APPROVED

LAWRENCE CACCIATORE
SECRETARY TO THE BOARD OF TRUSTEES

THE COOPER UNION FOR THE ADVANCEMENT OF SCIENCE AND ART

"RED FLAGS" IDENTITY THEFT PREVENTION PROGRAM

February 24, 2010

I. Introduction

A. Purpose

The Cooper Union for the Advancement of Science and Art ("The Cooper Union" or the "College") has developed this Identity Theft Prevention Program (its "Program") pursuant to the Federal Trade Commission's final rules and guidelines ("Rules and Guidelines") implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"). The Rules and Guidelines require financial institutions and creditors to implement a written Identity Theft Prevention Program to detect, prevent and mitigate the risk of identity theft in connection with the opening and maintenance of certain types of accounts.

The Cooper Union has appointed the Vice President of Finance, Administration and Treasurer, as the administrator of this program (the "Program Administrator").

B. Definitions

The Rules and Guidelines define "identity theft" as a fraud committed or attempted using the identifying information of another person without authority.

The Rules and Guidelines define a "Red Flag" as a pattern, practice or specific activity that indicates the possible existence of identity theft.

The Rules and Guidelines apply to "financial institutions" and "creditors."

> Financial institutions are defined in accordance with the Fair Credit Reporting Act ("FCRA") and include banks, mortgage lenders, savings and loan associations, mutual savings banks, credit unions and any other person that, directly or indirectly, holds a transaction account belonging to a consumer.
>
> Creditors are defined as persons or businesses that arrange for the extension, renewal, or continuation of credit.

The Rules and Guidelines apply to "covered accounts" maintained by "financial institutions" and "creditors."

> A covered account is defined as (1) an account primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonable foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.

C. Scope

The Cooper Union as a Financial Institution

The Cooper Union is not a "financial institution" as defined by the Rules and Guidelines. It neither issues debit cards or stored value cards to students nor acts as a custodian of other transaction accounts.

The Cooper Union as a Creditor

In some cases, The Cooper Union would be considered a creditor with regard to some of its student and employee loan programs, and, where payment is allowed in arrears, its student fee accounts and continuing education tuition and fee accounts.

- At The Cooper Union, every student receives a full tuition scholarship and is not responsible for tuition-related costs. Nevertheless, students are responsible for living and miscellaneous expenses. To that end, The Cooper Union participates in various federal student loan and grant programs, including the Federal Perkins, Pell, Stafford, and Plus Loan programs. The Cooper Union also offers its own private loan program, Cooper Union Loans. In this program, which mirrors the Federal Perkins Loan program, the College acts as the lender. The Department of Education has stated the Rules and Guidelines apply to universities participating in the Federal Perkins Loan Program, a program in which The Cooper Union does participate, as well as other loan programs.

- The Cooper Union also offers loans through its Tuition Assistance Program for eligible employees.

- In some cases, The Cooper Union may allow students to pay fees, or continuing education students to pay tuition or fees (or portions thereof) in arrears.

- The Cooper Union does not issue credit cards or provide student health services.

Covered Accounts

The risk-based nature of the Rules and Guidelines allows each financial institution or creditor flexibility to determine which accounts will be covered by its

Program through a risk evaluation process. In addition to its student loan accounts, The Cooper Union maintains "student accounts" to which students pay for dormitory fees, lab fees, book fees, health insurance fees and other student fees. Similar to these student accounts, the College maintains accounts for its continuing education students through which continuing education students may pay tuition and other fees. The Cooper Union also offers its employees loans. The Cooper Union does not have a book store and does not offer a meal plan.

The Cooper Union has determined that this Program should apply to accounts related to its loan programs, its student accounts, including accounts for continuing education students, and its employee loan accounts (collectively, its "covered accounts").

The Cooper Union believes that it is unlikely that identity theft of one of its students or employees will occur via the use of The Cooper Union's accounts, programs, systems or services. Nonetheless, The Cooper Union has designed this Program to detect, prevent and mitigate the risk of identity theft in connection with the opening of a covered account or any existing covered account. This Program corresponds to The Cooper Union's actual operations, and thus takes into account not only the risk of identity theft but also the methods available to The Cooper Union to detect and respond to Red Flags.

II. Identification of Red Flags

The Cooper Union has identified the following identity theft Red Flags applicable to the College:

Suspicious documents:

1. Documents provided for identification appear to have been altered or forged.

2. The photograph or physical description on the identification is not consistent with the appearance of the individual presenting the identification.

3. Other information on the identification is not consistent with information provided by the individual opening a new covered account or individual presenting the identification.

4. Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check.

5. An application or other documentation appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious personal information:

1. Personal identifying information provided is inconsistent when compared against external information sources used by the College (e.g., address does not match address in consumer report, SSN has not been issued, or is listed in the SSA's Death Master File).

2. Personal identifying information provided by the individual is not consistent with other personal identifying information provided by the individual (e.g., lack of correlation between SSN range and date of birth) or information that the College already has on file.

3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College (e.g., address or phone number on application is same as that on a fraudulent application, address on application is fictitious, a mail drop or a prison, phone number is invalid or associated with a pager or answering service).

4. Personal identifying information (e.g., SSN, address, phone number) is the same as that submitted by other individuals or by an unusually large number of other persons opening accounts.

5. An applicant fails to provide all required personal identifying information on an application or in response to notifications that the application is incomplete.

6. When the College uses challenge questions to authenticate an individual, the individual cannot provide authenticating information beyond that which would generally be available from a wallet or consumer report.

Unusual use of account:

1. Account used in a manner that is not consistent with historical patterns of activity, including nonpayment or a material increase in the use of available credit.

2. Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the individual's covered account.

3. The Cooper Union is notified that the individual is not receiving paper account statements.

Notice from students, employees, applicants, law enforcement or other persons:

1. Student, employee, applicant or other person notifies The Cooper Union of unauthorized charges or account activity.

2. The Cooper Union is notified that it has opened or otherwise is maintaining a fraudulent account for a person engaged in identity theft.

III. Detection and Reporting/Escalation of Red Flags

Relevant departments and staff of The Cooper Union, including relevant staff within the Office of Financial Aid, the Office of Continuing Education, and the Business Office, will be provided with the above list of identity theft Red Flags and will be instructed to detect the Red Flags as part of their ordinary operations. Once detected, staff within the Office of Financial Aid will report Red Flags to the Director of Financial Aid, staff from the Office of Continuing Education will report Red Flags to the Director of Continuing Education and Public Programs, and staff from the Business Office will report Red Flags to the Controller. Each of the Director of Financial Aid, the Director of Continuing Education and Public Programs, and the Controller shall be considered the "Red Flag Office Administrator" of its respective Office. When the Director of Financial Aid, Director of Continuing Education and Public Programs, or Controller cannot rectify a Red Flag that has been detected by their respective offices, they will report the Red Flag to the Program Administrator, who will address them using reasonable measures under the circumstances to mitigate the risk of identity theft.

IV. Response to Red Flags

The personnel of The Cooper Union will investigate Red Flags that are detected and will respond appropriately. At all times when responding or investigating Red Flags, The Cooper Union will comply with the Family Educational Rights and Privacy Act ("FERPA"). In determining the proper response, The Cooper Union will take into consideration aggravating factors that may heighten the risk of identity theft. Aggravating factors include a data security incident that results in unauthorized access to a student's or employee's account records or notice that a student or employee has provided information related to a covered account to someone fraudulently claiming to represent the covered entity.

After a Red Flag is detected, The Cooper Union may take the following actions if deemed applicable and necessary:

- Determine no response is warranted;
- Contact the student or employee;
- Change passwords or other security devices permitting access to an account;
- Refuse to open a new account;
- Close an existing account;
- Notify the United States Department of Education's Office of Inspector General;
- Notify law enforcement; or
- Follow incident response procedures of the Program Administrator.

In particular, The Cooper Union will take the following steps in response to certain identified Red Flags:

Suspicious documents:

1. Documents provided for identification appear to have been altered or forged.

Staff will not accept the apparently altered or forged documents as forms of identification, and will input comments into the individual's account to alert other staff members of the potential identity theft. If the individual cannot produce original identification documents that do not appear to have been altered or forged, the Red Flag will be escalated to the Red Flag Office Administrator to be rectified in a safe and reasonable manner, including taking additional measures to authenticate the identity of the individual, geared toward mitigating the risk of identity theft.

2. The photograph or physical description on the identification is not consistent with the appearance of the individual presenting the identification.

Staff will not accept the documents as forms of identification, and will input comments into the individual's account to alert other staff members of the potential identity theft. If the individual cannot produce original identification documents that match the appearance of the individual, the Red Flag will be escalated to the Red Flag Office Administrator to be rectified in a safe and reasonable manner, including taking additional measures to authenticate the identity of the individual, geared toward mitigating the risk of identity theft.

3. Other information on the identification is not consistent with information provided by the individual opening a new covered account or individual presenting the identification.

Staff will not accept the documents as forms of identification, and will input comments into the individual's account to alert other staff members of the potential identity theft. If the individual cannot produce original identification documents that reflect consistent information, the Red Flag will be escalated to the Red Flag Office Administrator to be rectified in a safe and reasonable manner, including taking additional measures to authenticate the identity of the individual, geared toward mitigating the risk of identity theft.

4. Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check.

Staff will not accept the documents as forms of identification, and will input comments into the individual's account to alert other staff members of the potential identity theft. If the individual cannot produce original identification documents that contain consistent information, the Red Flag will be escalated to the Red Flag Office Administrator to be rectified in a safe and reasonable manner, including taking additional

measures to authenticate the identity of the individual, geared toward mitigating the risk of identity theft.

5. An application or other documentation appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Staff will not accept the apparently altered or forged documents, and will input comments into the individual's account to alert other staff members of the potential identity theft. If the individual cannot authenticate his or her identity and produce original documents that do not appear to have been altered or forged, the Red Flag will be escalated to the Red Flag Office Administrator to be rectified in a safe and reasonable manner, geared toward mitigating the risk of identity theft.

Suspicious personal information:

1. Personal identifying information provided is inconsistent when compared against external information sources used by the College (e.g., address does not match address in consumer report, SSN has not been issued or is listed in the SSA's Death Master File).

Staff will ask the individual to explain the inconsistent information. If a satisfactory explanation is not provided and reasonably verified by the staff, the Red Flag will be escalated to the Red Flag Office Administrator to be rectified in a safe and reasonable manner, geared toward mitigating the risk of identity theft. The College will not accept SSNs that it has knowledge have not been issued or are listed in the SSA's Death Master File. If the individual replaces the SSN with an alternative SSN that is one digit different from the SSN originally provided with the explanation that the original SSN was provided by a clerical error, the Red Flag Office Administrator or staff may consider accepting this explanation if reasonable under the circumstances.

2. Personal identifying information provided by the individual is not consistent with other personal identifying information provided by the individual (e.g., lack of correlation between SSN range and date of birth) or information that the College already has on file.

Staff will ask the individual to explain the inconsistent information. If a satisfactory explanation is not provided and reasonably verified by the staff, the Red Flag will be escalated to the Red Flag Office Administrator to be rectified in a safe and reasonable manner, geared toward mitigating the risk of identity theft.

3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College (e.g., address or phone number on application is same as that on a fraudulent application, address on application is fictitious, a mail drop or a prison, phone number is invalid or associated with a pager or answering service).

Staff will escalate the Red Flag to the Red Flag Office Administrator, who will investigate the situation and determine whether or not the individual has a history of fraud, and if so, recommend that the individual not be permitted to open an account, or alternatively that the individual's account be actively monitored for fraudulent activity. The fact that an individual's address is a mail drop, or that an individual's phone number is associated with a pager or answering service, alone, does not necessitate the conclusion that the individual is committing fraud, however it does warrant a reasonable investigation taking into consideration that fraudsters often use these types of contact points to open fraudulent accounts.

4. Personal identifying information (e.g., SSN, address, phone number) is the same as that submitted by other individuals or by an unusually large number of other persons opening accounts.

Staff will escalate the Red Flag to the Red Flag Office Administrator, who will investigate the situation and determine whether or not a fraudster has (or fraudsters have) been using the personal identifying information to open multiple accounts.

5. An applicant fails to provide all required personal identifying information on an application or in response to notifications that the application is incomplete.

If after requesting the applicant to complete all of the personal identifying information on the application, the applicant has failed to do so, the staff will not accept the application, and will input a comment in the applicant's file to alert other staff members of the possibility of identity theft.

6. When the College uses challenge questions to authenticate an individual, the individual cannot provide authenticating information beyond that which would generally be available from a wallet or consumer report.

   Staff will not consider the individual to be authenticated.

<u>Unusual use of account:</u>

1. Account used in a manner that is not consistent with historical patterns of activity, including nonpayment or a material increase in the use of available credit.

Staff will investigate whether identity theft may be the cause of the unusual activity, and will not take adverse action against the individual until a reasonable investigation has been made. If the accurate contact information for the individual is in question, staff will take measures to determine accurate contact information, taking into consideration that an identity thief may have changed the address on file without authorization. Staff will review any recent changes to contact information in the account, in particular changes that preceded the pattern of non-payment. Staff may attempt to contact the individual using prior contact information provided that staff does not disclose sensitive individual information without adequately authenticating the individual

first. In any event, staff will attempt to authenticate the identity of the individual and obtain up-to-date contact information. After due consideration of these possibilities, Staff may consider closing the covered account.

2. Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the individual's covered account.

Staff will attempt to contact the individual in another way, for example by telephone or, if the individual is a student, through the individual's resident advisor (if the individual lives in a dorm) and/or through the individual's parent's address (if such contact can be made in compliance with FERPA). If the accurate contact information for the individual is in question, staff will take measures to determine accurate contact information, taking into consideration that an identity thief may have changed the address on file without authorization. Staff will review any recent changes to contact information in the account, in particular changes that preceded the date that mail started to be returned. Staff may attempt to contact the individual using prior contact information provided that staff does not disclose sensitive individual information without adequately authenticating the individual first. In any event, staff will attempt to authenticate the identity of the individual and obtain up-to-date contact information. After due consideration of these possibilities, staff may consider closing the covered account.

3. The Cooper Union is notified that the individual is not receiving paper account statements.

Staff will attempt to contact the individual in another way, for example by telephone or, if the individual is a student, through the individual's resident advisor (if the individual lives in a dorm) and/or through the individual's parent's address (if such contact can be made in compliance with FERPA). If the accurate contact information for the individual is in question, staff will take measures to determine accurate contract information, taking into consideration that an identity thief may have changed the address on file without authorization. Staff will review any recent changes to contact information in the account, in particular changes that preceded the date that the College received notice that the individual is not receiving paper account statements. Staff may attempt to contact the individual using prior contact information provided that staff does not disclose sensitive individual information without adequately authenticating the individual first. In any event, staff will attempt to authenticate the identity of the individual and obtain up-to-date contact information. After due consideration of these possibilities, staff may consider closing the covered account.

<u>Notice from students, employees, applicants, law enforcement or other persons:</u>

1. Student, employee, applicant or other person notifies The Cooper Union of unauthorized charges or account activity.

Staff will investigate the authenticity of the complaint and investigate possible identity theft. Staff will flag the individual's account as having possibly been subjected to identity theft. The College will not take adverse action against the individual on account of such unauthorized charges or account activity without escalation to the Red Flag Office Administrator and the Red Flag Office Administrator's investigation and determination that the charges / activity were in fact authorized by the individual. If the complaint is valid, The Cooper Union will notify the individual to alert credit reporting agencies, the Department of Education and law enforcement.

2. The Cooper Union is notified that it has opened or otherwise is maintaining a fraudulent account for a person engaged in identity theft.

Staff will flag the individual's account as having possibly been subjected to identity theft and escalate the Red Flag to the Red Flag Office Administrator, who will investigate the situation and use reasonable efforts to verify whether the account is fraudulent. As appropriate, the Red Flag Office Administrator will report the Red Flag to the Program Administrator, who may report it to law enforcement. Staff will close the account if the account is fraudulent. Staff also will notify the affected individual to alert credit reporting agencies, the Department of Education and law enforcement.

V. Review and Updating of Program

The Cooper Union will periodically review and update the Program to reflect any changes in risks to students, employees, its experiences with identity theft, including data security breach incidents experienced by the College, the methods of detecting, preventing and mitigating identity theft, and changes in the safety and soundness of its data security measures. As part of the review of the Program, the Program Administrator will determine whether any additional accounts should be included in the Program as covered accounts, and whether any additional Red Flags should be added to the Program. As part of the review and updating process, the Program Administrator will request and receive reports from the Red Flag Office Administrators regarding the types of Red Flags that have been detected, whether and how they were rectified, which Red Flags tended to be most indicative of actual identity theft or attempted identity theft, and whether additional Red Flags should be added to the Program.

VI. Governance/Oversight

The Program Administrator will administer the Program. Upon initiation of the Program, the Program Administrator will obtain approval of the Board of Trustees, or a committee thereof. Thereafter, on an annual basis, the Program Administrator will report to the Board of Trustees, or a committee thereof, detailing the College's compliance with the Rules and Guidelines. The Program Administrator will report to the Board on material matters related to the Program, including significant incidents involving identity theft and management's response thereto.

VII. Staff Training

Relevant staff will be trained initially regarding the implementation of the Program, then training will continue on a periodic basis and/or whenever the Program is updated.

VIII. Oversight of Service Providers

If The Cooper Union engages a service provider to perform an activity in connection with one or more covered accounts, The Cooper Union will take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

As an example, the College may contractually require the service provider to have policies and procedures to detect and respond appropriately to Red Flags, report them to the College and/or take steps to prevent or mitigate the risk of identity theft.

The following procedures will be followed to oversee service provider relationships:

- Upon the initiation of the Program, the Program Administrator will identify applicable service providers used by the College and contact them to ensure that they have adequate policies and procedures in place to detect, prevent and mitigate the risk of identity theft.

- Key individuals at the College who would be involved in putting into place new service provider relationships that relate to covered accounts will be trained to inform the Program Administrator reasonably in advance of putting such relationships into place so that the Program Administrator can ensure that the service provider has adequate policies and procedures in place to detect, prevent and mitigate the risk of identity theft.

- Each time the Program is updated (or at least annually), the Program Administrator will identify and contact new service providers who were not in place when the Program was initiated or last updated, and for whom this process has not occurred to date, to ensure that they have adequate policies and procedures in place to detect, prevent and mitigate the risk of identity theft.

- Periodically, the Program Administrator will contact all service providers that relate to covered accounts to verify that the service provider continues to have in place and follow adequate policies and procedures to detect, prevent and mitigate the risk of identity theft.