

## PROPOSED BOARD AUXILIARY POLICY

### IDENTITY THEFT RED FLAG AND SECURITY INCIDENT REPORTING

#### I. Purpose

In accordance with the provisions outlined in the Federal Trade Commission's Red Flag Rule, which implements Section 114 of the Fair and Accurate Transactions Act (FACTA) of 2003, the Maricopa County Community College District shall implement a program for Identity Theft Prevention. The purpose of the 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.

#### II. Definitions

- Covered Account – is a consumer account that involves multiple payments or transactions in arrears such as a loan that is billed or payable monthly. This includes accounts where payments are deferred and made by a borrower periodically over time such as with a tuition or fee installment payment plan.
- Creditor – is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal or continuation of credit. Examples of activities that would indicate a Maricopa college or the District as a creditor would include:
  - Participation in the Federal Perkins Loan program;
  - Participation as a school lender in the Federal Family Education Loan Program;
  - Offering institutional loans to students, faculty or staff
  - Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester.
  - Emergency loans.
- 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:
  - Legal name (first, last, middle)
  - Full date of birth
  - SSN
  - Driver's License Number
  - Enterprise ID
  - Financial account number
  - Password
  - Home address
  - Gender

- Race
- Medical information
- Payroll information
- 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.
- Security Incident – a collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

III. **Identification of Red Flags** – In order to identify relevant red flags, the MCCCDC 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:

- a. Alerts, notifications or warnings from a consumer reporting agency including fraud alerts, credit freezes or official notice of address discrepancies.
- b. 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.
- c. 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.
- d. 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;
- e. A request to mail something to an address that is not on file;
- f. Notice received from students, victims of identity theft, law enforcement, other persons regarding possible identity theft in connection with covered accounts.

IV. **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:

- a. Obtaining and verifying the identity of a person opening and using an account
- b. Authenticating customers
- c. Monitoring transactions
- d. Verifying the validity of change of address requests for existing covered accounts

V. **Response to Red Flags** – Maricopa’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:

- a. Monitoring covered accounts for evidence of identity theft;

- b. Denying access to a covered account until other information is available to eliminate the identified red flag, or close the existing covered account;
- c. Notify the customer
- d. Change any passwords, security codes or other security devices that permit access to a covered account
- e. Close an existing account;
- f. Reopen a covered account with a new account number;
- g. Notify law enforcement if suspected illegal activity ;
- h. Determine if no response is warranted given the particular circumstances.

**VI. Security Incident Reporting** – An employee who believes that a security incident has occurred, shall immediately notify their appropriate supervisor and the Program Manager. After normal business hours, notification shall be made to the college public safety office.

**VII. Service Providers Oversight** – The Maricopa County Community College 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 MCCCDC 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 MCCCDC of the detection of a Red Flag or if the service provider is responsible for implementing appropriate steps to prevent or mitigate identity theft.

**VIII. Program Oversight** – The Chancellor shall designate a program administrator. The Program Administrator shall exercise appropriate and effective oversight over the Program and shall report regularly to the Governing Board and the Chancellor on the Program. The program administrator shall be responsible for developing, implementing and updating the Program throughout the Maricopa district. The Program Administrator shall be responsible for ensuring the appropriate training of college and district employees, reviewing staff reports regarding the detection of Red Flags and implementing steps to identify, prevent and mitigate identity theft.