DMACC IDENTITY THEFT- RED FLAGS PROCEDURES

This document contains identity theft red flag procedures for Des Moines Area Community College.

1. PURPOSE

The purpose of these Identity Theft Red Flags Procedures is to detect, prevent, and mitigate loss due to errors or malicious behavior when working with consumers' new and existing covered accounts. DMACC recognizes that absolute security against all threats is an unrealistic expectation. Therefore, the goals of risk reduction and implementation of these procedures are based on:

- An assessment of the "covered accounts" handled by DMACC.
- The cost of preventative measures designed to detect and prevent errors or malicious behavior.
- The amount of risk that DMACC is willing to absorb.

These procedures were derived through a risk assessment of DMACC methods of opening new or accessing existing accounts. Determination of appropriate security measures must be a part of all operations and shall undergo periodic evaluation.

2. BACKGROUND

In October 2007, the Joint Committee of the Office of the Comptroller of Currency (OCC), the Federal Reserve Board, the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), and the Federal Trade Commission passed final legislation for sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). They are known as Red Flag Regulations and Guidelines. DMACC is required to comply with these regulations because DMACC One debit cards are issued and students are allowed to pay tuition via a deferred payment plan.

3. DEFINITIONS

3.1. Board of Directors

The collective body of directors or officers charged with managing the operations of DMACC. DMACC Board Policies are available at http://go.dmacc.edu/about/Pages/boardofdir.aspx.

3.2. Customer

A customer is any DMACC student, employee or other individual for which DMACC maintains a "covered account".

3.3. Covered Account

Both new and existing accounts where a continuing relationship exists between DMACC and the customer are considered “covered accounts.” There are two definitions.

3.3.1. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involve or is designated to permit multiple payments or transactions. Examples include a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account.

3.3.2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or mitigation risks.

3.4. Electronic or Soft Copy Format

Electronic or Soft Copy Format refers to any Confidential and Sensitive Information that exists electronically on CDs, DVDs, phones, computers, networks, portable devices, etc.

3.5. Hard Copy Format

Hard Copy Format refers to any Confidential and Sensitive Information that exists physically on paper.

3.6. Red Flags

Red Flags are patterns, practices, or specific activities involving covered accounts that indicate the possible risk of identity theft

3.7. Service Provider

A service provider is any individual, group, or entity that directly provides a service to DMACC or on behalf of DMACC for its customers or clients.

4. SUMMARY OF RESPONSIBILITIES

Red flags procedures are authorized methods for detecting, preventing, and mitigating identity theft. These procedures apply to all personnel that open new or access existing covered accounts. This includes all parties that may come into contact with covered accounts, such as, contractors, consultants, temporaries, and personnel of third party affiliates. DMACC will implement and enforce these procedures, as well as, design more specific or new guidelines as needed.

Only authorized personnel may open new or access existing covered accounts. Employees in the following departments have been approved by DMACC to work with covered accounts as authorized by their supervisor:

Departments	Opens New Covered Accounts	Provides Access to Existing Covered Accounts
1. Human Resources	X	X
2. Information Technology	X	X
3. Physical Plant	X	X

4. Student Services	x	x
5. Marketing		x
6. Iowa Employment Services	x	x
7. Business Office	x	x
8. DMACC Foundation	x	x
9. Dental Lab	x	x
10. Campus Health	x	x
11. Child Care	x	x
12. Continuing Ed	x	x
13. Program Development	x	x
14. Community Workforce Development	x	x
15. DMACC Business Resources	x	x
16. Purchasing	x	x
17. Academic Affairs	x	x

These accounts or records have been identified as examples of covered accounts at DMACC

Account Type	Red Flags Covered Account	Customer Access In -Person	Customer Access On-Line	Customer Access By Phone	Customer Access By Mail	Service Provider Access
1. Debit Cards – DMACC One Card	x	☐	☐	☐	☐	☐
2. Claims Records	☐	☐	☐	☐	☐	☐
3. Direct Deposit Records	x	☐	☐	☐	☐	☐
4. Health Insurance Records	x	☐	☐	☐	☐	☐
5. Life Insurance Records	x	☐	☐	☐	☐	☐
6. Auto Insurance Records	☐	☐	☐	☐	☐	☐
7. Student Records	☐	☐	☐	☐	☐	☐
8. Patient Records	☐	☐	☐	☐	☐	☐
9. Employee Records	☐	☐	☐	☐	☐	☐
10. Service Records	☐	☐	☐	☐	☐	☐
11. Accounts Payable/Receivable Records	x	☐	☐	☐	☐	☐
12. All Data Base Records with CSI	☐	☐	☐	☐	☐	☐
13. DMACC Foundation Records	☐	☐	☐	☐	☐	☐
14. DMACC Child Care Records	x	☐	☐	☐	☐	☐
15. Student Financial Aid Records	☐	☐	☐	☐	☐	☐
16.	☐	☐	☐	☐	☐	☐

5. SUMMARY OF PROCEDURES

Through the course of normal daily business operations authorized personnel may detect identity theft red flags when working with covered accounts. There are several procedures involved in making a reasonable effort to know our customers, accurately open new accounts, and securely access existing accounts. The Identity Theft Red Flag Procedures are arranged according to the following outline:

5.1. **Identification Verification Procedures.** Steps that DMACC personnel take to make a reasonable effort to know individuals opening new accounts or requesting access to an existing account. This includes both document and non-document forms of verification.

5.2. **Red Flags Response Procedures.** Acceptable actions that DMACC Personnel follow when detecting an identity theft red flag.

5.3. **Address Discrepancy Procedures.** Upon notification of an address discrepancy from a Consumer Reporting Agency (CRA), an organization commonly referred to as a credit bureau that prepares credit reports which are used by lenders to determine a potential borrower's credit history. The agency obtains data for these reports from a credit repository and from other sources. DMACC personnel are required to confirm the consumer's address and furnish it to the CRA.

6. IDENTIFICATION VERIFICATION PROCEDURES

Identification verification procedures are necessary for DMACC personnel to form a reasonable belief they know the identity of the individual opening a new covered account or accessing an existing covered account.

Each identified DMACC Department will develop and implement specific identification verification procedures for opening and accessing new and existing covered accounts.

7. RED FLAGS RESPONSE PROCEDURES

Red Flags Response Procedures must be followed when DMACC personnel detect a red flag while working with covered accounts. Each DMACC department and job classification may have different functions with covered accounts. Therefore, each department and job classification's responses to red flags may differ. A detailed list of relevant red flags is broken down by category in Appendix A.

7.1 All DMACC employees that work with covered accounts are authorized to take one or more of the following actions when a red flag is detected. A detailed list of relevant red flags is broken down by category in Appendix A. When all available actions have been exhausted, DMACC employees will escalate the response to their supervisor.

7.1.1. Response to Alerts, Notifications or Warnings from a Consumer Reporting Agency

When presented with an alert, notification or warning from a consumer reporting agency, act quickly in an effort to prevent or mitigate loss for the customer and DMACC. Appropriate responses are as follows:

- Take additional steps to verify identity.
- Flag relevant accounts.
- Monitor account activity.
- Decline account application.

- Validate address.
- Document with a DMACC Incident Report.
- Notify existing customer on record.
- Other

When all available actions have been exhausted, escalate the response to their supervisor.

7.1.2. Response to Suspicious Documents

While working with covered accounts, DMACC employees may be presented documents that appear suspicious or altered in some way. Appropriate responses are as follows:

- Verify using third party resources.
- Verify using existing account records.
- Decline application.
- Decline account access.
- Document with a DMACC Incident Report
- Notify law enforcement (if necessary)
- Notify existing customer on record
- Other

When all available actions have been exhausted, escalate the response to their supervisor.

Response to Suspicious Identifying Personal Information

When a person provides suspicious or inconsistent identifying information while opening or accessing a covered account, the response is as follows:

- Escalate verification to a higher level.
- Decline account application.
- Decline account access.
- Notify existing customer on record.
- Change account access information.
- Change account numbers.
- Document with a DMACC Incident Report.
- Involve law enforcement.
- Other

When all available actions have been exhausted, escalate the response to their supervisor.

7.1.3. Response to Unusual Use of, Suspicious Activity Related to, the Covered Account

Be vigilant in protecting customer accounts when transacting, servicing, or processing business. When suspicious activity or unusual patterns emerge in covered accounts, the appropriate responses are as follows:

- Use Personal Knowledge questions for verification.
- Validate address.
- Decline account access.
- Document with a DMACC Incident Report
- Notify existing customer on record.
- Change account access information.
- Change account numbers.

- Involve law enforcement.
- Other

When all available actions have been exhausted, escalate the response to their supervisor.

7.1.4. Response to Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts

When notified of a security incident from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts must immediately inform senior management and the Identity Theft Prevention Officer. Appropriate responses are as follows:

- Decline account access.
- Close fraudulent account.
- Document with a DMACC Incident Report
- Notify existing customer on record.
- Open new account.
- Do Not Attempt to Collect on the Fraudulent Account from the True Identity.
- Cooperate with law enforcement...
- Other

When all available actions have been exhausted, escalate the response to their supervisor.

8. ADDRESS DISCREPANCY PROCEDURES

8.1. Change of Address Requirements for Credit or Debit Card (DMACC One Card) Issuers

Section 114 of the FACT Act requires financial institutions and creditors that issue credit or debit cards to assess the validity of a request for a change of address before issuing additional or replacement cards. If the request for additional or replacement cards is within thirty (30) days of a request for a change of address, then **do not issue a new card** without performing one of the following actions.

8.1.1. Mail notification to the cardholder of the request at the cardholder's former address and provide the cardholder with a means to promptly report an incorrect address.

8.1.2. Notify the cardholder of the request by another means or by a form of communication previously agreed to by the issuer and the cardholder.

Notices to cardholders regarding requests for change of address, sent electronically or by mail, must be given in a clear and conspicuous manner. According to the Federal Register, dated November 9, 2007, "clear and conspicuous" means reasonably understandable and designed to call attention to the nature and significance of the information presented.

8.2. Notification of Address Discrepancies From Consumer Reporting Agencies

For financial institutions and creditors that use consumer reports, section 315 of the FACT Act requires reasonable policies and procedures when receiving a notice of address discrepancy. First, users must form a reasonable belief that they know the identity of the individual for whom it has obtained a consumer report. Second, the user must reconcile the address of the consumer with the consumer with the consumer reporting agency (CRA), if the user establishes a continuing relationship with the consumer and regularly furnishes information to the CRA.

8.2.1. Requirement to Form a Reasonable Belief

When a consumer report user receives a notice of address discrepancy from a consumer reporting agency (CRA), it must form a reasonable belief that it knows the identity of the consumer. Furthermore, that the consumer report relates to the consumer about whom it has requested the report. This includes comparing information received in the discrepancy notice with information that the user:

8.2.1.1. obtains and uses to verify the consumers identity in accordance with CIP Rules;
8.2.1.2. maintains in its' own records, such as applications, change of address notifications, other consumer account records, or retained CIP documentation; or
8.2.1.3. obtains from third-party resources.

NOTE: If a user cannot establish a reasonable belief that the consumer report relates to the consumer for which it has requested, then the report cannot be used.

8.2.2. Requirement to Provide the Consumers Address to a Consumer Reporting Agency

When a user of consumer reports receives notification of an address discrepancy from a consumer reporting agency (CRA), and has established a reasonable belief that the report in question fits the consumer for which it was requested, it must then confirm the address and furnish it to the CRA. The following are acceptable measures that a user may employ to confirm the address.

8.2.2.1. Verify the address with the person to whom the consumer report pertains.
8.2.2.2. Review its own records of the address provided to request the consumer report.
8.2.2.3. Verify the address through third-party sources.
8.2.2.4. Use other reasonable means.

Response Time. The consumer report user must provide the consumer address to the CRA within the reporting period in which the user's relationship with the consumer is established.

APPENDIX A

IDENTITY THEFT RED FLAGS

The following identity theft red flags have been identified as risks to the covered accounts at DMACC.

Alerts, Notifications or Warnings from a Consumer Reporting Agency

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

1.1.1.2. A customer reporting agency provides a notice of credit freeze in response to a consumer report.

1.1.1.3. A consumer reporting agency provides a notice of address discrepancy.

1.1.1.4. 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) a recent and significant increase in the volume of inquires; b) an unusual number of recently established credit relationship; c) a material change in the use of credit, especially with respect to recently established credit relationships; or d) an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Other

Suspicious Documents

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

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

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

1.1.1.8. 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.

1.1.1.9. An application appears to be altered or forged, or gives the appearance of being reassembled.

Other

Suspicious Identifying Personal Information

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

1.1.1.11. Personal identifying information provided by the consumer 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 the date of birth.

1.1.1.12. 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.

1.1.1.13. 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: a) The address on an application is fictitious, a mail drop, or prison; or b) The phone number is invalid, or is associated with a pager or answering service.

1.1.1.14. The SSN provided is the same as that submitted by other persons.

1.1.1.15. 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.

1.1.1.16. 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.

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

1.1.1.18. 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.

Other

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

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

1.1.1.20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example: a) the majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g.-electronic equipment or jewelry); or b) the customer fails to make the first payment or makes an initial payment but no subsequent payments.

1.1.1.21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: a) non-payment when there is no history of late or missed payments; b) a material increase in the use of available credit; c) a material change in purchasing or spending patterns; d) a material change in electronic fund transfer patterns in connection with a deposit account; or e) a material change in telephone call patterns in connection with a cellular phone account.

1.1.1.22. 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).

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

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

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

Other

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts

1.1.1.26. 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.

APPENDIX B

Acceptable Forms of Identification

Primary Identification	Secondary Identification	Alternative Documents for Elderly or Disabled
☑ US State Picture Driver's License ☑ US State Picture Issued ID Card ☑ US Passport ☑ US Military Picture ID ☑ Federal Picture ID ☑ Alien Registration ☑ Card	☑ Social Security card ☑ Individual taxpayer identification card ☑ EIN ☑ Voter registration, state of residence ☑ Birth Certificate ☑ Credit card ☑ Bank cards ☑ Insurance Cards ☑ State government ID ☑ Local government ID ☑ Company ID ☑ Police identification ☑ Temporary driver license ☑ US Federal Government issued Permanent Resident Card ☑ US Federal Government issued Employment Authorization	☑ Utility Bill: telephone, electricity, gas, water. ☑ Voters Registration ☑ Family Bible, on the "Birth" page the individual's name and date of birth ☑ State issued birth certificate ☑ Company retirement check payable to individual. ☑ Federal or state or county benefit check issued to individual. ☑ Court documents indicating custodian or fiduciary appointment ☑ Social Security Card. ☑ Individual Tax Identification Card