WASHTENAW COMMUNITY COLLEGE

IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION PROGRAM

PURPOSE AND SCOPE

The Identity Theft Prevention Program was developed pursuant to the Federal Trade Commission's Red Flag Rules promulgated as part of the Fair and Accurate Credit Transactions Act. The Program is designed to detect, prevent and mitigate identify theft in connection with the opening of a covered account or any existing covered accounts within Washtenaw Community College (College). The Program has been designed to be appropriate to the size and complexity of the College as a creditor and the nature and scope of its activities.

THE RED FLAGS RULES AND OVERVIEW

The Red Flag Rules, found at 16 CFR § Part 681, require users of consumer credit reports, certain creditors and certain card issuers to take various steps to protect consumers from identity theft.

Users of credit reports must respond to notices of address discrepancies and take reasonable steps to confirm the accuracy of the address it may have.

A creditor must periodically determine, by conducting a risk assessment, whether it offers or maintains covered accounts. Upon identifying any covered account(s), the creditor is required to develop and implement a written Identity Theft Prevention Program designed to:

A. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
B. Detect Red Flags;
C. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
D. Periodically update the program to reflect changes in risks to the account holders or to the safety and soundness of the creditor from Identity Theft.

A card issuer must establish and implement reasonable address verification procedures.

Oversight and administration of the Program shall be performed by the Office of the Vice President & Chief Financial Officer.

Washtenaw Community College administers a tuition payment plan that allows qualified students to pay their tuition and fees throughout the semester. This plan involves multiple transactions and

payments. As a result of this plan, the College is a "creditor" and the student accounts are "covered accounts" subject to the Red Flag Rule promulgated by the Federal Trade Commission under the Fair Credit Reporting Act.

The College may also from time to time use consumer reports to conduct credit or background checks on prospective employees. As a user of consumer reports, and as a "creditor" that holds "covered accounts," the College is required to develop and implement an identity theft prevention program.

RED FLAGS

Relevant patterns, practices, and specific activities that signal possible identity theft are "red flags" under the rule. Red flags include the following:

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

2. The presentation of suspicious documents;

3. The presentation of suspicious personal identifying information, such as a suspicious address change;

4. The unusual use of, or other suspicious activity related to, a covered account; and

5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

More detailed examples of these categories of red flags are included in Appendix A.

DEFINITIONS

A. **"Account"** means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes. It includes (i) an extension of credit, such as the purchase of property or services involving a deferred payment, and (ii) a deposit account.

B. **"Covered Account"** means (i) an account that a creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions and (ii) any other account that the creditor offers to maintain for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

C. **"Identity Theft"** means a fraud committed or attempted using the identifying information of another person without authority.

D. **"Red Flag"** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

E. **"Service Provider"** means a person that provides a service directly to the financial institution or creditor.

Covered Accounts Maintained by Washtenaw Community College

A. Internal Loan Programs
B. Student Accounts
C. Other accounts that may be identified by units as meeting the definition of Covered Account.

PROCEDURES

Notification and Protocol

Any employee who detects a red flag shall first notify the College's Controller. In the case of an employee in the financial aid area, the employee should notify the Director of Financial Aid, if available, and the Controller. The Controller shall consult with appropriate personnel to determine the most effective course of action. Action steps may include, but are not limited to, the following:
(a) Monitoring a covered account for evidence of identity theft;
(b) Contacting the customer;
(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
(d) Reopening a covered account with a new account number;
(e) Not opening a new covered account;
(f) Closing an existing covered account;
(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
(h) Notifying law enforcement; or
(i) Determining that no response is warranted under the particular circumstances

The Controller shall report incidents to the Vice President & Chief Financial Officer on an as needed basis.

Training

College personnel with responsibilities in the areas of student accounts and financial aid shall receive training as part of this plan. Training shall include detection and recognition of red flags,

appropriate handling of notices, and protocol and action steps. College staff in other areas, such as Human Resource Management and Student Services, may receive training as appropriate.

In the interest of preventing identity theft, all personnel shall also receive training with regard to the WCC Enterprise Information Security Plan.

PROGRAM ASSESSMENT AND UPDATE

The Controller shall report at least annually to the Vice President on the effectiveness of the program, significant incidents involving identity theft and management's response; and recommendations for material changes to the Program. Factors to consider when assessing the effectiveness of this program include: prior experiences with identity theft; changes in the methods of identity theft; changes in the method of detection, prevention and mitigation of identity theft; the covered accounts offered and administered by the College; and the potential Red Flags that may arise with respect to the Covered Accounts. This periodic assessment should consider any changes in risks to students and individual account holders of identity theft, findings from the annual departmental reports, and the safety and soundness of the College's identify protection systems. The Controller shall update the Program as needed.

Adopted October 28, 2008
Reviewed and Updated December 20, 2017

APPENDIX A

EXAMPLES OF RED FLAGS

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in Sec. 681.1(b) of the regulations.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, 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; or
   An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
The address does not match any address in the consumer report; or
The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

10. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

11. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

12. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
The address on an application is fictitious, a mail drop, or a prison; or
The phone number is invalid, or is associated with a pager or answering service.

13. The SSN provided is the same as that submitted by other persons opening an account or other customers.

14. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

15. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

16. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

17. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

Nonpayment when there is no history of late or missed payments;

A material increase in the use of available credit;

A material change in purchasing or spending patterns;

A material change in electronic fund transfer patterns in connection with a deposit account; or

A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.