AP 5800
Prevention of Identity Theft in Student Financial Transactions

I. Purpose of the Identity Theft Prevention Program

The purpose of this Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to students from identity theft, by providing for the identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could indicate 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.

II. Definitions

"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. (For example, payment plans for bookstore accounts or parking tickets, issued loans or issued student debit cards. Government entities that defer payment for services provided are not considered creditors for purposes of this ITPP.)

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

A "covered account" includes one that involves multiple payments or transactions.

"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.

III. Identifying and Detecting "Red Flags" For Potential Identity Theft

A. Risk Factors for Identifying "Red Flags"

The District will consider the following factors in identifying relevant "Red Flags:"

(1) The types of covered accounts the District offers or maintains;
(2) The methods the District provides to open the District's covered accounts;
(3) The methods the District provides to access the District's covered accounts; and
(4) The District's previous experience(s) with identity theft.

B. Sources of "Red Flags"

The District will continue to incorporate relevant "Red Flags" into this ITPP from the following sources:

(1) Incidents of identity theft that the District has experienced;
(2) Methods of identity theft that the District identifies that reflects changes in identity theft risks; and

(3) Guidance from the Districts supervisors who identify changes in identity theft risks.

C. Categories of "Red Flags"

The following Red Flags have been identified for the District's covered accounts:

Alerts, Notifications, or Warnings from a Consumer Reporting Agency or other Third Party reporting agency:

(1) A fraud or active duty alert is included with a consumer report the District receives as part of a background check.

(2) A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

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

(4) A consumer report indicates 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.

Suspicious Documents:

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

(6) The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

(7) Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

(8) 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.

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

Suspicious Personally Identifying Information:

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

(a) The physical address does not match any physical address provided by an external source; or

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

(11) Personal identifying information provided by a person is not consistent with other personal identifying information provided by the person. For example, there is a lack of correlation between the SSN range and date of birth.

(12) Personal identifying information is associated with known fraudulent activity as indicated by internal or third-party sources use by the District. For example:

(a) The physical address on an application is the same as the physical 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;

(13) 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 physical 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.

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

(15) The physical address or telephone number provided is the same or similar to the account number or telephone number submitted by an unusually large number of other persons being served by the District.

(16) 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.

(17) Personal identifying information provided is not consistent with personal identifying information that is on file with the District.

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

Unusual Use Of – Or Suspicious Activity Relating To – A Covered Account:

(19) A new covered account is used in a manner that is commonly associated with known patterns of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments made.

(20) 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.

(21) A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active.

(22) 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.

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

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

Notices From Customers/Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses About Possible Identity Theft in Connection with Covered Accounts:

(25) 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.

IV. Measures to Detect "Red Flags"

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

(1) A series of reports and data scans will be created that will assist in the automatic and iterative analysis of data to detect red flags. The scans will occur against data in the ERP system, and will specifically address the categories of red flags (wherever possible) identified in section III.C above. Upon detection of red flags, administrative personnel will automatically be notified, and mitigation efforts will then be taken per section V below. Report and data scan definitions will be reviewed and updated on an annual basis to determine if changes or additions are required

(2) Persons with covered accounts who request a change in their personal information on file, such as a change of physical address, will have the requested changes verified by the District.

The person shall provide at least one written form of verification reflecting the requested changes to the personal information. For example, if a physical address change is requested, then documentation evidencing the new physical address shall be obtained. If a phone number change is requested, then documentation evidencing the new phone number, such as a phone bill, shall be obtained.

V. 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:

(1) Monitor the covered account for evidence of identity theft;

(2) Contact the person who holds the covered account;

(3) Change any passwords, security codes, or other security devices that permit access to a covered account;
(4) Reopen the covered account with a new account number;
(5) Not open a new covered account for the person;
(6) Close an existing covered account;
(7) Not attempt to collect on a covered account or turn over a covered account to a debt collector;
(8) Notifying law enforcement;
(9) Correct the data element that created the flag;
(10) Determine that no response is warranted under the particular circumstances.

VI. Updating the ITPP

The District shall update this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, and/or to reflect changes in risks to the safety and soundness of the District from identity theft, based on 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.

VII. Methods for Administering the ITPP

A. Oversight of the ITPP

Oversight by the Director of Business Services shall include:

(1) Assigning specific responsibility for the ITPP's implementation;
(2) Reviewing reports prepared by the staff regarding compliance of the ITPP; and
(3) Approving material changes to the ITPP as necessary to address changing identity theft risks.

B. Reports

(1) *In General*. Staff responsible for the development, implementation, and administration of this ITPP shall report to the Governing Board on an annual basis.
(2) *Contents of Report*. The report shall address material matters to the ITPP and evaluate the following issues: the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with opening new covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the ITPP.
(3) *Oversight of Service Provider Arrangements*. 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 our service contractors, by contract, to have policies and procedures to detect relevant "Red Flags" that may arise in the performance of the service provider's activities, and either report the "Red Flags" to the District, or to take appropriate steps to prevent or mitigate identity theft.

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

Approved by Student Services Council March 20, 2013