LOS ANGELES COMMUNITY COLLEGES OFFICE OF THE CHANCELLOR ADMINISTRATIVE REGULATIONS	INDEX NUMBER E-114_
REFERENCE: **16 C.F.R. § 681.2**	**TOPIC: Identity Theft Prevention Program**
ISSUE DATE: June 23, 2009	**INITIATED BY:** Office of General Counsel
CHANGES: New Regulation	**DATES OF CHANGES:**

A. BACKGROUND

The Red Flags rules, issued by the Federal Trade Commission, are implementing regulations of the Federal Fair and Accurate Credit Transactions Act ("FACTA"). The Red Flags rules require that "financial institutions" or "creditors" holding "covered accounts" develop and implement identity theft prevention programs for new and existing accounts.

While the colleges are not "financial institutions," the colleges may, within in limited situations, be considered "creditors" offering "covered accounts" and consequently fall within the scope of the Red Flags rules. The purpose of this regulation is to detect Red Flags, and to prevent and mitigate identity theft.

B. DEFINITIONS

1. A **"creditor"** includes any person or entity that regularly extends, renews, or continues credit.

2. A **"covered account"** is an account which a creditor offers or maintains, for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. Within the District, these include: (a) student accounts under the Federal Perkins Loan program, and (b) student profiles in DEC (or its successor) when the colleges opt to provide institutional loans, or offer plans for the payment of tuition throughout the semester rather than requiring full payment at the beginning.

3. **"Personal identifying information"** includes, but is not limited to, name, address, date of birth, phone number, student ID number, Social Security number ("SSN").

4. A **"Red Flag"** is a pattern, practice, or specific activity that indicates the possible existence of identity theft, including but not limited to the following:

    a. **Alerts, notifications, or warnings from consumer reporting agencies**, such as fraud alerts, credit freezes, notices of address discrepancies, or consumer reports which indicate a pattern of activity that is inconsistent with the history and usual pattern of an applicant or customer.

    b. **Suspicious documents**, including but not limited to, documents which:

i. appear to have been altered or forged, or destroyed and reassembled;
ii. include photographs or physical descriptions which are not consistent with the appearance of the individual presenting the document;
iii. include other information which is not consistent with information provided by the student; or
iv. include other information which is not consistent with readily accessible information that is on file with the college.

c. **Suspicious personal identifying information**, including but not limited to, information which:

i. is inconsistent when compared against information provided by the student or against external information sources used by the college;
ii. is associated with known fraudulent activity as indicated by the college's records or by external information sources used by the college (e.g., the address and/or phone number provided is the same as those provided on a fraudulent application);
iii. is of a type commonly associated with fraudulent activity (e.g., the address on the application is fictitious, a mail drop, or a prison; or the phone number is invalid or is associated with a pager or answering service);
iv. is the same or similar to that provided by other persons (e.g., the SSN, address, phone number provided is identical to those provided by other persons);
v. is incomplete (e.g., the individual fails to provide all requested personally identifiable information on an application, or in response to a notification that the application is incomplete); or
vi. is inconsistent with information on file with the college.

d. **Unusual use or suspicious activity**, including but not limited to the following:

i. material changes in payment or use patterns not consistent with the established patterns on the account (e.g., nonpayment when there is no history of late or missed payments);
ii. mail sent to the student is returned repeatedly as undeliverable;
iii. notification to the college that the student is not receiving paper account statements; or
iv. notification to the college of unauthorized charges or transactions.

e. **Notice from students, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with a covered account**.

5. A "**service provider**" means a person or entity that provides a service directly to the college.

C. DETECTION OF RED FLAGS

Red Flags may be detected in the following circumstances:

1. **New covered accounts**

   a. With respect to new applications for admission, the colleges shall collect all required personally identifiable information. However, submission of picture identification is not required with the initial admissions application. (Administrative Regulation E-108.)

   b. With respect to applications for financial aid (e.g., Perkins Loans), the colleges shall collect all required personal identifying information, and take appropriate measures to verify the applicant's identity, such as examining presented government issued photo identification.

2. **Existing covered accounts**

   a. The colleges shall take appropriate measures to verify the identity of students seeking to make changes to components of their personal identifying information with respect to covered accounts. Picture identification is required for all in-person transactions that would otherwise require a personal identification number (PIN) if conducted online.

   b. The colleges shall take appropriate measures to safeguard the confidentiality of records containing personal identifying information, including ensuring the physical security of records and limiting access to such records to only those employees who have a legitimate business related reason. (Board Rule 8404.)

D. RESPONSES TO RED FLAGS

1. Once a Red Flag is detected, the college shall investigate the matter further and take appropriate steps to mitigate identity theft. Appropriate responses may include the following:

   a. cancelling or voiding the attempted transaction;
   b. notifying the affected student(s) or individual(s);
   c. notifying and communicating with other college departments;
   d. assisting in the changing of passwords, PIN's or other security devices which permit access to a covered account;
   e. consolidating two or more covered accounts;
   f. suspending collection on the covered account;
   g. monitoring the covered account for indications of identity theft;

h. closing the covered account;
i. notifying appropriate law enforcement authorities;
j. referring the student for disciplinary action by the Office of Student Services; or
k. determining that no further action is warranted under the particular circumstances.

2. In the event that an unauthorized breach of personal identifying information occurs, the college shall make efforts to inform, as soon as practicably possible, the affected students or individuals, by sending them written notice that a breach has occurred. The notice may advise students about initiating credit freezes with the three major credit reporting bureaus, Equifax, Experian, and TransUnion.

E. SERVICE PROVIDERS

1. The colleges shall ensure that service providers who provide services in connection with covered accounts have appropriate identity theft prevention policies in place.

2. Contracts and written agreements with third party service providers, by way of appropriate contractual provisions, shall require that such service providers have reasonable identity theft prevention policies to detect Red Flags in connection with the service providers' activities and that mechanisms exist to allow for the updating of such policies.

F. ADMINISTRATION, REPORTS AND UPDATES TO THE IDENTITY THEFT PREVENTION PROGRAM

1. The District shall designate a Program Administrator for the oversight of the Identity Theft Prevention Program.

2. District committees involved with the implementation of the Identity Theft Prevention Program should, on at least an annual basis, provide reports to the Program Administrator regarding the effectiveness of Red Flag policies and procedures, service provider arrangements, significant incidents involving identity theft, and any recommendations for changes to the Program.

3. Training may be provided as appropriate to apprise District employees of their obligations under this Program.