Procedure: 4.17A

Identity Theft Prevention (Red Flags)

Purpose

To provide guidance for the Identify Theft Prevention policy.

Procedure Statement

Specific "Red Flags" as identified in the Policy include:

- Notification and Warnings from Credit Reporting Agencies
- Suspicious Documents
- Suspicious Personal Identifying Information
- Suspicious Account Activity or Unusual Use of Account
- Alerts from Others

Detecting "Red Flags"

The Plan's general "Red Flag" detection practices are described in this procedure document. The Plan Administrator will develop and implement specific methods and shall provide for appropriate responses to detected "Red Flags" to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed.

1) New Accounts

   To detect any of the "Red Flags" associated with the opening of a new account, College personnel will take the following steps to obtain and verify the identity of the person opening the account:

   - Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification.
   - Verify the customer's identity (for instance, review a driver's license or other identification card).
   - Independently contact the customer.

2) Existing Accounts

   To detect any of the "Red Flags" for an existing account, College personnel will take the following steps to monitor transactions with an account:

   - Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email).
   - Verify the validity of requests to change billing addresses.
   - Verify changes in banking information given for billing and payment purposes.

Responding to "Red Flags" and Mitigating Identity Theft

Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the College from damages and loss. The employee must gather all related documentation and write a description of the situation. This information must be presented to a department supervisor for determination. The supervisor will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

1) Appropriate responses to the detection of "Red Flags" include:
    - Monitor a covered account for evidence of identity theft.
    - Contact the customer.
    - Change any passwords, security codes or other security devices that permit access to a covered account.
    - Reopen a covered account with a new account number.
    - Not open a new covered account.
    - Close an existing covered account.
    - Notify law enforcement.
    - Determine no response is warranted under the circumstances.

Staff Training and Reporting

College employees responsible for implementing the Plan shall be trained under the direction of the Plan Administrator in the detection of "Red Flags", and the responsive steps to be taken when a "Red Flag" is detected.

Appropriated staff shall provide reports to the Plan Administrator on incidents of identity theft, the effectiveness of the Plan and the College's compliance with the Plan.

Service Provider Arrangements

In the event the College engages a service provider to perform an activity in connection with one or more accounts, the College will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft:

- Require, by contract, that service providers have such policies and procedures in place.
- Require, by contract, that service providers review the Utility's Plan and report any "Red Flags" to the Plan Administrator.

Periodic Updates to the Plan

At periodic intervals, or as required, the Plan will be re-evaluated to determine whether all aspects of the plan are up to date and applicable in the current business environment.

Created: 05/18/2021