Policy Series 3000
Policy 3005

Procedure 3005.2
Identity Theft Prevention Program

I. Background

In compliance with the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003, the Northern Wyoming Community College District (NWCCD or District) developed this procedure initially in 2010.

II. Definitions

Identity theft – fraud committed or attempted using the identifying information of another person without authority.

Covered account – an account that a creditor offers or maintains, primarily for personal, educational, family, or household purposes, that involves or is designed to permit multiple payments or transactions.

Red flag – a pattern, practice, or specific activity that indicates the possible existence of identity theft.

III. Purpose

The purpose of the Identity Theft Prevention Program (ITTP) is to prevent, detect, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the ITTP. The ITTP shall include the following processes and incorporate existing procedures and processes that control reasonably foreseeable risks:

a. Identification of relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
b. Detection of red flags that have been incorporated into the Program;
c. Appropriate responses to any red flags that are detected, to prevent and mitigate identity theft; and
d. Assurance that the program is reviewed annually and updated as needed to reflect changes in risks from identity theft to individuals, and to the safety and soundness of the creditor.

IV. Covered accounts include the following:

- Student accounts, degree-seeking
- Student accounts, non-degree-seeking
- Employee accounts

V. Identification of relevant red flags

a. The ITTP considers the following risk factors in identifying relevant red flags for covered accounts:
   i. The types of covered accounts as noted above;
   ii. The methods provided to open covered accounts: acceptance to the District and enrollment in classes requires a common application with personally identifying information; employment with the District requires a background check and confirmation of personally identifying information.
   iii. The methods provided to access covered accounts:
      1. Username and password generated from a verified student application or employment.
      2. Disbursements obtained in person require photo identification.
      3. Disbursements obtained by mail can only be mailed to an address on file.
      4. Disbursements via ACH are verified by a pre-note process.
   iv. The District's previous history with identity theft.

b. The ITTP identifies the following red flags:
   i. Documents provided for identification appear to have been altered or forged;
   ii. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
   iii. A request to mail something to an address not listed on file; or
   iv. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

c. The ITTP detects red flags relevant to each type of covered account as follows:
   i. Degree-seeking student account with a credit balance involving a PLUS loan – as directed by federal regulation (U.S. Department of Education) these balances are required to be refunded in the parent's name and mailed to their address on file within the time period specified. No request is required. **Red Flag** – none as this is initiated by the District.
   ii. Student account with a credit balance, no PLUS loan – the refund check can only be mailed to an address on file or be deposited directly into a student's preferred banking account via ACH.   **Red Flag** – information does not match District records.
   iii. Requests from current or former students via phone require confirmation of identify using the Student Identification Verification process which is maintained by the Colleague Manager's Group. **Red Flag** – information does not match District records.
   iv. Emergency funding - Requests must be made in person by presenting a photo ID. The check can only be mailed to an address on file or picked up in person by showing photo ID. **Red Flag** – photo ID not appearing to be authentic or not matching the appearance of the student presenting it.

VI. Response – The ITTP provides appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate response(s) to the relevant red flags are as follows (more than one response may apply):

- Deny access to the covered account until other information is available to eliminate the red flag;
- Contact the student;
- Change any passwords, security codes or other security devices that permit access to a covered account;
- Notify law enforcement; or
- Determine no response is warranted upon review.

VII. Oversight of the ITTP

Responsibility for developing, implementing, and updating this Program lies with the Vice President for Administration/CFO. As named in *Procedure 3005.1: Data Security Information Program*, the members of the Colleague Manager's Group are responsible for the daily management of the program implementation; ensuring appropriate training of District staff on the program; reviewing any staff reports regarding the detection of red flags and the steps for preventing and mitigating identity theft; determining which steps of prevention and mitigation should be taken in particular circumstances; recommending improvements to the program; and producing an annual report that includes all red flag reports.

This ITTP will be reviewed annually and updated to reflect changes in risks from identity theft to students and the soundness of the District. The Colleague Manager's Group will consider any experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the District maintains, and changes in the District business arrangements with other entities.

VIII. Staff Training

The Colleague Manager's Group will provide leadership to the development, execution, and assessment of the training program for the District staff responsible for implementing the ITTP.

IX. Oversight of Service Providers

The District shall take steps to ensure that the activity of a service provider that interacts with student accounts (e.g., collection agency, payment plan processor) is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. Current contracts are kept with the Director of Finance/Controller.