SAN DIEGO COMMUNITY COLLEGE DISTRICT

Administrative Procedure

Chapter 5 – Student Services

AP 5800 – PREVENTION OF IDENTITY THEFT IN STUDENT FINANCIAL TRANSACTIONS

The purpose of the Identity Theft Prevention Program (ITPP) is to provide information that will assist individuals in detecting, preventing, and mitigating identity theft in connection with the opening of a "covered account" or any existing "covered account," or who believe that a security incident has occurred, and to provide information for the reporting of a security incident.

1. DEFINITIONS

   a. "Identity theft" is a fraud attempted or committed using identifying information of another person without authority.

   b. A "creditor" includes government entities who defer payment for goods (e.g. enrollment fees, payment plans for enrollment fees, financial aid, parking tickets, bookstore accounts, etc.).

   c. "Deferring payments" refers to postponing payments to a future date and/or installment payments on fines or costs.

   d. A "covered account" includes any new or existing account offered for personal, family or household purposes that includes or is designated to permit multiple payments or transactions (e.g. enrollment fees, payment plans for enrollment fees, financial aid, parking tickets, bookstore accounts, etc.).

   e. "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft. Detection or discovery of a "Red Flag" implicates the need to take action under the ITPP to help prevent, detect and correct identity theft.

   f. "Person" means any individual who is receiving goods, receives a loan, and/or is issued a debit card from the District and is making payments on a deferred basis for said goods, loan, and/or debit card.

   g. "Sensitive 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, name, social security number, ethnicity, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, bank account number, bank routing number, credit card number, credit card expiration date, security code, card holder name or address, pay rate, direct deposit information, or student identification number.

2. DETECTING “RED FLAGS” FOR POTENTIAL IDENTITY THEFT

a. Risk Factors for Identifying “Red Flags”

1) The District will consider the following factors in identifying relevant “Red Flags”:

a) The types of covered accounts the District offers or maintains;
b) The methods the District provides to open the District’s covered accounts;
c) The methods the District provides to access the District’s covered accounts; and
d) The District’s previous experience(s) with identity theft.

b. Sources of “Red Flags”

1) The District will continue to incorporate relevant “Red Flags” into the ITPP from the following sources:

a) Incidents of identity theft that the District has experienced;
b) Methods of identity theft that the District identifies that reflect changes in identity theft risks; and
c) Guidance from the District’s employees who identify changes in identity theft risks.

c. Identification of “Red Flags”

The following “Red Flags” have been identified for the District’s covered accounts.

1) Alerts, notifications, or warnings from a consumer reporting agency.

2) Suspicious or possibly forged documents:

a) Documents provided for identification appear to have been forged or altered.
b) The photography or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
c) Other information on the identification is not consistent with the information provided by the person opening a new covered account or customer presenting the identification.
d) Other information on the identification is not consistent with readily accessible information that is on file with the District, such as a signature card or a recent check.
e) An application for admissions that appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled.

d. Suspicious Personally Identifying Information

1) Personally identifying information provided is inconsistent when compared against external information sources used by the District. (i.e. mismatched SSN or Date of Birth).

2) Personal identifying information provided by a person is not consistent with other personal identifying information provided by a person.

3) Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources used by the District.

4) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the District.

5) During the normal course of business, it is noticed that personal identifying information provided is not consistent with personal identifying information that is on file with the District.

e. Unusual Use Of, Or Suspicious Activity Relating To A Covered Account

1) A new covered account is used in a manner that is commonly associated with known patterns or fraud patterns (e.g. a person makes a first payment, but there are no subsequent payments made).

2) A covered account is used in a manner that is not consistent with established patterns of activity on the account.

3) Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person's covered account.

4) The District is notified that the person is not receiving paper account statements.

5) The District is notified of unauthorized transactions in connection with a person's covered account.

6) The District becomes aware of an electronic data security breach relating to a specific covered account.

f. Notices from students/persons, victims of identity theft, law enforcement authorities, or other business about possible identify theft in connection with covered accounts:

1) The District is notified by a person with a covered account, a victim of identity theft, a law enforcement authority, or any other person, that it has opened a fraudulent account for a person engaged in identity theft.

3. PREVENTING AND MITIGATING IDENTITY THEFT

One or more of the following measures, as deemed appropriate under the particular circumstances, shall be implemented to respond to "Red Flags" that are detected:

a. Monitor the covered account for evidence of identity theft;

b. Contact the person who holds the covered account;

c. Change any passwords, security codes, or other security devices that permit access to a covered account;

d. Do not open a new covered account;

e. Close an existing covered account;

f. Do not attempt to collect on a covered account or not sell a covered account to a debt collector;

g. Notify law enforcement;

h. Where a consumer reporting agency provides an address for a consumer that substantially differs from the address that the consumer provided, the District shall take the necessary steps to form a reasonable belief that the District knows the identity of the person for whom the District obtained a credit report;

i. Determine that no response is warranted under the particular circumstances;

j. Withhold requested information

4. SERVICE PROVIDERS OVERSIGHT

The District remains responsible for compliance with the Red Flag Rules even in instances where services are outsourced to a third party. The written agreement between the District and the third party service provider shall require the third party to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service activities. The written agreement must also indicate whether the service provider is responsible for notifying the District of the detection of a Red Flag or if the service provider is responsible for implementing appropriate steps to prevent or mitigate identity theft.

5. PROGRAM OVERSIGHT

Oversight of the ITPP by the Chancellor or designee shall include:

a. Assigning specific responsibility for the ITPP's implementation;

b. Reviewing reports prepared by the staff regarding compliance with the ITPP; and

c. Reviewing and updating the ITPP if needed on an annual basis.

References: 15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act - FACT ACT or FACTA)

Approved by
the Chancellor: November 28, 2016

Supersedes: New Procedure