

Identity Theft Prevention Program

I. Title of Policy

Identity Theft Prevention Program (the “Program”).

II. Purpose and Objective

The County College of Morris is committed to preventing fraud associated with the misuse of identifying information (identity theft) of staff students, faculty, or others who have relationships with the College to obtain educational or financial services. This is accomplished through systematic detection of “Red Flags,” prompt response to potential incidents, and regular evaluation and updates to the Program.

III. Definitions

1. **Account:** A relationship established with an institution by a student, employee, or other person to obtain educational or financial services.
2. **Identity theft:** Fraud committed or attempted using another individual identifying information without authority.
3. **Covered account:** Any account primarily for personal, family, or household purposes, involving multiple payments or transactions, including student and employee accounts, as well as any College account or database vulnerable to identity theft.
4. **Red Flag:** A pattern, practice or specific activity indicating the possible existence of identity theft.
5. **Program Administrator:** The College’s Director of Budget and Compliance, responsible for oversight and administration of the Program.
6. **Identifying information:** Data that identifies a specific person, such as name, address, date of birth, Social Security number, drivers’ license number, passport number, student or employee ID, IP addresses, etc.
7. **Service Provider:** Any person or entity providing services directly to the College.

IV. Regulatory Authority

This Program is developed in accordance with the Federal Trade Commission’s Red Flags Rule (sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003), and adheres to all applicable federal and state regulations.

V. Policy Statement

The College has designed a Program to reasonably detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program includes:

1. Identification and incorporation of relevant Red Flags for new and existing covered accounts.
2. Procedures for detecting Red Flags in day-to-day operations.
3. Established responses to Red Flags to prevent and mitigate identity theft.
4. Periodic review and update to the Program to address evolving risks and circumstances.

The Program supplements existing College policies designed to manage foreseeable risks and circumstances.

VI. Program Administration

Ultimate responsibility for the identity theft prevention initiative lies with each office and employee handling covered accounts or sensitive databases. The Executive Vice President for Business & Finance oversees the Program, with day-to-day administration and compliance conducted by the Director of Budget and Compliance (the “Program Administrator”).

The Program Administrator is responsible for:

1. Administering the Program and ensuring staff receive appropriate training.
2. Reviewing and investigating reports of potential Red Flag incidents.
3. Coordinating College responses to identity theft incidents.
4. Recommending updates to the policy in response to changing risks.
5. Managing and reviewing all requests for access to sensitive information, such as Social Security numbers

VII. Covered Accounts

The College has identified several types of covered accounts: accounts administered by the College and accounts administered by service providers.

1. The covered accounts administered by the College are:
 - a. Student accounts;
 - b. Employee accounts; and
 - c. Employee records.
2. The covered accounts administered by service providers are:
 - a. Payment plan accounts;
 - b. Collection accounts; and
 - c. Other external covered accounts.

VIII. Identification of Red Flags

Potential Red Flags may include, but are not limited to:

1. Alerts notifications, or other warnings from consumer reporting agencies or service providers, such as fraud detection services.
2. Suspicious documents or information presented by individuals that appear altered or forged or where a person’s photograph or physical description is not consistent with the person presenting the document, or the information is not consistent with existing student information.
3. Unusual or suspicious account activity.
4. Requests from non-college e-mail accounts.
5. Requests to mail information to addresses not on file.
6. Notifications from students, law enforcement, or others regarding suspected identity theft.

IX. Detection of Red Flags

The Program will detect Red Flags by:

1. Obtaining and verifying identifying information during account opening.
2. Authenticating identity when students/employees request information in-person, by phone or by e-mail.
3. Verifying billing address or banking information changes for existing accounts.
4. Requiring written address confirmation for employment background or credit checks.
5. Confirming the accuracy of addresses when notified of discrepancies by reporting agencies.

X. Response to Detection

When Red Flags are detected, the following actions may be taken to prevent or mitigate identity theft:

1. Monitoring a covered account for evidence of identity theft.
2. Denying access to or closing the affected account until Red Flags are resolved.
3. Contacting the affected individual and, if appropriate, issuing a new student identification number;
4. Changing passwords, security codes, or other access credentials.
5. Opening a new account with a different number or withholding new account creation as needed.
6. Notifying the Program Administrator to determine additional steps.
7. Contacting law enforcement authorities, if warranted.
8. Documenting and determining if no response is necessary based on the situation.

XI. Reporting and Documentation

Any detected incident of identity theft must be reported by the relevant office manager or director using an identity theft detection form, which is then submitted to the Program Administrator for evaluation.

All instances are also reported to the Committee on Audit of the Board of Trustees. The Program Administrator prepares an annual report outlining the state of the Program and recommendations for improvement, which is shared with the Executive Vice President for Business & Finance.

XII. Protecting Identifying Information

The Director of Network User Services & Chief Information Security Officer, in conjunction with Information Technologies and under the oversight of the Executive Vice President of Business and Finance, is responsible for ensuring these safeguards are implemented, monitored, and routinely reviewed to maintain the security and confidentiality of all identifying information:

1. Securely destroy all paper documents containing identifying information no longer needed, following a documented disposal policy, such as shredding confidential information prior to disposal.
2. Limit access to Social Security numbers and other sensitive data to authorized staff approved by the Program Administrator, granting access only for legitimate College business needs.

3. Retain only necessary information for College purposes, regularly reviewing data holdings to ensure outdated records are disposed of securely.
4. Store physical records in secure areas with restricted access; maintain an inventory of servers or computers containing customer information.
5. Ensure that office computers with access to covered account information are password protected.
6. Ensure that electronic customer information is entered only into secure, password-protected systems with access based on business need and require password protection on all computers accessing covered accounts. Passwords must comply with National Institute of Standards and Technology (NIST) guidelines.
7. Use secure connections (such as encryption and secure servers) when transmitting or accessing data outside the College network.
8. Completely and securely destroy electronic files containing identifying data when obsolete, including permanently erasing information from computers, diskettes, magnetic tapes, hard drives, or other electronic media before resale, transfer, recycling, or disposal.
9. Maintain up-to-date antivirus software and install software patches promptly to address vulnerabilities; implement firewall and filtering technologies to protect against unauthorized access.
10. Back up data regularly and store backups in secure, off-site locations to ensure data integrity and system recovery capability.
11. Promptly report any loss or theft of customer information or media to the Program Administrator for incident management.
12. Ensure the College website is secure or clearly notify users if it is not, reflecting web security best practices.

XII. Staff Training

All College employees responsible for handling covered accounts are trained under the direction of the Program Administrator on the detection, reporting, and mitigation of Red Flags.

XIV. Oversight of Service Provider Arrangements

The College ensures that service providers handling covered accounts comply with reasonable policies and procedures to detect, prevent, and mitigate the risk of identity theft.

XV. Program Review and Updates

The Program Administrator regularly reviews and recommends updates based on:

1. College experiences with identity theft.
2. New methods and techniques of identity theft.
3. Changes in detection, prevention, or mitigation technologies, and methods.
4. Modifications in account types or business arrangements.
5. The effectiveness of the Program, service provider compliance, incident management, and material changes are all evaluated annually.