29429
ADOPTED - BOARD OF TRUSTEES
COMMUNITY COLLEGE DISTRICT NO. 508
MAY 7, 2009

BOARD OF TRUSTEES OF COMMUNITY COLLEGE DISTRICT NO.508
County of Cook and State of Illinois

RESOLUTION

DATA SECURITY AND IDENTITY THEFT PREVENTION PROGRAM
INTERNAL AUDIT
DISTRICT OFFICE

WHEREAS, CCC is required to comply with the Federal Trade Commission (FTC) Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003, which provides protection of personal identifiable information from possible identity theft for "covered accounts," which includes students, employees and vendors; and

WHEREAS, the compliance requirements include board of directors approval of a written Identity Theft Prevention Program that helps to protect CCC from non-compliance penalties including:

- Civil money penalty for each violation
- Cease and desist Order
- Lowering of examination rating
- Consumer lawsuit
- Negative publicity, loss of business

NOW, THEREFORE, BE IT RESOLVED that the Board of Trustees approve the "Data Security and Identity Theft Prevention Program."

May 7, 2009

Data Security and Identity Theft Prevention Program
Policy and Procedure

PREFACE

City Colleges of Chicago (CCC) developed this Identity Theft Prevention program pursuant to the Federal Trade Commission (FTC) Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003. This Program was developed in considering the size and complexity of CCC's operations and account systems, and the nature and scope of CCC's handling of personal identifiable information (PII).

DEFINITIONS

"Identity Theft" is a "fraud committed or attempted by using identity information of another person or vendor without permission."

A "Red Flag" is a "pattern, practice or specific activity that indicates the possible existence of identify theft."

A "Covered Account" includes all student, employee and vendor information maintained by CCC.

"Identifying information" is any PII that may be used, alone or in conjunction with any other information, to identify a specific person or vendor. Specific examples included:

- Name
- Address
- Social Security Number
- Date of Birth
- Driver's License
- Alien Registration Number
- Passport Number
- Federal Employer or Tax Identification Number (FEIN or TIN)
- Identification Number (Student, Employee, Vendor)
- Credit Card Number
- Bank Account Data
- Email Address(es)
- Phone Number(s)
- Benefits Enrollment, Dependents and Beneficiaries

PROGRAM

CCC has established this Identity Theft Prevention Program to detect, prevent and mitigate identify theft. The Program includes reasonable policies and procedures to:

- Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program
- Detect the red flags that have been incorporated into the Program
- Respond appropriately to any red flags that are detected to prevent and mitigate identify theft; and
- Update the program periodically to reflect changes in risks to covered accounts

IDENTIFICATION OF RED FLAGS

The Program addresses the detection of red flags in connection with the opening of covered accounts and existing covered accounts. Provided below are examples of red flags in each of the exiting categories:

Suspicious Documents

- that appear to be forged, altered or unauthentic
- that are of a person's photograph or physical description and inconsistent with the person presenting the document

- that are not consistent with existing student, employee or vendor information

Suspicious Personal Identifying Information

- that is inconsistent with other information the student, employee or vendor provides (e.g. date of birth, social security number, Federal Employer Identification Number (FEIN)) or other authentic information/documentation sources
- that is consistent with other fraudulent documentation or activity
- that is a duplicated social security number for more than one individual or FEIN/TIN of more than one named company
- that is a duplicate address or phone number for more than one unrelated individuals or companies
- that is a deliberate omission by an individual or company when requested to do so
- that is identifying information that is inconsistent with documentation maintained in CCC files

Suspicious Covered Account Activity or Unusual Use of Account

- that changes the address for an account followed by a request to change the student, employee or vendors name
- that show payments have stopped on an otherwise consistently up-to-date account
- that indicates an account was used in a way that is not consistent with prior use
- that reveals mail sent to a student, employee or vendor address and repeatedly returned as undeliverable
- that is a notice to CCC that a student, employee or vendor is not receiving mail sent from within CCC
- that is a notice to CCC that an account has unauthorized activity
- that is a breach in CCC's computer system, and
- that is unauthorized access to or use of student, employee or account information

PREVENTING AND MITIGATING IDENTITY THEFT

In the event that a Red Flag is identified, CCC personnel shall do one or more of the following:

- Continue to monitor a covered account for evidence of identity theft
- Change any passwords or other security devices that permit access to covered accounts
- Not open a new covered account
- Provide the student, employee or vendor with a new identification number
- Notify the Program Administrator or "Data Security and Identity Theft Prevention Committee" for determination of the appropriate steps to take
- Notify law enforcement

To prevent the likelihood of identify theft occurring, CCC will take the following steps relating to internal controls to protect student, employee and vendor PII:

- Ensure that its website is secure or provide clear notice that the website is not secure
- Facilitate complete and secure destruction of paper documents and electronic files containing PII information in accordance with a records retention policy or when a decision has been made to no longer maintain such information
- Secure computers with passwords and limit access to electronic data as well as paper documentation of covered account information
- Avoid the use of social security number or mask first 5 numbers
- Update computer virus protection
- Limit the retention of PII to meet CCC purposes

Data Security and Identify Theft Prevention Program
Policy and Procedure

PROGRAM OVERSIGHT

The Data Security and Identity Theft Prevention committee is responsible for implementing and updating the Program. The committee shall consist of, at a minimum, representatives from Risk Management, General Counsel, Human Resources, Information Technology, Student Administration and/or Finance, Internal Audit, and the Inspector General. The committee shall be responsible for the following:

- Developing training for CCC personnel who have access to PII
- Hearing, auditing, investigating and monitoring final disposition of suspected data security breaches and identity theft
- Continuing to monitor a covered account for evidence of identity theft

CCC management (College Presidents and Vice Chancellors) will be responsible the following:

- Identifying CCC personnel who specifically handles PII
- Providing training to those identified personnel
- Documenting and reporting training to the Data Security and Identity Theft Prevention Committee
- At least annually CCC management should affirm in writing and supporting documentation of training provided

Service Provider Arrangements

In the event CCC engages a service provider to perform an activity in connection with any covered account, the following steps will be implemented to help prevent data breaches and identity theft of CCC's covered accounts:

- Require by contract that service providers have similar policies and procedures in place; and
- Require by contract that service providers review CCC's Data Security and Identify Theft Prevention Program
- Require by contract that service providers report any red flags, data breaches or identity theft of a CCC covered account

PROCEDURE SCOPE

Consistent information protection must exist throughout the life cycle of the information. This protection must be commensurate with the sensitivity of the information, regardless of where it resides, the form it takes, or the technology used to handle it. This procedure provides overall guidance for the consistent protection of all CCC's information, and applies to all users of CCC's information.

HANDLING OF PPI PROCEDURE

Physical Security of PII

- PII must not be left unattended on desks
- Paper and removable computer media containing PII must be stored in lockable storage, when not in use
- When documents with CCC's covered account PII are received via fax or mail, it must be immediately removed from the machines and or secured in a locked drawer or file cabinet.
- No CCC documentation containing PII is to be provided over the phone or faxed. To the degree possible, these documents should be provided only to the student on CCC property after identification is verified.

Distribution of PII

Internal

To the degree possible, all PII should be only accessed through a secure network and not printed, carried or forwarded through interoffice mail. Under no circumstance should PII be emailed. Should documents containing PII need to be printed and forwarded to other campuses,

it must be properly sealed in an envelop, marked as confidential delivered by campus or district office security or courier, and only delivered to the person or their designee in that requesting department.

External

No PII should be sent via email outside of CCC. Should PII need to be sent via U.S. mail, the addressee should be verifiable. Additionally, should PII need to be sent outside of CCC, one of the following manners, or manner such that the same levels of security are applied to maintain the confidentiality, availability, and integrity:

- By use of a bonded courier in a sealed and correctly labeled container placed inside a transit container bearing only the intended recipient and address.
- By common carrier, with complete tracking ability, in a sealed and/or lockable container, with the appropriate markings, and then placed in an unmarked and sealed transit container.
- By U.S. mail services sent "Certified" or "Return Receipt Requested." The information must be sent in a properly marked envelope or container placed inside an unmarked transit envelope or container bearing only the recipient and address.
- All packages must have an additional marking on the inside envelope or container stating, "To Be Opened by Addressee Only!"

All PII sent over the Internet and/or the CCC's Intranet with must use one of the following transport methods:

- SSL
- SSH
- SFTP
- HTTPS
- VPN