that is designed to meet the requirements of the Rule to identify, prevent, and mitigate identity theft. This written Program is attached to this Policy as Appendix A. The Program is tailored to NYU’s size, complexity and the nature of its operations, and is based upon the University’s previous experience with identity theft associated with covered accounts. The Program contains mechanisms to: identify and detect relevant Red Flags; respond appropriately to prevent Identity Theft and mitigate damages; and ensure that the Program is updated periodically to reflect changes in risks.
Scope of this Policy

This Policy applies to all University employees, students, volunteers and agents who are involved in handling information that can be used to identify a specific person in connection with certain accounts of that person maintained by NYU. Specific operations and activities that implicate application of this policy include, but are not limited to, the following:

- The Bursar’s Office - Participating in the Federal Perkins loan program, participating as a school lender in the Federal Family Education Loan Program (FFELP)
- The Financial Aid Office - Offering loans to students or a plan for payment of tuition during the school year or thereafter
- NYU-sponsored housing and general loan programs

Policy Adoption and Oversight

The Audit and Compliance Committee of the NYU Board of Trustees has oversight of the adoption and implementation of and compliance with this Policy. The Chief Financial Officer, as the Responsible Officer for this Policy, will provide the Audit and Compliance Committee with periodic reports concerning the implementation of and compliance with this Policy and with such other reports as may be requested by the Audit and Compliance Committee.

Policy Definitions

The following Rule definitions apply to this Policy and the Program:

“Creditor” means any natural person, corporation or other entity that regularly, and in the ordinary course of business advances funds to or on behalf of a person based on an obligation to repay the funds or repayable from specific property pledged by the person.

“Covered Account” means an account that is (1) primarily for personal, family or household purposes and is designed to permit multiple payments or transactions, or (2) any account that is subject to a reasonably foreseeable risk of identity theft.

“Identifying Information” means 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, driver’s license or identification number, alien registration number, passport number, employer or taxpayer identification number.
“Identity Theft” means a fraud committed or attempted using the identifying information of another person without authority.

“Red Flag” is a pattern, practice or specific activity that indicates the potential for Identity Theft.

“Program Administrator is the University Controller or such other individual designated by the Chief Financial Officer to have primary responsibility for oversight of the Program.

Notes

1. Dates of official enactment and amendments:
   Adopted on _____
   Approved by the Audit and Compliance Committee of the Board of Trustees

2. History:
   Amended:

3. Cross References
   15 U.S.C. Section 1681m (e); 16 C.F.R. Section 68
APPENDIX A

The Identity Theft Prevention Program

Identification of Red Flags

To identify relevant Red Flags, the University considers the types of Covered Accounts that it offers and maintains; the methods it provides to open and access the Covered Accounts, including in-person, mail or online methods, and the University’s previous experience with Identity Theft. Covered Accounts include but are not limited to the following:

- Accounts managed by Faculty Housing or other units related to the administration of housing or general loan programs for faculty and staff
- Accounts managed by the Bursar’s Office related to the administration of student loan programs including the federal Perkins Loan, Health Professions Student Loan and Nursing loan programs
- Accounts managed by the Financial Aid Office related to the administration of emergency short-term loans and disbursement of funds from money specifically donated to be used for student loans, or tuition payment plans

The University has identified the following Red Flags:

- **Notifications or Warnings from Consumer/Credit Reporting Agencies**: Alerts, notifications, or other warnings received from consumer reporting agencies or service providers indicating:
  - A credit freeze
  - Active duty alert
  - Address discrepancy in response to a credit report request
  - Activity that is inconsistent with the usual pattern or activity of the account holder

- **Suspicious Documents**: Presentation of suspicious documents which appear to be altered, forged or inauthentic, including inconsistent appearance of photographs or physical description on a document with the person presenting it.

- **Suspicious Personal Identifying Information**: Presentation of inconsistent personal identifying information such as:
• An inconsistent birth date
• An address that does not match a prior address submitted on an application
• A social security number, telephone number or address that is the same as that given by another account holder
• Repeated failure to provide identifying information on an application

• **Suspicious Use or Activity in Covered Account**: Unusual use of or other suspicious activity related to a covered account including but not limited to:
  - Requests made from a non-University issued email account
  - “Unofficial” forms which are presented with requests for information
  - Mail returned as undeliverable
  - Notice of change in payments for an otherwise consistent account
  - Patient tests or lab results do not match the background information provided
  - The same identification used by multiple family members for patient services
  - Complaint from a recipient of healthcare services based on receipt of:
    - A bill for another individual
    - A bill for a product or service the patient denies receiving
    - A bill from a healthcare provider that the patient never patronized
    - A notice of insurance benefits (or Explanation of Benefits) for healthcare services never received

• **Alerts from Others**: Notice from an account holder, victim of identity theft or law enforcement authorities that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

## II Detection of Red Flags

The Program is required to establish procedures for the detection of Red Flags in the designated areas of activity. These procedures are set forth below:

• **Opening of Covered Accounts**: Identity verification of first-time account holders will be required, including presentation of identifying information such as name, date of birth, academic records or insurance card, and home address, which will be subsequently verified by review of driver’s license, passport or other government-issued photo identification and insurance company information.
• **Existing Covered Accounts**: Authentication of account holders and monitoring of transactions on the covered account will be required, including:
  - Verification of the identity of account holders if they request information (in person, via telephone, via facsimile, via email)
  - Verification of changes in banking information given for billing or payment purposes
  - Requests for billing address changes for covered Accounts must be verified and means provided to account holders for notification of changed or incorrect billing addresses
  - Students requesting medical or dental records (identity should match photo on file/identification card)
  - Patients arriving for treatment need to provide proof of identity by government issued identification or insurance card copied and checked against data in existing medical/dental records; Name, gender and DOB matched against the patient presenting insurance card

• **Consumer/Credit Report Requests**: When a consumer/credit report request results in notice of an address discrepancy from the reporting agency, University personnel will request written verification from the subject of the report that the address he/she provided is accurate, and once an address is verified, University personnel will report such address to the reporting agency.

• **Risk Assessment**: A risk assessment will be conducted annually as well as in the event that actual instances of Identity Theft occur.

### III Responses to Red Flags

In response to the detection of Red Flags, University personnel will take the appropriate action to prevent and mitigate Identity Theft depending upon the degree of risk posed by the Red Flags, including:

- Monitoring a Covered Account for suspicious activity
- Denying access to the Covered Account until information is verified to eliminate Red Flags
- Contacting the account holder to verify activity in the Covered Account
- Changing passwords, security codes or other security devices
- Closing and reopening the Covered Account
- Refusing to open a new Covered Account
- Notifying law enforcement
- Determining that no response is warranted upon reasonable investigation of the particular circumstances

IV. Updating the Program

NYU shall update this Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to students, faculty members, or others or to the safety and soundness of NYU from identity theft, based on factors such as:

- The experiences of NYU with identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent, and mitigate identity theft
- Changes in the types of accounts that NYU offers or maintains
- Changes in the business arrangements of NYU, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements

V. Methods for Administering the Program

- **Oversight of Program**: This Program shall be overseen by the Audit and Compliance Committee of the Board of Trustees. This oversight shall include:
  - The Program shall be implemented by the Chief Financial Officer with primary responsibility for oversight of the Program by a Program Administrator designated by the Chief Financial Officer
  - Reports prepared by staff regarding compliance by NYU with the Identity Theft Prevention Policy and Program shall be reviewed by the Chief Financial Officer and the Audit and Compliance Committee
  - Material changes to the Program as necessary to address changing Identity Theft risks shall be approved by the Audit and Compliance Committee
• **Staff Training and Reporting:** University personnel will be trained by or under the direction of the Program Administrator to effectively implement the Program and detect and respond to Red Flags. University personnel will notify the Program Administrator of any incident of Identity Theft or the University’s failure to comply with the Program. University personnel designated by the Program Administrator will report to the Program Administrator at least annually, or as requested. Such reports will include, among other relevant issues:
  - The effectiveness of the specific policies and procedures for addressing the current risks of Identity Theft in connection with the Covered Accounts
  - Any significant incidents involving Identity Theft and the response taken
  - Recommendations for material changes to the Program

• **Oversight of Service Providers:** In the event that the University contracts with an outside service provider to perform any activity in connection with Covered Accounts, the University will ensure that:
  - The service provider’s activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate risk of Identity Theft
  - The service provider reviews the Program and reports any Red Flags to the Program Administrator or the designated University personnel with primary oversight of the service relationship