MORTON COLLEGE BOARD POLICY

Illinois Community College District No. 527

TITLE: Identity Theft Prevention **NO.** 8.22

SECTION: Institutional **PAGE:** 1 of 10

I. INTRODUCTION

Morton College (the "College") developed this Identity Theft Prevention Program (this "Program") pursuant to the Federal Trade Commission's Red Flag Rules (the "Red Flag Rules"), which require financial institutions and creditors to develop and implement written identity theft prevention programs as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. 16 C.F.R. §681.1, *et seq*. This Program was developed to detect, prevent and mitigate Identity Theft (as defined below) in connection with the opening of certain Covered Accounts (as defined below) and certain existing Covered Accounts. This Program was developed with the oversight and approval of the Board of Trustees of the College (the "College Board"). After consideration of the size and complexity of the College's operations and account systems, and the nature and scope of the College's activities, the College Identity Theft Program Administrator (the "Program Administrator") determined that this Program was appropriate for the College and, therefore, approved this Program.

II. PROGRAM APPL/CATION & DEFINITIONS

All individual student ("customer") accounts fall within the scope of this Program. Therefore, reasonable policies and procedures for identification, detection and response to Identity Theft will be developed and maintained, and certain College employees will be trained to identify, detect and respond to Identity Theft.

A. Fulfilling the Requirements of the Red Flag Rules

Under the Red Flag Rules, every creditor is required to establish an Identity Theft prevention program tailored to the size, complexity and nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags (as defined below) for new and existing Covered Accounts and incorporate those Red Flags into the program;
2. Detect Red Flags that have been incorporated into the program;
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 customers or to the safety and soundness of the creditor from Identity Theft.

DATE APPROVED BY BOARD OF TRUSTEES: May 20, 2009; February 27, 2019

DATES REVISED:

REVIEWED DATES: January 23, 2019

B, *Red Flag Rules Definitions*

For purposes of this Program, the following terms shall have the meanings set forth below. Where applicable, words used in the present tense include the future tense of the word and words in the singular include the plural form of the word.

A "Covered Account" is: (1) an account that the creditor offers or maintains, primarily for personal, family or household purposes, that involves multiple payments or transactions; and (2) any other account the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from Identity Theft.

"Identifying Information" is defined as any name or number that may be used, alone or in conjunction with any other information, to identify a specific person. Identifying Information specifically includes name, address, telephone number, social security number, date of birth, government issued driver's license or identification number,
or any official identification issued by a government, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's internet protocol address and routing code.

"Identity Theft" is defined as fraud committed using the Identifying Information of another person.

A "Red Flag" is defined as a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

According to the Red Flag Rules, the College is a creditor subject to the Red Flag Rule requirements. The Red Flag Rules define creditors to include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where non-profit and government entities defer payment for goods or services, they too, are to be considered creditors.

Ill. ***SENSITIVE INFORMATION POLICY***

College personnel are encouraged to use common sense judgment in securing confidential and sensitive information. Sensitive information includes, without limitation, credit card information, social security numbers, payroll information, medical

information, birth dates and maiden names. All sensitive information shall be secured when not in use.

IV. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the College considers the types of Covered Accounts that it offers and maintains, the methods it provides to open its Covered Accounts, the methods it provides to access its Covered Accounts, and any previous experiences with Identity Theft. The College identifies the following Red Flags in each of the listed categories:

A. *Notifications and Warnings From Credit Reporting Agencies*

Red Flags:

1. Receiving a report of fraud accompanying a credit report;
2. Receiving notice or a report from a credit agency of a credit freeze on a customer or applicant;
3. Receiving notice or a report from a credit agency of an active duty alert. for an applicant;
4. Receiving notice or a report from a credit agency of an address discrepancy; and
5. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity, such as: (a) an unusual increase in the volume of credit inquiries; (b) an unusual increase in the number of established credit relationships; (c) a material change in the use of credit; or (d) an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

B. *Suspicious Documents*

Red Flags:

1. An identification document or card appears to be forged, altered or inauthentic;
2. An identification document or card on which a person's photograph or physical description is not consistent with the appearance of the person presenting the document;

3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification customer information;
4. Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check;
5. An application for service appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled; and
6. Conflicting information as defined by Title IV of the Higher Education Act of 1965 exists.

C. ***Suspicious Personal Identifying Information Red Flags:***

1. Identifying Information presented is inconsistent with other information the customer provides (for example, inconsistent birth dates and/or social security numbers);
2. Identifying Information presented is inconsistent when compared against external information sources used by the College, for example
   (a) the address does not match any address inthe consumer report; or
   (b) the Social Security Number has not been issued, or is listed on the Social Security Administration's Death Master File;
3. Identifying Information presented is the same as information shown on other applications that were found to be fraudulent, 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;
4. Identifying Information presented is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. The social security number presented is the same as one given by another customer;
6. An address or phone number presented is the same as that of another person;
7. A person fails to provide complete personal Identifying Information on an application when reminded to do so;

DATE APPROVED BY BOARD OF TRUSTEES: May 20, 2009; February 27, 2019

DATES REVISED:

REVIEWED DATES: January 23, 2019

8. A person fails to provide complete personal Identifying Information on an application when reminded to do so;
9. Conflicting information as defined by Title IV of the Higher Education Act of 1965 exists

D. Suspicious Account Activity or Unusual Use of Account

Red Flags:

1. A change of address for a Covered Account is followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date Covered Account;
3. The Covered Account is used in a way that is not consistent with prior use (for example, a material increase in the use of available credit);
4. The Covered Account is used in a way that is not consistent with standard use (for example, the student drops all his/her classes, but retains funds provided);
5. Mail sent to the account holder is repeatedly returned as undeliverable;
6. Receiving notice that a customer is not receiving mail sent by the College;
7. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into account the pattern of usage and other relevant factors);
8. Receiving notice that a Covered Account has unauthorized activity;
9. Breach in the computer system security; and
10. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flags:

1. Notice from a customer, Identity Theft victim, law enforcement agency or other person or entity that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft; and
2. Receiving a report of fraud from the Department of Education.

V. DETECTION OF RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above and associated with the opening of a new Covered Account, College personnel will take the following steps to obtain and verify the identity of the person opening the Covered Account:

1. Require certain Identifying Information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
2. Verify the customer's identity (for instance, review a driver's license or state identification card);
3. Review documentation showing the existence of a business entity;
4. Independently contact the customer; and
5. Comply with Title IV of the Higher Education Act of 1965.

B. Existing Accounts

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

1. Verify the identification of customers 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; and
4. Comply with Title IV of the Higher Education Act of 1965.

VI. RESPONDING TO RED FLAGS - PREVENTING AND MIT/GATING IDENTITY THEFT

In the event College personnel detect any identified Red Flags, College personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft;

2. Contact the customer;
3. Change any passwords or other security devices that permit access to Covered Accounts;
4. Do not open a new Covered Account;
5. Close an existing Covered Account;
6. Reopen a Covered Account with a new number;
7. Notify the Program Administrator for a determination of the appropriate step(s) to take;
8. Notify law enforcement; and/or
9. Determine that no response is warranted under the particular circumstances; and in any event,
10. Comply with Title IV of the Higher Education Act of 1965.

A. Protect Customer-Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect customer Identifying Information:

1. Identify, inventory and track everything that stores or could store sensitive information (whether electronically or conventionally);
2. Inventory sensitive information by type and location;
3. Maintain central log files of sensitive information to monitor activity on network to spot and respond to any attacks;
4. Limit access to sensitive information to only those who need access thereto;
5. Implement appropriate access controls for areas containing sensitive information;
6. Conduct background checks and check references on persons who will have access to sensitive information;
7. Train employees regarding security policies;
8. Impose disciplinary measures for security policy violations;
9. Ensure secure web applications;
10. Ensure computer virus protection is current;
11. Assess whether sensitive information needs to be stored on a laptop and if so, require employees to store laptops in a secure place;
12. Identify all connections to the computers where sensitive information is stored, assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks, ensure security;

13. Disable all network services not used in order to prevent hacking;
14. Ensure that the College's website is secure;
15. Monitor incoming traffic for signs of hacking and outgoing traffic for signs of data breach;
16. Ensure password integrity by ensuring: (a) passwords are not shared or posted, (b) the use of "strong" passwords, (c) passwords of former employees are disabled, (d) passwords of current employees are periodically changed, and (e) vendor-supplied default passwords are changed;
17. Ensure that computers are password protected and computer screens lock after a set period of time;
18. Encrypt sensitive information sent to third parties over public networks;
19. Keep offices clear of papers containing customer information;
20. Keep hard copies of sensitive information and electronic storage devices with sensitive information saved thereon under lock and key except when an employee is working on the file;
21. Require employees put files away, log off their computers, and lock their file cabinets and office doors at the end of the day;
22. Require and keep only the kinds of customer information that are necessary for utility purposes and revise data retention policy to reflect the same;
23. Ensure complete and secure destruction of customer information;
24. When disposing of old computers and portable storage devices, use wipe utility programs;
25. Request only the last four (4) digits of social security numbers (if any);
26. Truncate electronically printed credit and debit card receipts given to customers to no more than the last five digits of the card number and delete the expiration date;
27. Have a plan in place to respond to security incidents; and
28. Comply with Title IV of the Higher Education Act of 1965.

*VII. **PROGRAM UPDATES***

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the College from Identity Theft. At least annually, the Program Administrator will consider the experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention

DATE APPROVED BY BOARD OF TRUSTEES: May 20, 2009; February 27, 2019

DATES REVISED:

REVIEWED DATES: January 23, 2019

methods, changes in types of Covered Accounts maintained and changes in business arrangements with other entities. After considering the foregoing factors, the Program Administrator will determine whether changes to this Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will present the College Board with recommended changes and the College Board will make a determination of whether to accept, modify or reject the changes to this Program.

VIII. PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Committee (the "Committee") for the College. The Program Administrator shall head the Committee, which shall be comprised of two (2) additional individuals, who shall be appointed by the College President. The Program Administrator will be responsible for: (1) administering this Program; (2) ensuring appropriate training of staff on this Program; (3) reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft;
(4) determining which steps of prevention and mitigation should be taken in particular circumstances; and (5) considering periodic changes to this Program.

B. Staff Training and Reports

Staff responsible for implementing this Program shall be trained either by or under the direction of the Program Administrator. Staff shall be trained in Red Flag detection and the responsive steps to be taken when a Red Flag is detected. The Committee shall report to the College Board, at least annually, on the College's compliance with this Program. The report should address material matters related to this Program and evaluate issues such as: (1) the effectiveness of the policies and procedures of the College in addressing the risk of Identity Theft; (2) service provider arrangements; (3) significant incidents involving Identity Theft; and (4) the College's response and material changes to this Program.

C. *Service Provider Arrangements*

In the event the College engages a service provider to perform an activity in connection with Covered Accounts, the College will take the following steps to ensure

the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft:

1. Require, by contract, that service providers have Red Flags policies and procedures in place; and
2. Require, by contract, that service providers review this Program and report all Red Flags to the Program Administrator.