

STUDENT SERVICES

**AP 5900 PREVENTION OF IDENTITY THEFT IN STUDENT FINANCIAL
TRANSACTIONS****References:**

Fair and Accurate Credit Transactions Act (FACT Act) (15 U.S. Code Section 1681m(e))

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.

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 the 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.

Detecting “Red Flags” For Potential Identity Theft

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

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

- the types of covered accounts the District offers or maintains
- the methods the District provides to open the District’s covered accounts
- the methods the District provides to access the District’s covered accounts
- the District’s previous experience(s) with identity theft

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

- incidents of identity theft that the District has experienced

- 36
- 37
- 38
- 39
- 40
- methods of identity theft that the District identifies that reflects changes in identity theft risks
 - guidance from the District's management, legal counsel, and/or risk management advisors who identify changes in identity theft risks

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

- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60
- 61
- 62
- 63
- 64
- 65
- 66
- 67
- 68
- 69
- 70
- 71
- 72
- 73
- 74
- 75
- 76
- 77
- 78
- 79
- 80
- 81
- Alerts, Notifications, or Warnings from a Consumer Reporting Agency, such as:
 - 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.
 - A consumer reporting agency provides a notice of 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.
 - 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 the section titled Preventing and Mitigating Identity Theft for specific steps that must be taken to address this situation.
 - 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 recent and significant increase in the volume of inquiries
 - An unusual number of recently established credit relationships
 - A material change in the use of credit, especially with respect to recently established credit relationships
 - An account that was closed for cause or identified for abuse of account privileges by a creditor or financial institution
 - Suspicious Documents, such as:
 - Documents provided for identification appear to have been forged or altered
 - The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification
 - Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification
 - 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
 - An application appears to have been altered or forged, or gives the appearance of having been destroyed or reassembled
 - Suspicious Personally Identifying Information, such as:
 - When necessitated by the presence of an applicable red flag, checks of provided personally identifying information reveal inconsistencies when

82 compared against external information sources used by the District. For
83 example:

- 84 • The address does not match any address in the consumer report
- 85 • The Social Security Number (SSN) has not been issued, or is listed on the
86 Social Security Administration's Death Master File, or
- 87 • There is a lack of correlation between the SSN range and date of birth

- 88 ○ Personal identifying information provided by a person is not consistent with
89 other personal identifying information provided by the person and the types of
90 inconsistencies suggest possible identity theft. For example:

- 91 • The name or identifying number on a document does not match identifying
92 information on other immigration documents

- 93 ○ Personal identifying information is associated with known fraudulent activity
94 as indicated by internal or third-party sources used by the District. For
95 example:

- 96 • The address on an application is the same as the address provided on a
97 fraudulent application
- 98 • The phone number on an application is the same as the phone number
99 provided on a fraudulent application

- 100 ○ Personal identifying information provided is of a type commonly associated
101 with fraudulent activity as indicated by internal or third-party sources used by
102 the District. For example:

- 103 • The address on an application is fictitious, a mail drop, or a prison or
- 104 • The phone number is invalid or is associated with a pager or answering
105 service

- 106 ○ The SSN provided is the same as that submitted by other persons currently
107 being served by the District and such submittal or use is suspected of being
108 fraudulent, intentionally incorrect, or otherwise malicious.

- 109 ○ The address or telephone number provided is the same or similar to the
110 address or telephone number submitted by an unusually large number of
111 other persons being served by the District and such submittal or use is
112 suspected of being fraudulent, intentionally incorrect, or otherwise malicious.

- 113 ○ The person opening the covered account fails to provide all required personal
114 identifying information on an application or in response to notification that the
115 application is incomplete.

- 116 ○ Personal identifying information provided is not consistent with personal
117 identifying information that is on file with the District.

- 118 ○ The person opening the covered account cannot provide authenticating
119 information beyond that which generally would be available from a wallet or
120 consumer report when required or requested.

- 121
- 122 • Unusual Use of (or Suspicious Activity Relating to) a Covered Account, such as:
 - 123 ○ A new covered account is used in a manner that is commonly associated with
124 known patterns of fraud. For example, a person makes a first payment, but
125 there are no subsequent payments or explanatory contacts made and/or
126 he/she continues to attempt to conduct business beyond the timeframes
127 typically associated with such circumstances.

- 128 ○ A covered account is used in a manner that is not consistent with established
129 patterns of activity on the account. For example, there is:
130 • Nonpayment when there is no history of late or missed payments, or
131 • A material change in electronic fund transfer patterns in connection with a
132 payment.
133 ○ A covered account that has been inactive for a reasonably lengthy period of
134 time is suddenly used or active without reasonable purpose such as without
135 enrollment of for non-enrollment-related fees due such as for transcript
136 requests.
137 ○ Mail sent to the person holding the covered account is returned repeatedly as
138 undeliverable although transactions continue to be conducted in connection
139 with the person's covered account.
140 ○ The District is notified that the person is not receiving paper account
141 statements and at least one other "red flag" condition type exists.
142 ○ The District is notified of unauthorized transactions in connection with a
143 person's covered account.
144
145 • Notices from Persons, Victims of Identity Theft, Law Enforcement Authorities, or
146 Other Businesses About Possible Identity Theft in Connection with Covered
147 Accounts, such as:
148 ○ The District is notified by a person with a covered account, a victim of identity
149 theft, a law enforcement authority, or any other person, that it has opened a
150 fraudulent account for a person engaged in identity theft.
151

152 **Measures to Detect "Red Flags"**

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

- 154 • When a new covered account is opened, the District may obtain identifying
155 information about, and information verifying the identity of, the student or other
156 person seeking to open a covered account if one or more "red flags" are
157 indicated. The following are examples of the types of valid identification that a
158 person may provide to verify the identity of the person seeking to open the
159 covered account:
160 ○ Valid state-issued driver's license
161 ○ Valid state-issued identification card
162 ○ Current passport
163 ○ Social Security Card
164 ○ Other photo identification believed to be authentic
165 ○ Current residential lease, or
166 ○ Copy of a deed to the person's home or invoice/statement for property taxes
167
168 • Persons with covered accounts who request a name change will be required to:
169 ○ Make the change in person
170 ○ Provide documentation proving the change
171 ○ Show valid photo identification, such as state-issued driver's license or
172 identification card or current passport
173

- 174
- 175
- 176
- 177
- 178
- 179
- 180
- 181
- 182
- 183
- 184
- 185
- 186
- 187
- 188
- 189
- 190
- 191
- 192
- 193
- 194
- 195
- 196
- 197
- 198
- 199
- Persons with covered accounts who request a change in their personal information on file, other than a name change, will have the requested changes verified by the District, as follows:
 - Any changes made on-line will be considered verified by reason of valid entry into the account using personal username and password.
 - Any 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. For example, if an address change is requested, then documentation evidencing the new 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.
 - When a student obtains the District 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 or identification card or a current passport.
 - When a breach of the District's electronic or other security measures, including firewalls, is detected, an analysis shall be performed to identify any suspicious activity, attempted breaks, and violations.
 - The District shall consider implementation of any new technologies for identity verification and "red flag" detection in application, enrollment and other on-line processes when they become available.

Preventing and Mitigating Identity Theft

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

- 202
- 203
- 204
- 205
- 206
- 207
- 208
- 209
- 210
- 211
- 212
- 213
- 214
- 215
- 216
- 217
- 218
- 219
- Monitor the covered account for evidence of identity theft
 - Contact the person who holds the covered account
 - Block all online transactions and process transaction requests in-person with appropriate identification
 - Change any passwords, security codes, or other security devices that permit access to a covered account
 - Reopen the covered account with a new account number
 - Not open a new covered account for the person
 - Close an existing covered account
 - Not attempt to collect on a covered account or not sell a covered account to a debt collector
 - Notifying law enforcement
 - 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,

- 220 and in the course of business, provides information to the credit reporting
221 agency, or
222 • Determine that no response is warranted under the particular circumstances.
223

224 **Updating the ITPP**

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

- 228 • The experiences of the District with identity theft
- 229 • Changes in methods of identity theft
- 230 • Changes in methods to detect, prevent and mitigate identity theft
- 231 • Changes in the types of covered accounts that the District maintains
- 232 • Changes in the business arrangements of the District, including service provider
233 arrangements

234
235 **Methods for Administering the ITPP**

236 Oversight by the District’s Vice President of Finance and Administrative Services and
237 Vice President of Student Services shall include:

- 238 • Assigning specific responsibility for the ITPP’s implementation
- 239 • Reviewing reports prepared by the staff regarding compliance of the ITPP
- 240 • Approving material changes to the ITPP as necessary to address changing
241 identity theft risks

242
243 Staff responsible for the development, implementation, and administration of this ITPP
244 shall report to the Vice President of Finance and Administrative Services and Vice
245 President of Student Services on an annual basis, or as necessary. The report shall
246 address material matters to the ITPP and evaluate the following issues: the
247 effectiveness of the policies and procedures in addressing the risk of identity theft in
248 connection with opening new covered accounts and with respect to existing covered
249 accounts; service provider arrangements; significant incidents involving identity theft
250 and management’s response; and recommendations for material changes to the ITPP.
251

252 Whenever the District engages a service provider to perform an activity in connection
253 with one or more covered accounts the District shall take steps to ensure that the
254 activity of the service provider is conducted in accordance with reasonable policies and
255 procedures designed to detect, prevent, and mitigate the risk of identity theft. To that
256 end, the District shall require our service contractors, by contract, to have policies and
257 procedures to detect relevant “Red Flags” that may arise in the performance of the
258 service provider’s activities, and either report the “Red Flags” to the District, or to take
259 appropriate steps to prevent or mitigate identity theft.

260 Offices of Primary Responsibility: Student Services and Finance and Administrative
261 Services