Monroe Community College
STATE UNIVERSITY OF NEW YORK

2.1P Identity Theft Prevention Procedure

Category: Administration

Name of Responsible Office: Administrative Services

Title of Responsible Executive: CFO/Vice President, Administrative Services

Date Established: June 8, 2009

Date Last Approved: June 11, 2024

Process

Description of Process

Two types of accounts must be monitored:

1. Accounts that are ***designed to permit multiple payments or transactions*** (i.e. periodic crediting and debiting activity), such as Student Accounts, accounts associated with student lending activity (Perkins, FFELP, PLUS), etc.
2. Accounts for which there is a ***reasonably foreseeable risk of identity theft*** such as email accounts or Banner accounts.

Identify Red Flags

The following categories, while not all-inclusive, are considered Red Flags:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as a notice of credit freeze, fraud alert, or address discrepancy;
- Presentation of suspicious documents or personal identifying information, such as inconsistent address or name spelling, alterations, or a photo that does not appear to match the student;
- Unusual use of, or other suspicious activity related to, a Covered Account, such as a suspicious address change request or the use of an account that is inconsistent with the account history or the known attributes of the account holder;
- Notice from students, faculty, staff, and victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft or information security breach in connection with Covered Accounts held by the campus. Such notice must be reported to Public Safety.
- Any type of security breach involving the theft of personal information.

Detect Red Flags

The following categories, while not all-inclusive, are considered in the detection of Red Flags:

- Verifying identifying information upon opening accounts or authorizing access to accounts;
- Authenticating changes to identifying information (e.g. name and address changes); and
- Monitoring account activity.

Respond to Red Flags

The following categories, while not all-inclusive, may be considered appropriate responses to identified Red Flags:

- Close monitoring of the account;
- Contacting the student;
- Changing access information such as passwords or security codes;
- Freezing an account; or
- Notifying Public Safety/law enforcement.

Identification of Covered Accounts; Responsible Staff; Red Flags; Responses

Covered Account

Student Records

Responsible Staff: Staff in: Admissions, Student Accounts, Records & Registration, Financial Aid, Human Resources, Controller's, Counseling and Disability Services, Advisement and Transfer Services, PSTF, Public Safety, and Testing Services

- **Red Flag 1**: Suspicious ID presented by a student who is trying to access or alter account.
    - Response: Deny access to account until the student's identity has been established through acceptable means.
- **Red Flag 2**: A change of address (home or email) request occurs under suspicious circumstances. Example – a student requests change of address then requests a refund distribution.
    - Response: Ask student to come in and personally verify address and any suspicious usage activity.
- **Red Flag 3**: A change of name request occurs without appropriate identification and/or documentation.
    - Response: Deny name change request until student's identity has been established through acceptable means and/or appropriate documentation is provided.
- **Red Flag 4**: A student refund check as listed on the positive payee system appears altered.
    - Response: Deny check and report to Public Safety. Contact student to inform them of any suspicious activity.
- **Red Flag 5**: Student's tax documents or other documents containing personally identifiable information (PII) sent to erroneous shared folder instead of financial aid mailbox.
    - Response: Determine if folder was accessed by unauthorized individuals. Assemble data breach team (if formed). Notify US Department of Education if breach suspected. Prevent future creation of folders.

Financial Aid Account

Responsible Staff: Financial Aid Staff

- **Red Flag 1**: Department of Education selects student's FAFSA for verification.
    - Response: Collect supplemental information from student and resolve any conflict between FAFSA and supplemental information provided by student.

- **Red Flag 2**: Student submits multiple FAFSAs containing conflicting information.
    - Response: Contact student to resolve conflict and verify information.

Email Accounts

Responsible Staff -Technology Services; Public Safety

- **Red Flag**: Notification from student or employee that email has been accessed without authorization.
    - Response(s): Technology Services will invalidate password immediately, report to Chief Information Officer, Chief Information Security Officer (CIO/CISO) and Public Safety, and place a litigation hold on the account if requested. The employee should reset their password using the self-service tool.

Banner Accounts

Responsible Staff: Technology Services; Public Safety

- **Red Flag 1**: Notification from student or employee that Banner has been accessed without authorization.
    - Response(s): Technology Services will invalidate password immediately and report to CIO/CISO and Public Safety. The employee should reset their password using the self-service tool.
- **Red Flag 2**: Multiple failed login attempts.
    - Response: Account will be locked after five (5) failed login attempts.
- **Employee Password Reset**:
    - Password reset is self-service. With the provision of appropriate identification (including M-number) Technology Support Center will assist employees with the process if necessary.
- **Student Password Reset**:
    - Password reset is self-service. Registration & Records or the Student Technology HelpDesk will provide direction to students on the password reset process.

Deferred Tuition Payment Plan

Responsible Party: Outsourced to third party service provider – Nelnet Business Solutions

- Response: Obtain/review Nelnet's Identity Theft Prevention.

Contact Information

Office of Administrative Services

History

Item	**Date**	**Explanation**
Established	June 8, 2009	

Item	Date	Explanation
Three-year review	2014	No change
Three-year review	2017	Recommended updates to properly identify responsible offices and reflect current practice.
Recommended revisions approved	September 9, 2018	College Officer Approval
Five-year review	2024	Recommended minor revisions