AP 5800 Prevention of Identity Theft in Student Financial Transactions

Reference:
Fair and Accurate Credit Transactions Act, (Pub. L. 108-159)

Note: This procedure is legally required.

5800.1 These procedures shall be administered by the Chief Student Services Officer (CSSO) or designee responsible for student financial transactions

5800.2 Definitions

"Identity Theft Prevention Program" (ITPP) is a program designed to prevent identity theft in student financial transactions.

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

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

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

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 (for example financial aid programs, enrollment fees, bookstore accounts, payment plans for enrollment fees, parking tickets, etc.).

"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 this ITPP to help prevent, detect and correct identity theft.

"Person" means any individual who is receiving goods and/or services from the District and is making payments on a deferred basis for said goods and/or services or receiving financial aid payments.

"Sensitive Information" means any name or number that may be used alone, or in conjunctions 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, card holder name or address, pay rate, direct deposit information, or student identification number.

5800.3 Purpose – The purpose of the Identity Theft Prevention Program (ITPP) is to control reasonable foreseeable risks to students from identity theft in student financial transactions, by providing for the identification, detection, and response to patterns, practices or specific activities ("Red Flags") that could indicate identity theft. In so

doing, the District is complying with the regulatory requirements of the Federal Trade Commission, which issued regulations known as the "Red Flag Rules" under the Fair and Accurate Credit Transactions (FACT) Act, Sections 114 and 315 (16 CFR Part 681), amending the Fair Credit Reporting Act with the intent to reduce the risk of identity theft.

5800.4 Securing Sensitive Student Information – These procedures apply to all District students, faculty, staff and others granted use of District materials and systems. Sensitive information elements shall never be used as a "key" to a system.

5800.5 Hard Copy Distribution – Each employee and contractor performing work for the District shall comply with the following procedures:

A. File cabinets, desk drawers, overhead cabinets, and any other storage unit containing documents with sensitive information will be locked when left unsupervised.

B. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.

C. Desks, workstations, work areas, printers, credit card machines, fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use and when left unsupervised.

D. Whiteboards, blackboards, dry-erase boards, writing tablets, etc in common shared work areas will be erased, removed, or shredded when not in use.

E. When documents containing sensitive information are discarded, they will be placed inside a locked shred bin or immediately shredded using a District shredding device.

F. Sensitive information is never to be removed from the work area without the approval of the supervisor.

G. Sensitive information being scanned into the District's document imaging data storage system or any electronic information storage system must be immediately returned to a secure location or shredded once scanning is complete. See Board Policy 535 and AP 535.

H. Documents containing sensitive information must be picked up immediately if being printed to a common area printer.

5800.6 Electronic Distribution – Each employee and contractor performing work for the District will comply with the following policies:

A. Internally, sensitive information may be transmitted using approved District e-mail. All sensitive information must be encrypted when stored in an electronic format.

B. Sensitive information sent externally must be encrypted and password protected and only to approved recipients.

5800.7 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 provide 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 this 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. Categories of "Red Flags"

1. The following "Red Flags" have been identified for the District's covered accounts.

a. Alerts, notifications, or warnings from a Consumer Reporting Agency:

1) A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student or other person substantially differs from the one the credit reporting agency has on file. (See Section 5800.9.A.9 for specific steps that must be taken to address this situation.)

2) A consumer reporting agency provides notice of a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant, such as:

a) A recent and significant increase in the volume of inquiries;

b) An unusual number of recently established credit relationships;

c) A material change in the use of credit, especially with respect to recently established credit relationships; or

d) An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution.

b. Suspicious Documents:

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

2) The photography or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

3) 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.

4) 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.

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

c. Suspicious Personally Identifying Information

1) Personal identifying information provided is inconsistent when compared against external information sources used by the District. For example:

a) The address does not match any address in the consumer report; or

b) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

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. For example:

a) The address of an application is the same as the address provided on a fraudulent application;

b) The phone number on an application is the same as the phone number provided on a fraudulent application.

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. For example:

a) The address on an application is fictitious, a mail drop, or a prison; or

b) The phone number is invalid, or is associated with a pager or answering service.

5) The SSN provided is the same as that submitted by other persons currently being served by the District.

6) During the normal course of business, it is noticed that the address or telephone number provided is the same or similar to the address or telephone number submitted by an unusually larger number of other persons being served by the District.

7) The person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

8) 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.

9) The person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

d. 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. (For example, 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. For example, there is:

a) Nonpayment when there is no history of late or missed payments; or

b) A material change in electronic fund transfer patterns in connection with a payment.

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.

e. Notices from customers/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.

5800.8 Measures to Detect "Red Flags"

A. The District shall do the following to aid in the detection of "Red Flags":

1. When deemed necessary, the District shall obtain identifying information about, and information verifying the identity of, the student or other person seeking to open a covered account. Two forms of identification shall be obtained, at least one of which must be photo identification. The following are examples of the types of valid identification that a person my provide to verify the identity of the person seeking to open the covered account: valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security card, current resident lease, or copy of a deed to the person's home or in voice/statement for property taxes.

2. Persons with covered accounts may make changes to personal information online by accessing their personal account with a user name and password.

5800.9 Preventing and Mitigating Identity Theft

A. 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:

1. Once potentially fraudulent activity is detected, the staff member making the discovery shall gather all related documentation and write a description of the situation and present this information to their immediate supervisor for follow-up action as necessary.

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

3. Contact the person who holds the covered account;

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

5. Do not open a new covered account;

6. Close an existing covered account;

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

8. Notify law enforcement;

9. 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, and reconcile the address of the consumer with the credit reporting agency, if the District establishes a continuing relationship with the consumer, and regularly, and in the course of business, provides information to the credit reporting agency; or

10. Determine that no response is warranted under the particular circumstances.

5800.10 Updating the Identity Theft Prevention Program (ITPP)

A. The CSSO or designee shall review and revise as needed this ITPP on an annual basis to reflect changes in risks to the safety and soundness of the District from identity theft, based upon the following factors:

1. The experiences of the District with identity theft;

2. Changes in methods of identity theft;

3. Changes in methods to detect, prevent, and mitigate identity theft;

4. Changes in the types of covered accounts that the District maintains;

5. Changes in the business arrangements of the District, including service provider arrangements.

5800.11 Staff Training

A. New employees or contractors who may come into contact with accounts or personally identifiable information that may constitute a risk to the District or its customers must receive training in all elements of this policy.

B. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the District's administrative procedures are made.

5800.12 Oversight of Service Provider/Contractor Arrangements

A. Whenever the District engages a service provider to perform an activity in connection with one or more covered accounts, the District shall 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. To that end, the District shall require service contractors, by contract, to have policies and procedures to detect relevant "Ref Flags" that may arise in the performance of the service provider's activities, and either report the "Red Flags" to the District, or take appropriate steps to prevent or mitigate identity theft.

B. A service provider or contractor that maintains its own identity theft prevention procedure, consistent with the guidance of the
Red Flag" rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

C. A service provider must provide an updated copy of its ITPP annually as part of the District's annual review process.

5800.13 Methods for Administering the ITPP

A. Oversight of the ITPP by the CSSO or designee shall include:

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

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

3. Approving material changes to the ITPP as necessary to address changing identity theft risks.

Approved 07/13/11