5.075 Identity Theft, Red Flag and Security Incident Reporting 5.075

The Mohave Community College Board of Trustees shall implement a program for Identity Theft Prevention. (Section 114 of the Fair and Accurate Transactions Act (FACTA) of 2003).

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 Mohave Community College District has directed the implementation of 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 security incident.

A. The President shall designate a Program Administrator. The Program Administrator shall exercise appropriate and effective oversight over the Program and the Red Flag Taskforce and shall report regularly to the Risk Management Committee and to the President regarding program outcomes and to Governing Board (as required). The Program Administrator shall be responsible for developing, implementing and updating the Program throughout the Mohave Community College District. The Program Administrator shall be responsible for ensuring the appropriate training of college and district personnel, reviewing staff reports regarding the detection of Red Flags and implementing steps to identify, prevent and mitigate identity theft.

B. Mohave Community College remains responsible for compliance with the Red Flag Rules even in instances where services are outsourced to a third party. However, any written agreement between Mohave Community College and the third party 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 contracted activities. The written agreement or contract must also indicate whether the contracted third party provider is responsible for implementing appropriate steps to prevent and mitigate identity theft, and/or if the provider is responsible for notifying Mohave Community College of the detection of Red Flag events.

C. An employee who believes that a security incident has occurred shall immediately notify their immediate supervisor and the Program Administrator. After normal business hours, notification shall be made to the Chief Financial Officer.

D. The Program Administrator shall appoint a review committee, designated the Red Flag Taskforce, consisting of appropriate Mohave Community College administrators to review issues, assist with training, and monitor the policy for future issues. The Taskforce shall meet on at least a quarterly basis, during which time the Program Administrator will report on events, findings, issues, and trends to the Red Flag Taskforce for their understanding and advice.

E. The Program Administrator shall ensure that the Mohave Community College Identity Theft Prevention Program shall provide for appropriate responses to detected red Flags in order to prevent and mitigate identity theft. Appropriate Responses would include:

1. Monitoring covered accounts for evidence of identity theft;
2. Denying access to a covered account until other information is available to eliminate the identified red flag, or close the existing covered account;
3. Notify the customer
4. Change any passwords, security codes or other security devices that permit access to a covered account;
5. Close an existing account;
6. Reopen a covered account with a new account number;
7. Notify law enforcement if suspected illegal activity;
8. Determine if no response is warranted given the particular circumstances.

F. The Program Administrator will provide for 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:

1. Obtaining and verifying the identity of a person opening and using an account;
2. Authenticating customers;
3. Monitoring transactions;
4. Verifying the validity of change of address request for existing covered accounts.

G. In order to identify relevant red flags, Mohave Community College takes into consideration 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 and investigation of newly reported types of identity theft by federal, state and other agencies.

H. The following categories are identified as “red flags”:

1. Alerts, notifications or warning from a consumer reporting agency including fraud alerts, credit freezes or official notice of address discrepancies.
2. 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.

3. 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 or individual presenting the identification; discrepancies in address, Social Security Number, Student ED, 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.
4. Unusual use or suspicious account activity that would include material changes in payment patterns, notification that the account holder is not receiving mailed statements, or that the account has unauthorized charges.
5. A request to mail something to an address that is not on file;
6. Notice received from students, victims of identity theft, law enforcement, other persons regarding possible identity theft in connection with covered accounts.

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 person or entity that regularly arranges for the extension, renewal or continuation of credit. Examples of activities that would indicate Mohave Community College is a creditor would include:

1. Offering institutional loans to students, faculty or staff;
2. Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester;
3. 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:

1. Legal name (first, last, middle)
2. Full date of birth
3. SSN
4. Driver's license Number
5. Enterprise ID
6. Financial account number

7. Password
8. Home address
9. Gender
10. Race
11. Medical Information
12. 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.

Date of Adoption: *Adoption of Manual: July 2008*

References: *ARS 13-3821 and ARS 13-3826, et seq*