AP 5800 PREVENTION OF IDENTITY THEFT IN STUDENT FINANCIAL TRANSACTIONS

Reference:

Fair and Accurate Credit Transactions Act (15 U.S.C. 1681m(e))

I. The 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.

II. Definitions

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

A "creditor" includes government entities that defer payment for goods (for example, payment plans for bookstore accounts or parking tickets), and 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.

Detection or discovery of a "Red Flag" implicates the need to take action under this ITPP to help prevent, detect, and correct identity theft.

III. 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" types:

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 New and/or Other Additional "Red Flag" Types

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 reflect changes in identity theft risks; and
3) guidance from the District's management, legal counsel, and/or risk management advisors 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:

1) A fraud or active-duty alert is included with a consumer report the District receives as part of a background check of an individual with any duties in, or access to, or who holds covered accounts, and the alert suggests that the individual may be a perpetrator.
2) A consumer reporting agency provides a notice of a credit freeze in response to a request for a consumer report of an individual with any duties in, or access to, or who holds covered accounts, and the alert suggests that the individual may be a perpetrator.
3) A consumer reporting agency provides a notice of address discrepancy. An address discrepancy occurs when an address provided by a student substantially differs from the one the credit reporting agency has on file. See Section V.I. 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 individual with any duties in, or access to, or who holds covered accounts, 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:

1) Documents provided for identification appear to have been forged or altered.
2) The photograph or physical description on the identification is not consistent with the appearance of the individual presenting the identification.

3) Other information on the identification is not consistent with information provided by the person opening a new covered account or individual 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.

Suspicious Personal 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 a report from a consumer reporting agency;
    (b) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File; and/or
    (c) There is a lack of correlation between the SSN range and date of birth.
2) Personal identifying information provided by a person is not consistent with other personal identifying information provided by the person and the types of inconsistencies suggest possible identity theft.
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 on 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, at a prison, or other "red flags" are present, and it is at a mail drop; or
    (b) The phone number is invalid and other "red flags" are associated with the account.
5) The SSN provided is the same as that submitted by other persons currently being served by the District and such submittal or use is suspected of being fraudulent, intentionally incorrect, or otherwise malicious.
6) The address or telephone number provided is the same or similar to the address or telephone number submitted by an unusually large number of other persons being served by the District and such submittal or use is suspected of being fraudulent, intentionally incorrect, or otherwise malicious.

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) 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 when required or requested.

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 of fraud patterns. For example, a person makes a first payment, but there are no subsequent payments or explanatory contacts made and/or he/she/they continues to attempt to conduct business beyond the timeframes typically associated with such circumstances.
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) A pattern of 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) A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active without reasonable purpose such as without enrollment or for non-enrollment-related fees due such as for transcript requests.
4) 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.
5) The District is notified that the person is not receiving paper account statements and at least one other "red flag" condition type exists.
6) The District is notified of unauthorized transactions in connection with a person's covered account.

Notices from Persons, Victims of Identity Theft, Law Enforcement Authorities, or Other Businesses or Individuals About Possible Identity 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.

IV. Measures to Detect "Red Flags"

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

A. When a new covered account is opened, the District shall obtain identifying information about the student or other person seeking to open a covered account.

When collection of additional identifying information is indicated by one or more red flags, the following are examples of the types of valid identification that a person may provide to verify the identity of the person seeking to open or continue using a covered account: Valid state-issued driver's license, valid state-issued identification card, current passport, a Social Security Card, current residential lease, or copy of a deed to the person's home, or invoice/statement for property taxes.

B. Persons with covered accounts who request a name change will be required to (1) make the change in person, (2) provide documentation proving the change, and (3) show valid photo identification.

C. Persons with covered accounts who request a change in their personal information on file, other than a name change which has additional requirements (see IV.B.), will have the requested changes verified by the District.
   1. Such changes made online will be considered verified by reason of valid entry into the account via personal username and password.
   2. Such change requests made in person shall be accompanied by the photo identification of the requester and at least one written form of verification reflecting the requested changes to the personal information. Examples of written verification include a utility bill for an address change or a phone bill for a telephone number change.

D. When a student obtains the college photo identification card, the student shall be required to provide, in person, photo identification in the form of a valid state-issued driver's license, valid state-issued identification card, or current passport.

E. When a breach of electronic or other security measures, including firewalls, is detected, the District shall investigate for suspicious activity, attempted breaks, and violations.

F. When compatible new technologies for identity verification and "red flag" detection in application, enrollment, and other online processes become viable, the District shall consider acquisition.

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:

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. Reopen the covered account with a new account number;
E. Not open a new covered account for the person;
F. Close an existing covered account;
G. Not attempt to collect on a covered account or not sell a covered account to a debt collector;
H. Notify law enforcement;
I. 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
J. Determine that no response is warranted under the particular circumstances.

VI. Updating the ITPP

The District shall update this ITPP on an annual basis or as necessary 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:

A. The experiences of the District with identity theft;
B. Known changes in methods of identity theft;
C. Known changes in methods to detect, prevent, and mitigate identity theft;
D. Changes in the types of covered accounts that the District maintains; and
E. 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 District's Vice President of Business Services and Vice President of Student 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 Vice President of Business Services and Vice President of Student Services on an annual basis or as necessary.

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, and/or to take appropriate steps to prevent or mitigate identity theft.

Offices of Primary Responsibility: Vice President, Business Services
Vice President, Student Services

Date Approved: August 24, 2009
Dates Revised: April 11, 2011; January 27, 2025
Date Reviewed: February 20, 2019