THE CITY UNIVERSITY OF NEW YORK
IDENTITY THEFT PREVENTION PROGRAM

1. Program Adoption

The City University of New York (the "University") developed this Identity Theft Prevention Program (the "Program") pursuant to the Federal Trade Commission's Red Flags Rule (the "Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. On November 9, 2007, a joint notice of final rulemaking was published in the Federal Register (72 FR 63718) finalizing the Rule. The Rule requires each creditor that offers or maintains one or more "covered accounts", as defined below, to develop and provide for the continuing administration of a written program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or with any existing covered account.

This Program was developed with oversight and approval of the University's Board of Trustees. After 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's Board of Trustees determined that the Program was appropriate for the University and therefore approved the Program, to be effective as of October 1, 2009.

2. Definitions

2.1 "Covered Account" means: (1) An account that a Creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and (2) any other account that the Creditor offers or maintains for which there is a reasonably foreseeable risk to Customers or to the safety and soundness of the Creditor from Identity Theft, including financial, operational, compliance, reputation, or litigation risks. Examples of Covered Accounts at the University include Perkins loan accounts, tuition payment plan accounts, and accounts established for the repayment of loans provided to students by the University's college associations, which, for the purpose of the Program, will be considered to be part of the University.

2.2 "Creditor" means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

2.3 "Customer" means any person who has a Covered Account with the University.

2.4 "Identity Theft" means a fraud committed or attempted using the Identifying Information of another person without authority.

2.5 "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 but not limited to any name, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, and employer or taxpayer identification number.

2.6 “Program Administrator” means the individual designated with primary responsibility for oversight of the Program, as described in Section 7.1 below.

2.7 "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

3. Identification of Red Flags

In order to identify relevant Red Flags, the University has considered the types of Covered Accounts that it offers and maintains, the methods it provides to open and to access these accounts, and its previous experiences with Identity Theft. The University has identified the following Red Flags in each of the five listed categories:

3.1 Suspicious Documents

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the Customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new Covered Account or the Customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the University.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

3.2 Suspicious Personal Identifying Information

- Personal Identifying Information provided is not consistent with personal Identifying Information that is on file with the University.
- Personal Identifying Information provided is not consistent with external information sources used by the University.

- Personal Identifying Information provided by the Customer is not consistent with other personal Identifying Information provided by the Customer.

- Personal Identifying Information provided is associated with known fraudulent activity, as indicated by internal or third-party sources used by the University.

- Personal Identifying Information provided is of a type commonly associated with fraudulent activity, as indicated by internal or third-party sources used by the University.

- The social security number provided is the same as that submitted by other persons opening an account or other Customers.

- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other Customers.

- The person opening the Covered Account or the Customer fails to provide all required personal Identifying Information on an application or in response to notification that the application is incomplete.

- If the University uses a challenge question for the purpose of authentication, the person opening the Covered Account or the Customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

3.3 Unusual Use of, or Suspicious Activity Related to, the Covered Account

- Shortly following the notice of a change of address for a Covered Account, the University receives a request for a new, additional, or replacement card or for the addition of authorized users on the account.

- A new revolving credit account is used in a manner commonly associated with known patterns of fraud.

- A Covered Account is used in a manner that is not consistent with established patterns of activity on the account.

- A Covered Account that has been inactive for a reasonably lengthy period of time is used.

- Mail sent to the Customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Customer's Covered Account.

- The University is notified that the Customer is not receiving paper account statements.

- The University is notified of unauthorized charges or transactions in connection with a Covered Account.

- Unauthorized access to or inappropriate disclosure of Identifying Information occurs in connection with a Covered Account.

3.4 Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons regarding Possible Identity Theft in Connection with Covered Accounts

- The University is notified by a Customer, a victim of Identity Theft, a law enforcement authority, or any other person that the University has opened a fraudulent account for a person engaged in Identity Theft.

3.5 Alerts, Notifications, or Warnings from a Consumer Reporting Agency

- A fraud or credit alert is included with a consumer report.

- A notice of credit freeze on a consumer report is provided from a consumer reporting agency.

- A consumer reporting agency provides a notice of address discrepancy.

- A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a Customer.

4. Detecting Red Flags

4.1 Student Enrollment

In order to detect any of the Red Flags identified in Section 3 above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

- Require certain Identifying Information such as name, date of birth, academic records, home address, or other identification; and

- Verify the student's identity at time of issuance of a student identification card, including review of a driver's license or other government-issued photo identification.

4.2 Existing Accounts

In order to detect any of the Red Flags identified in Section 3 above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:

- Verify the identification of a student in person or via telephone if he or she requests information related to the Covered Account by asking questions with readily accessible information that is on file with the University;

- Verify the validity of a student request by mail or e-mail to change an address or banking information in connection with the Covered Account by asking questions with readily accessible information that is on file with the University; and

- Provide students a reasonable means of promptly reporting incorrect changes in addresses or banking information in connection with Covered Accounts.

4.3 Consumer Report Requests

In order to detect any of the Red Flags identified in Section 3 above in a case in which the University seeks a consumer report, University personnel will take the following steps to assist in identifying address discrepancies:

- Require written verification from the subject of the consumer report that the address provided by him or her is accurate at the time the request for the consumer report is made to the consumer reporting agency; and

- In the event that notice of an address discrepancy is received, verify that the consumer report pertains to the subject of the requested report and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

5. Preventing and Mitigating Identity Theft

In the event any University personnel detects any of the Red Flags identified in Section 3 above, he or she will take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

- Not open a new Covered Account;
- Change any passwords or other security devices that permit access to the Covered Account;
- Contact the student or the applicant for which a consumer report was run;
- Notify the Program Administrator or his or her designee to determine the appropriate step(s) to take;
- Continue to monitor the Covered Account for evidence of Identity Theft;
- Notify law enforcement; and/or
- Determine that no response is warranted under the particular circumstances.

6. Protecting Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the University has established and disseminated Information Technology Security Procedures to limit access and disclosure of Identifying Information and require that all individuals permitted access to such information in University files and systems, whether in computerized or printed form, are continually responsible for maintaining the integrity, accuracy, and privacy of such information. These Information Technology Security Procedures are available online at http://portal.cuny.edu/cms/id/cuny/documents/INFOSEC/Policies/PDFs/policy8.pdf

7. Program Administration

7.1 Oversight

The development, implementation, and updating of the Program are the responsibility of the University's Identity Theft Prevention Committee (the "Committee") established under the Program. The Committee will be headed by the Program Administrator, who will be the University Controller or his or her designee. Two or more other individuals who represent functional departments within the University that are responsible for opening and/or maintaining Covered Accounts and who are appointed by the Program Administrator will comprise the remainder of the Committee's membership. The Committee will be responsible for ensuring appropriate training of University personnel with respect to the Program, reviewing any reports concerning 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 in the Program.

7.2 Staff Training and Reports

University personnel responsible for implementing the Program will be trained under the direction of the Committee to detect Red Flags and determine the responsive steps to be taken when a Red Flag is detected. University personnel will be trained, as necessary, to carry out the Program effectively. University personnel are expected to notify the Committee once they become aware of an incident of Identity Theft or the University's failure to comply with the Program. At least annually or as otherwise requested by the Committee, University personnel responsible for the development, implementation, and administration of the Program will report to the Committee on compliance with the Program. The report will cover such issues as effectiveness of the University's policies and procedures in addressing the risk of Identity Theft in connection with the opening and maintenance of Covered Accounts, the effectiveness of the University's service provider arrangements in complying with the Program, significant incidents involving Identity Theft at the University and the University's response, and recommendations for changes in the Program.

7.3 Service Provider Arrangements

In the event the University has engaged or engages in the future any service provider to perform an activity in connection with any 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:

- Require, by contract, that the service provider have its own similar policies and procedures in place; and

- Require, by contract, that the service provider review the University's Program and report any Red Flags to the Program Administrator or the University employee with primary oversight of the relationship with the service provider.

7.4 Program Updates

The Committee will periodically review and update the Program to reflect changes in risks to Customers or to the safety and soundness of the University from Identity Theft. In doing so, the Committee will consider the University's experiences with Identity Theft, changes in methods of Identity Theft, changes in methods to detect, prevent, and mitigate Identify Theft, and changes in the University's business arrangements with other entities. After considering these factors, the Committee will determine whether changes in the Program, including the list of Red Flags, are warranted. If warranted, the Committee will update the Program.