



Connecticut State University System

39 Woodland Street ■ Hartford, CT 06105-2337 ■ 860-493-0000 ■ www.ctstateu.edu

BR# 09-36

RESOLUTION

concerning

IDENTITY THEFT PREVENTION PROGRAM

for the

CONNECTICUT STATE UNIVERSITY SYSTEM

April 8, 2009

WHEREAS, Part 681 of Title 16 of the Code of Federal Regulations (the “Red Flags Rule”) implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended the Fair Credit Reporting Act (FCRA); and

WHEREAS, The Red Flags Rule requires “financial institutions” and “creditors” that hold “covered accounts” to develop and implement an identity theft prevention program for new and existing accounts by May 1, 2009; and

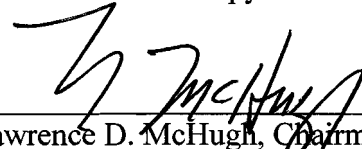
WHEREAS, The Board of Trustees recognizes that some activities conducted by the System and its universities are subject to FACTA and the Red Flags Rule; and

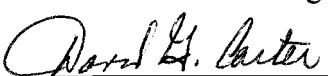
WHEREAS, The Board of Trustees has considered the extent, nature and complexity of the operations and account systems of CSUS and its universities and has determined that the attached Identity Theft Prevention Program is appropriate for the System; therefore be it

RESOLVED, That the attached Identity Theft Prevention Program be adopted immediately and become fully implemented by May 1, 2009; and be it further

RESOLVED, That the Chancellor is authorized to make such changes to the Program as deemed necessary.

A Certified True Copy:


Lawrence D. McHugh, Chairman


David G. Carter, Chancellor

CONNECTICUT STATE UNIVERSITY SYSTEM IDENTITY THEFT PREVENTION PROGRAM

I. AUTHORITY

The Connecticut State University System (“CSUS”) has developed this Identity Theft Prevention Program (“Program”) in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, which amended the Fair Credit Reporting Act (FCRA). These regulations have been named the “Red Flags Rules.”

II. PURPOSE

This Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account and to provide for continued administration of the Program. The purpose of the Program is to enable CSUS and its universities to:

- (i) Identify relevant Red Flags for Covered Accounts offered or maintained by CSUS and incorporate those Red Flags into the program;
- (ii) Detect relevant Red Flags; and
- (iii) Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.

III. DEFINITIONS

Identity Theft means fraud committed or attempted using the identifying information of another person without authority.

Identity 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, Social Security Number, Date of Birth, State or Federal issued drivers license or identification number, Alien registration number, Government passport number, Employer of taxpayer identification number, fingerprints, voice prints, retina or iris image, social security number and date of birth.

A Red Flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Credit means the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefor.

A Covered Account is an account used mostly for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts include credit card accounts, cell phone accounts, checking accounts and savings accounts. A covered

account is also any other account for which there is a reasonably foreseeable risk to customers or to the safety and soundness of CSUS from identity theft, including financial, operational, compliance, reputational or litigation risks, such as student loans.

A **Customer** is any person who has a covered account with a creditor.

A **Creditor** is any entity that regularly extends, renews, or continues credit, any entity that regularly arranges for the extension, renewal or the continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew or continue credit. Activities that cause CSUS to be classified as a creditor under the Red Flags Rule include, but are not limited to, the following:

- (i) Participating in the Federal Perkins Loan program;
- (ii) Participating as a direct lender in the federal Stafford Loan program;
- (iii) Participating as a school lender in the Federal Family Education Loan Program;
- (iv) Offering institutional loans to students, faculty, or staff;
- (v) Offering a plan for payment of tuition throughout the semester rather than requiring full payment at the beginning of the semester; and/or
- (vi) Offering a deferral of tuition payment pending the award of financial aid.

A **Program Administrator** is a person appointed to administer and oversee the Identity Theft Prevention Program. There shall be a Program Administrator for the system and for each CSUS university.

IV. RELEVANT RED FLAGS

In order to identify relevant Red Flags, CSUS has considered the types of accounts that it offers and maintains, the methods it utilizes to establish those accounts, the procedures it utilizes to access those accounts, and its experiences with Identity Theft. CSUS has identified the following relevant Red Flags in each of the listed categories:

- A. Suspicious Documents:
 - (i) Identification document or card that appears to be altered or forged;
 - (ii) Identification document or card on which the applicant's photograph does not match the person presenting the document;
 - (iii) Other supporting documents containing information that is inconsistent with the history or profile of the applicant;

- (iv) Other information provided that is not consistent with readily accessible information that is on file, such as a recently provided check;
- (v) Application that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled; and/or
- (vi) Repeated email requests that password and /or username does not match.

B. Suspicious Personal Identifying Information:

- (i) Identification information presented that is inconsistent with other information the applicant provides (e.g. inconsistent birth dates);
- (ii) Identification information presented that is inconsistent with other sources of information (an address not matching an address on a loan application);
- (iii) Identification information presented that is similar to information shown on other fraudulent applications;
- (iv) Identification information presented that is not consistent with the information on file with the university;
- (v) Address, phone number or social security number that is the same as one given by another applicant;
- (vi) Identifying information provided that is of a type commonly associated with fraudulent activity (such as an invalid phone number or fictitious address);
- (vii) Repeated appearance of incomplete or incorrect information on individual's applications; and/or
- (viii) Failure to provide complete identifying information on an application despite being reminded to do so.

C. Suspicious Covered Account Activity or Unusual Use of Account:

- (i) 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;
- (ii) Mail sent to the student that is repeatedly returned as undeliverable;
- (iii) The University receives notice that a Customer is not receiving mail sent by the University;

- (iv) The University receives notice that an account has unauthorized activity;
- (v) Breach in the university's computer system security;
- (vi) Unusual activity related to login accounts or other access methods, such as repeated password resets or account lockout;
- (vii) Unauthorized access to or use of student account information;
- (viii) Request for multiple changes to student profile;
- (ix) Payments stop on an otherwise consistently up-to-date account; and/or
- (x) The account is used in a manner not consistent with prior use (e.g., very high activity).

D. Alerts, notifications and other warnings from Outside Law Enforcement, Customers or Victims of Identity Theft:

Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identify theft in connection with Covered Accounts.

E. Alerts from Credit Reporting Agencies:

Alerts, notification or other warnings received from consumer reporting agencies or service providers, such as fraud detection services. Such alerts may include:

- (i) A fraud or active duty alert is included with a consumer report
- (ii) A consumer report agency provides a notice of credit freeze in response to a request for a consumer report;
- (iii) A consumer reporting agency provides a notice of address discrepancy; and/or
- (iv) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of a Customer.

V. DETECTING RED FLAGS

In order to detect the existence of Red Flags in connection with the opening of new accounts or activity in existing accounts, University personnel will take the following steps:

- A. New Accounts:
- (i) Require certain identifying information, such as name, date of birth, and address; and
 - (ii) Verify the identity of the Customer:
 - (a) through documents, by requiring a government-issued identification card (such as a driver's license or passport); or
 - (b) through non-documentary methods, such as independently contacting the Customer or verifying identity by comparing information provided with information obtained from a consumer reporting agency or other source.,
- B. Existing Accounts:
- (i) Verify the identification of customers requesting information;
 - (ii) Verify changes in banking information given for billing and payment purposes; and
 - (iii) Verify the validity of change of address requests.

VI. PREVENTING AND MITIGATING IDENTITY THEFT

If a Red Flag is detected, the appropriate responses to the Red Flag are as follows:

- (i) Notify the university Program Administrator immediately upon detection of a Red Flag or of any failure to comply with this program;
- (ii) Continue to monitor a Covered Accounts for evidence of Identity Theft;
- (iii) Deny access to the Covered Account until other information is available to eliminate the Red Flag;
- (iv) Contact the student/account holder;
- (v) Provide the student with a new student identification number;
- (vi) Change any passwords, security codes or other security devices that permit access to a Covered Account;
- (vii) Reopen a Covered Account with a new account number;
- (viii) Refuse to open a new Covered Account;

- (ix) Close a Covered Account;
- (x) Notify law enforcement; or
- (xi) Determine no response is warranted under the particular circumstances.

In addition, the System and its universities shall take the following steps to protect student identification information:

- (i) Avoid use of Social Security numbers for students;
- (ii) Require and keep only student information that is absolutely necessary for System or university purposes;
- (iii) Require that access to systems containing or related to covered accounts is protected using a unique login ID and password, and that passwords conform to guidelines for minimum length, composition, and change frequency;
- (iv) Keep computer virus protections up to date;
- (v) Secure their websites, or provide clear notice that their websites are not secure; and
- (vi) Securely destroy paper and computer files containing Covered Account information when these are no longer needed.

VII. ADMINISTRATION OF THE PROGRAM

A. Oversight of the Program:

The Chancellor shall appoint a Systemwide Program Administrator with accountability for developing, implementing and updating this program, as well as administration and oversight of this program at the System Office, including training of appropriate System Office personnel and review of any reports regarding the detection of Red Flags. Each university President shall appoint a university Program Administrator responsible for proper administration and oversight of the program at their university, including training of applicable personnel and review of any reports regarding the detection of Red Flags.

B. Updating the Program:

This Program will be reviewed and updated annually to reflect changes in risks and to verify that the program contains the most up-to-date practices and procedures needed to protect the System and its universities from Identity Theft. By July 31st of each year, the university Program Administrators will consider the universities' experiences with identity theft, changes in identity theft methods, changes in identity theft detection and

prevention methods, changes in types of covered accounts the university maintains, and changes in university business arrangements with other entities. After considering these factors, the university Program Administrators will determine whether changes to the Program, including the listing of Red Flags, are warranted. By August 31st of each year, the university Program Administrators will forward any proposed changes to the Systemwide Program Administrator, who will coordinate the update of the program.

VIII. STAFF TRAINING AND REPORTING

A. CSUS staff responsible for Program implementation shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags and the responsive steps to implement the program.

B. CSUS employees shall notify the Program Administrator once they become aware of an incident of Identity Theft or of any failure to comply with this Program.

C. At least annually or as otherwise requested by the Systemwide Program Administrator, the university Program Administrators shall report to the Systemwide Program Administrator on compliance with this Program. The report shall address such issues as effectiveness of the policies and procedures in addressing the risks of Identity Theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving Identity Theft and management's response thereto, and recommendations for changes to the Program.

IX. OUTSIDE SERVICE PROVIDERS

In the event the System or a System university engages a service provider to perform an activity in connection with one or more Covered Accounts, the System or university shall require, by contract, that the service provider:

- (i) Have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider's activities;
- (ii) Provide a copy of such policies and procedures to the System and/or university Program Administrator, as appropriate; and
- (iii) Report Red Flags to the System and/or university Program Administrator.