POLICY
1088

SCHOOLCRAFT COLLEGE

18600 Haggerty Road, Livonia, Michigan 48152-2696

IDENTITY THEFT PREVENTION PROGRAM

PURPOSE

To establish an Identity Theft Prevention Program designed to detect, prevent 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 Program in compliance with the Federal Trade Commission's Red Flags Rule which implements Section 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Under the Red Flags Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags when they occur in covered accounts;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically, to reflect changes in risks to students and to implement additional steps to protect them from Identity Theft if necessary.

DEFINITIONS

A RED FLAG means a pattern, practice or specific activity that indicates the possible existence of identity theft.

IDENTIFYING INFORMATION means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

IDENTIFY THEFT means fraud committed or attempted using the identifying information of another person without authority.

A COVERED ACCOUNT is an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.

IDENTIFICATION OF RED FLAGS

The College identifies the following Red Flags, in each of the listed categories:

SUSPICIOUS DOCUMENTS

1. Documents provided for identification that appear to have been forged, altered or inauthentic;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. A request to mail something to an address not on file.

SUSPICIOUS PERSONAL IDENTIFYING INFORMATION

1. Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);
2. Social security number presented that is the same as one given by another student;
3. A person's identifying information is not consistent with the information that is on file for the student.

SUSPICIOUS ACCOUNT ACTIVITY OR UNUSUAL USE OF ACCOUNT

1. Change of address for an account followed by a request to change the account holder's name;
2. Stop payment request on an otherwise consistently up-to-date account;
3. Mail sent to the account holder is repeatedly returned as undeliverable;
4. Notice to the College that a customer is not receiving mail sent by the College.

ALERTS FROM OTHERS

1. Notice from a student, identity theft victim, law enforcement or other person regarding possible identity theft in connection with covered accounts.

DETECTING RED FLAGS

NEW STUDENTS

In order to detect any of the Red Flags identified above 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:

1. Verify the student's identity and address (for instance, review a driver's license or other identification card).

EXISTING ACCOUNTS

In order to detect any of the Red Flags identified above for an existing account, College personnel will take the following steps to monitor transactions with an account:

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

RESPONSE

The Program shall provide for appropriate responses to detected Red Flags to prevent and mitigate identity theft. The appropriate responses to the relevant Red Flags are as follows:

1. Deny access to the covered account until other information is available to eliminate the Red Flag;
2. Contact the student;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.

PROGRAM ADMINISTRATION

OVERSIGHT

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee for the College. The Committee is headed by the Vice President and Chief Financial Officer with the Vice President and Chief Student Affairs Officer, the Chief of Police, the Controller and Director of Finance, and an Information Services Administrator comprise the remainder of the committee membership. The Vice President and Chief Financial Officer and the Vice President and Chief Student Affairs Officer will be responsible for the Program administration in their respective areas and for ensuring appropriate training of their staff. The Committee will be responsible for 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 and considering periodic changes to the Program.

REPORTS

Staff is required to provide reports to the Identity Theft Committee on incidents of Identity Theft, the College's compliance with the Program and the effectiveness of the Program.

SPECIFIC PROGRAM ELEMENTS AND CONFIDENTIALITY

For the effectiveness of Identity Theft Prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the College's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices are to be limited to the Identity Theft Committee and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general Red Flag detection, implementation and prevention practices are listed in this document.

OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

The College shall take steps to ensure that the activity of a service provider 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.

Currently the College uses Nelnet to administer the Deferred Tuition Payment Plan. Students contact Nelnet directly through its website or by telephone and provide personally identifying information to be matched to the records that the College has provided to Nelnet.

Adopted—April 22, 2009
(2009-48)
Revised—VP and CFO
August 1, 2019