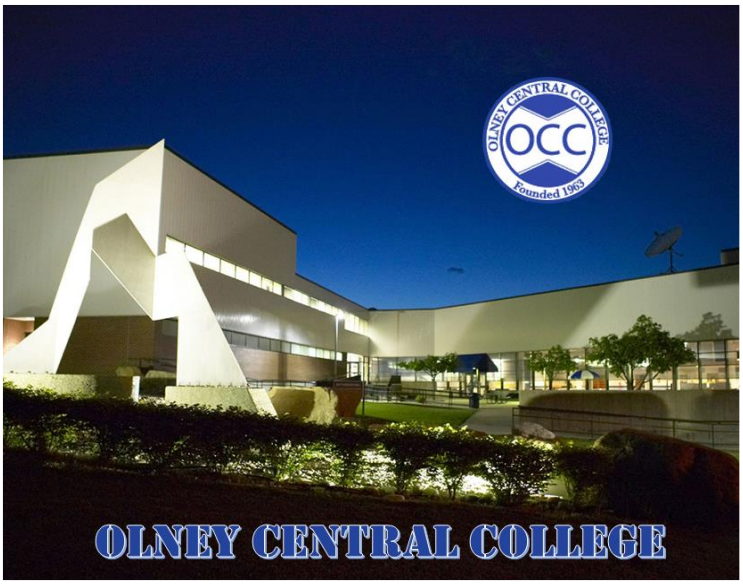
ILLINOIS EASTERN COMMUNITY COLLEGES

Identity Theft Prevention Program



Our mission is to deliver exceptional education and services to improve the lives of our students and to strengthen our communities.

Approved by Cabinet: April 4, 2023 **Approved by Board of Trustees: April 25, 2023**

Background

The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) issued regulations (Red Flags Rule) requiring financial institutions and creditors to develop and implement written identity theft prevention programs. The Red Flags Rule was developed pursuant to the Fair and Accurate Credit Transaction (FACT) Act of 2003. Under the Rule, financial institutions and creditors with covered accounts must have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. The Red Flags Rule became effective January 1, 2008, with a mandatory compliance date of November 1, 2008; however, on October 22, 2008, the FTC granted a delay of enforcement of the new Red Flags Rule until May 1, 2009.

IECC Identity Theft Prevention Program Requirement

Illinois Eastern Community Colleges participates in the Direct Student Loan Program, offers institutional loans to students, and administers a tuition payment plan that allows qualified students to pay their tuition and fees throughout the semester. Therefore, IECC is a creditor and student accounts are covered accounts subject to the Red Flags Rule which requires IECC to develop and implement an identity theft prevention program.

The Red Flags Rule allows Illinois Eastern Community Colleges to design and implement an identity theft prevention program that is appropriate to our size, complexity, and the nature of our operation. Programs must contain reasonable policies and procedures to:

- identify relevant "Red Flags" and incorporate them into the program;
- detect the red flags that the program incorporates;
- respond appropriately to detected red flags to prevent and mitigate identity theft; and
- ensure that the program is updated periodically to reflect changes in risks.

Definitions

Red Flag – A red flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Identity Theft – Identity theft is a fraud committed or attempted using the identifying information of another person without authority.

Covered Account – A covered account is a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made periodically over time such as a tuition or fee installment payment plan. Student accounts and loans administered by IECC are covered accounts.

Creditor – A creditor is defined as someone who regularly extends, renews, or continues credit. Illinois Eastern Community Colleges is considered a creditor due to our participation in the following activities:

- Participation as a school in the Federal Direct Student Loan Program;
- Offering institutional loans to students, faculty, or staff;

- Offering a plan of payment or fees throughout the semester, rather than requiring full payment at the beginning of the semester.

Personal Information – Personal information is identifying information which is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, computer's Internet Protocol address, or routing code.

Red Flags

Red Flags are relevant patterns, practices, and specific activities that signal possible identity theft and fall in the following five categories:

- alerts, notifications, or warnings from consumer reporting agencies;
- suspicious documents;
- suspicious personally identifying information, such as a suspicious address change;
- unusual use of, or other suspicious activity related to, a student or employee account; and
- notices from students, employees, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with student accounts or employee payroll information held by IECC.

Identification and Examples of Red Flags

In order to identify relevant Red Flags, IECC has reviewed the types of accounts offered and maintained, the methods provided to open and access these accounts, and previous experiences with identity theft. IECC identified the following twenty-six (26) Red Flags in the below five categories.

Alerts, Notifications, or Warnings from Consumer Reporting Agency

- If a fraud or active duty alert is included with a consumer report.
- If a consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- If a consumer reporting agency provides a notice of address discrepancy.
- If a consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an application, such as:
    - A recent and significant increase in the volume of inquiries;
    - An unusual number of recently established credit relationships;
    - A material change in the use of credit, especially with respect to recently established credit relationships, or
    - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

- If documents provided for identification appear to have been altered, forged or inauthentic.
- If the photograph or physical description on the identification is not consistent with the appearance of the student or employee presenting the identification.
- If other information on the identification is not consistent with the information provided by the student or employee.
- If other information on the identification is not consistent with readily accessible information that is on file with Illinois Eastern Community Colleges, such as a signature on a registration form or other document.
- If a document appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

- If personal identifying information provided is inconsistent when compared against external information sources used by Illinois Eastern Community Colleges such as inconsistent birth dates or addresses.
- If personal identifying information provided by the student or employee is not consistent with other personal identifying information provided by the student or employee. For example, there is a lack of correlation between the SSN range and the date of birth.
- If personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by Illinois Eastern Community Colleges. For example;
    - The address on the document is the same as the address provided on a fraudulent document, or
    - The phone number on the document is the same as the number provided on a fraudulent document.
- If personal identifying information provided is a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Illinois Eastern Community Colleges. For example:
    - The address on the document is fictitious, a mail drop or a prison; or
    - The phone number is invalid.
- If the SSN provided is the same as that submitted by other students or employees.
- If the address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other students or employees.
- If the student or employee fails to provide all required personal identifying information on a document or in response to notification that the information is incomplete.

- If personal identifying information provided is not consistent with personal identifying information that is on file with Illinois Eastern Community Colleges.
- If Illinois Eastern Community Colleges uses challenge questions, the student or employee cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Student Account

- If shortly following the notice of a change of address for a student account, Illinois Eastern Community Colleges receives a request for the addition of other authorized users on the account.
- If a student account is used in a manner commonly associated with patterns of fraud. For example, the student fails to make the first payment or makes an initial payment but no subsequent payments.
- If a student account is used in a manner that is not consistent with established patterns of activity on the account. For example, nonpayment when there is no history of late or missed payments or a material change in usage patterns.
- If a student account that has been inactive for a reasonably lengthy period of time is used.
- If mail sent to the student is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the student's account.
- If Illinois Eastern Community Colleges is notified that the student is not receiving paper account statements.
- If Illinois Eastern Community Colleges is notified of unauthorized charges or transactions in connection with the student's account.

Notices from Students, Victims of Identity Theft, Law Enforcement Authorities or Others

- If Illinois Eastern Community Colleges is notified by a student, a victim of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with student accounts held by IECC.

Detection and Response to Red Flags

Detection

In order to detect any of the Red Flags identified above associated with student accounts, IECC staff will take the following steps to obtain and verify the identity of a student by:

- Requiring certain identifying information such as name, date of birth, academic records, home address, mother's maiden name, or other identification; and
- Verifying the student's identity at time of issuance of any student records, academic information or financial aid by reviewing driver's license or other government-issued photo identification.

For existing student accounts, IECC staff will take the following steps to monitor transactions on an account by:

- Verifying the identification of students if they request information in person, via telephone, via facsimile or via email;
- Verifying the validity of requests to change billing address by mail or email and providing the student with a reasonable means of promptly reporting incorrect billing address changes; and
- Verifying changes in banking information given for billing and payment purposes.

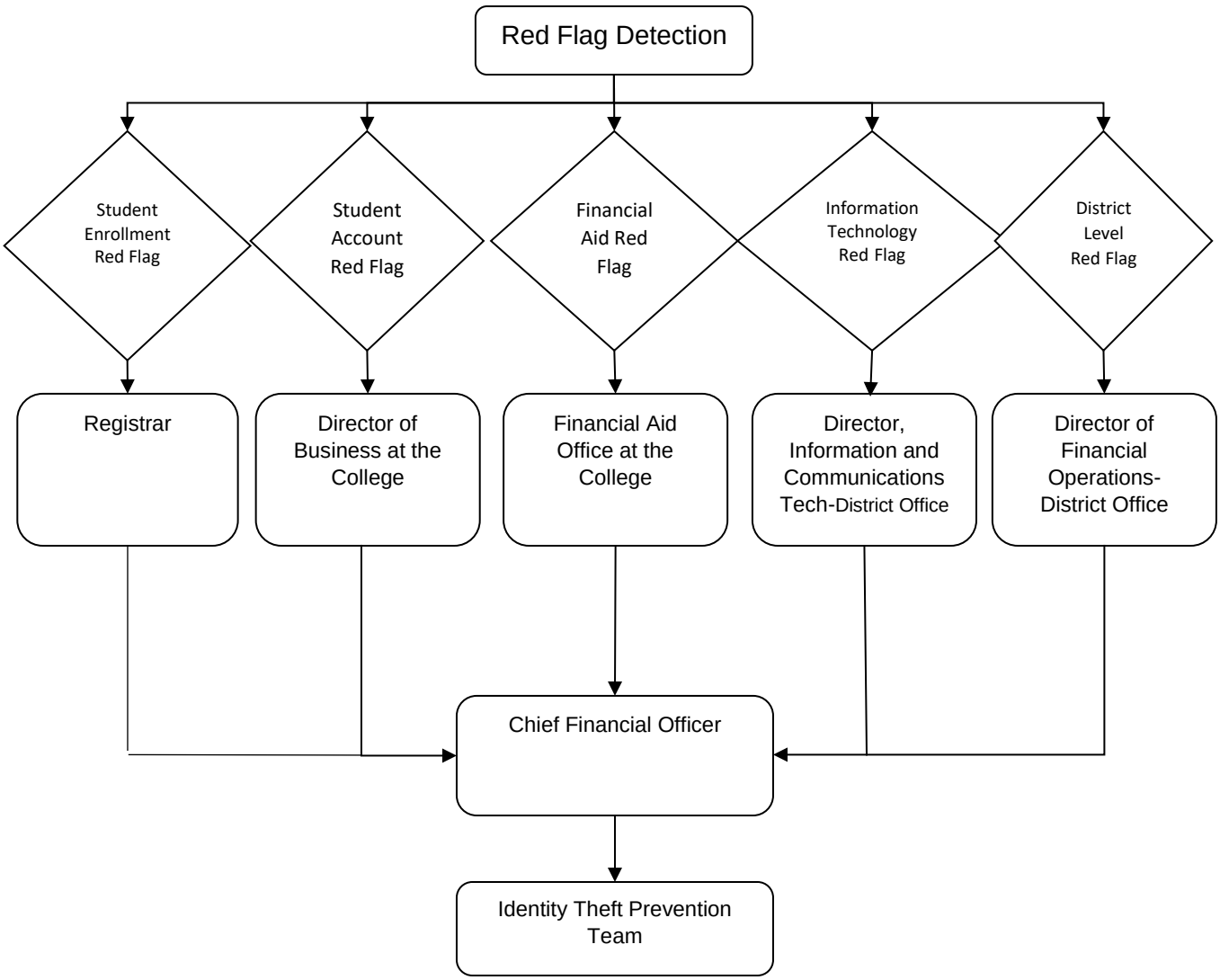
IECC staff will monitor any proposed changes to employee payroll accounts by requiring verbal verification in addition to any required forms from the employee making the proposed change.

Response

In the event IECC staff detects any identified Red Flags, action steps may include, but are not limited to, one or more of the following, depending on the degree of risk posed by the Red Flag:

- Monitoring a student account for evidence of identity theft;
- Contacting the student;
- Changing any passwords, security codes or other security devices that permit access to a student account;
- Reopening a student account with a new account number;
- Providing the student with a new identification number;
- Not opening a new student account;
- Closing an existing student account;
- Not attempting to collect on a student account or not selling a student account to a debt collector;
- Notifying law enforcement;
- Filing or assisting in filing a Suspicious Activities Report; or
- Determining that no response is warranted under the particular circumstances.

Any employee who detects a Red Flag associated with student enrollment will notify the IECC Registrar. Employees who detect a Red Flag with a student account will notify the college's Director of Business or the Director of Financial Operations at the District Office. The Financial Aid Office shall be notified if any Red Flag is detected within the financial aid area. Any Information Technology related Red Flag will be reported to the Director of Information and Communications Technology. All detections of Red Flags will be reported to the College Deans and the Associate Dean of Admissions & Records. The Identity Theft Prevention Team will review any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft. The flowchart below outlines this reporting process:



Identity Theft Prevention Team

Amber Malone	Associate Dean of Admissions & Records
Libby McVicker	Program Director of Grants & Compliance
Bonnie Chaplin	Director of Financial Operations
Alex Cline	Director of Information and Communications Technology
Steve Patberg	Registrar
Krystle Riggle	Program Director of Financial Aid
Doug Shipman	Director of Business

Prevention and Protection of Student and Employee Identifying Information

In order to prevent and mitigate identity theft, IECC will take the following steps with respect to internal operating procedures to protect student identifying information:

- Ensure IECC website is secure or provide clear notice that the website is not secure;

- Ensure complete and secure destruction of paper documents and computer files containing student account information or employee payroll information when a decision has been made to no longer maintain such information;
- Ensure office computers with access to student account information or employee payroll information are password protected;
- Limit use of social security numbers;
- Ensure computer virus protection is up to date;
- Implement and maintain cyber security managed detection and response(MDR) and managed risk(MR) systems to improve overall cyber security posture.
- Require and keep only student or employee information that is necessary for college purposes; and
- Provide identity theft information on IECC's webpage in the Consumer Information/Student Right to Know section.
- Provide Release of Student Information Guidelines to new and current staff who work with student accounts, student records, financial aid or other personal identifiable information.

Program Administration

Program Oversight and Reports

The Identity Theft Prevention Program is the responsibility of the administration of the District Office and the Colleges. Approval of the initial program and policy must be appropriately documented and approved by the Cabinet and the Board of Trustees.

The Associate Dean of Admissions & Records at the District Office is responsible for developing and implementing the program. An Identity Theft Prevention Team was formed and is responsible for monitoring and updating the program. The Identity Theft Prevention Team is responsible for ensuring appropriate training of IECC staff on the program, for reviewing any staff reports regarding the detection of Red Flags, and for reviewing the steps for preventing and mitigating identity theft. The Associate Dean of Admissions & Records will report annually, or as needed, to the Cabinet on the effectiveness of the program, significant incidents involving identity theft and IECC's response, and recommendations for material changes to the program. The Associate Dean of Admissions & Records will update the program as necessary.

Training

IECC staff with responsibilities in the areas of student accounts, student records, and financial aid will receive annual training as part of this prevention program. Training shall include detection and recognition of red flags, appropriate handling of notices, and action steps. Staff training shall be conducted for any other employees and all new employees for whom it is reasonably foreseeable may come into contact with student accounts, employee payroll information, or personally identifiable information. To ensure maximum effectiveness, employees will continue to receive additional training as changes to the program are made.

Service Provider Arrangements

In the event IECC engages a service provider to perform an activity in connection with one or more student accounts, IECC will take the following steps to make every reasonable effort that

the service provider performs its activity in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

1. Provide service providers with IECC's Identity Theft Prevention Program; and,
2. Request service providers to certify that they have received, and will abide by IECC's Identity Theft Prevention Program, and will report any Red Flags to the IECC employee with primary oversight of the service provider.

Program Updates

The Identity Theft Prevention Team will periodically review and update this program to reflect changes in risks to students and the soundness of IECC from identity theft. The program will be re-evaluated to determine whether all aspects are up to date and applicable in the current business environment. Red flags will be reviewed and may be revised, replaced, or eliminated as determined.

Program Status and Report as of March 2023

In February 2023, the Identity Theft Prevention Team reviewed and updated the prevention program, as necessary. The Team will continue to annually review the program, and training will be provided to appropriate administration, staff, and/or faculty. The training provided is Vector Solutions/Safe Colleges FACTA: Identity Theft and Consumer Protection training. Documentation of completed training documents are kept with the Program Director of Grants and Compliance.