AP 5800 Prevention of Identity Theft in Student Financial Transactions

Reference:

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

1.0 The purpose of the Identity Theft Prevention Program 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.

2.0 Definitions:

2.1 Account: Any relationship to obtain a product or service that a customer may have with the District.

2.2 Covered Account: An account that involves multiple payments or transactions.

2.3 Creditor: Government entities who defer payment for goods or services. Examples of activities that would indicate the District/college as a creditor would include:

2.3.1 Participation in the Federal Perkins Loan Program.

2.3.2 Offering institutional loans to students, faculty, or staff.

2.3.3 Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester.

2.3.4 Emergency loans.

2.4 Personal Information: Specific information that represents a legal or personal identity or that could result in public impersonation of identity or identity theft if such information were stolen or compromised. This would also consist of using information in combination with one or more data elements when either the name or elements are not encrypted or redacted. Sensitive personal information includes but may not be limited to the following:

2.4.1 Legal name (first, last, middle).

2.4.2 Full date of birth.

2.4.3 Social security number.

2.4.4 Driver's license number.

2.4.5 Banner ID.

2.4.6 Financial account number.

AP 5800 Prevention of Identity Theft in Student Financial Transactions

2.4.7 Password.

2.4.8 Home address.

2.4.9 Gender.

2.4.10 Race.

2.4.11 Medical information.

2.4.12 Payroll information.

2.5 Red Flag: A pattern, practice, or specific activity that indicates the existence of identity theft or possible attempted fraud via identity theft on covered accounts.

2.6 Security Incident: A collection of related activities or events, which provide evidence that personal information, could have been acquired by an unauthorized person.

3.0 Identification of Red Flags: In order to identify relevant red flags, the District considers the types of accounts that it offers and maintains, the methods provided to open accounts, the methods provided to access accounts , as well as previous experiences with identity theft. The following categories are identified as red flags:

3.1 Alerts, notifications or warnings from a consumer-reporting agency, including fraud alerts, credit freezes, or official notice of address discrepancies.

3.2 The presentation of suspicious documents such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application that appears to have been cut up, reassembled, and photocopied.

3.3 The presentation of suspicious personal identifying information such as a photograph or physical description on the identification that is not consistent with the appearance of the student presenting the identification; discrepancies in address, social security number, student ID, or other information on file; an address that is a mail-drop, a prison, or is invalid; a phone number that is likely to be a pager or answering service; and/or failure to provide all required information.

3.4 Unusual use or suspicious account activity that would include material changes in payment patterns, notification that the account holder is not receiving mailed statement, or that the account has unauthorized charges.

3.5 A request to mail something to an address that is not on file.

3.6 Notice received from students, victims of identity theft, law enforcement, or other persons regarding possible identity theft in connection with covered accounts.

AP 5800 Prevention of Identity Theft in Student Financial Transactions

4.0 Detection of Red Flags: The detection of red flags in connection with the opening of covered accounts and the processing of existing accounts can be made through internal controls such as:

4.1 Obtaining and verifying the identity of a person opening and using an account.

4.2 Authenticating the identity of students or staff.

4.3 Monitoring transactions.

4.4 Verifying the validity of change of address requests for existing covered accounts.

5.0 Response to Red Flags: The District's Identity Theft Prevention Program shall provide for appropriate responses to detected red flags in order to prevent and mitigate identity theft. This would include:

5.1 Monitoring covered accounts for evidence of identity theft.

5.2 Denying access to a covered account until other information is available to eliminate the identified red flag or close the existing covered account.

5.3 Notifying the customer.

5.4 Changing any passwords, security codes, or other security devices that permit access to a covered account.

5.5 Closing an existing account.

5.6 Reopening a covered account with a new account number.

5.7 Notifying law enforcement if suspected illegal activity.

5.8 Determining if no response is warranted given the particular circumstances.

6.0 Security Incident Reporting: An employee who believes that a security incident has occurred shall immediately notify their immediate management supervisor. After normal business hours, notification shall be made to the Campus Safety Office.

7.0 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.

AP 5800 Prevention of Identity Theft in Student Financial Transactions

8.0 Program Oversight: The Chancellor or designee shall be the program administrator. The administrator shall exercise appropriate and effective oversight over the Identity Theft Prevention Program and shall report regularly to the Board of Trustees on the program. The administrator is also responsible for developing, implementing, and updating the Identity Theft Prevention Program, including the appropriate training of college and District employees regarding the program.

Date of Adoption: August 22, 2011