Identity Theft Prevention Program/Red Flags Rule

Background

In response to the growing threat of identity theft and the North Carolina Identity Theft Protection Act (NCITPA) Isothermal Community College adopted a Social Security Number and Personal Identifying Information Policy in May 2008.

In 2003, the United States Congress passed the Fair and Accurate Credit Transactions Act (FACTA). Public Law 108-159. This amendment to the Fair Credit Reporting Act dictated that the Federal Trade Commission (FTC) promulgate rules to address identity theft. The rules promulgated by the FTC (Red Flag Rules) require any financial institution and creditor that holds any type of consumer account or other account for which a potential risk of identity theft exists to create and implement a written Identity Theft Prevention Program in order to prevent identity theft associated with new and existing accounts. This Identity Theft Prevention Program is appropriate to the size and complexity of the College and the nature and scope of the College's activities.

Purpose

The College adopts this Identity Theft Prevention Program to enact reasonable policies and procedures to protect students, employees, and other persons with whom the college is affiliated from damages associated with the compromise of sensitive personal information.

Definitions

1. **Creditor –** Any organization, including community colleges, which regularly:
    a. extends, renews, or continues credit;
    b. arranges for someone else to extend, renew, or continue credit; or
    c. is the assignee of a creditor involved in the decision to extend, renew, or continue credit.
2. **Credit -** Deferral of payment of a debt incurred for the purchase of goods or services, including educational services.
3. **Covered account –**An account with a creditor used by individuals, families, or households which involves multiple payments to that creditor. Examples include emergency loan accounts, scholarships which could involve repayment if the terms of the scholarship are not met, and deferred payment accounts approved by colleges' trustees.
4. **Financial institution –**Typically a bank, credit union, or other entity that holds for an individual an account from which the owner can make payments, and transfers.
5. **Identifying information –**Information which alone, or in combination with other information, can be used to identify a specific individual. Identifying information includes, identification card number, employer or taxpayer identification number, biometric data, unique electronic identification numbers, address or routing code, or certain electronic account identifiers associated with telephonic communications.
6. **Identity theft –** A fraud attempted or committed using identifying information of another person without proper authority.
7. **Red Flag –** A pattern, practice, or specific activity which indicates the possibility of identify theft.

8. **Sensitive information –** Personal information belonging to any student, employee, or other person with whom the College is affiliated.
9. **Service provider –** Person providing a service directly to the financial institution or creditor.

Scope

Activities in which the College is often involved that require compliance with the Red Flag Rules and/or
protection of identifying information include, but not limited to:

1. Utilization of deferred payment plans as authorized by 2D.SBCCC.0201;
2. Maintaining an account for students from which the student can authorize payments for goods and services such as tuition, fees, books and supplies using FA Link;
3. Using debit/credit card accounts;
4. Persons attempting to access academic or financial information;

Identification of Relevant Red Flags/Identity Threats

The College must identify which Red Flags/identity threats are relevant to the institution considering the size of the College and the complexity of duties and activities. The Red Flags/identity threats categories and related examples are based on the types of accounts the College offers and maintains, the methods used to create accounts, methods of accessing information, and previous experiences the College has had with identity theft. Additionally, the College will incorporate the Red Flags/identity threats deemed relevant from incidents the College has experienced or other local colleges have experienced, methods of identity theft that the College has identified that reflect changes in identity theft risks, and guidance from senior administrators.

Red Flag/Identity Threats Category	Examples of Red Flags/Identity Threats
Alerts, notifications, or other warnings received from the Attorney General's Office, consumer reporting agencies, service providers such as fraud detection services, or other entities used to collect data	A consumer reporting agency issues a fraud or active duty alert.
	A consumer reporting agency provides a notice of address discrepancy.
	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:

	1. A material change in the use of credit, especially with respect to recently established credit relationships; or 2. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
The presentation of suspicious documents	Documents provided for identification appear to have been altered or forged.
	The photograph/physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
	Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
	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.
	An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
The unusual use of, or other suspicious activity related to, a covered account	Any student account is used in a manner commonly associated with known patterns of fraud.

For example: The customer fails to make the first payment or makes an initial payment but no subsequent payments.

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) Nonpayment 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.

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.

Mail sent to the student, sponsor, employee, WNCW member, vendor or other persons with whom the college is affiliated is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

The College is notified that the customer is not receiving paper account statements.

The College is notified of unauthorized charges or transactions in connection with a customer's covered account.

	A customer initiates multiple address changes over a short period of time.
	A customer is attempting to access information about a deceased student.
	The College 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.
Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the college	A student, borrower, law enforcement personnel or service provider notifies the college of unusual activity related to a covered account. This may include discrepancies in social security number to a named, address difference, or data between the College and the responsible party.
	A student or customer does not know personal information that they should know, i.e. social security number, date of birth, student identification number.
Requests for access to information	A person attempts to access student information without proper identification.
Access to Information	Open access to information due to multiple locations, multiple records, multiple account managers, and multiple off-campus instructors or other

	representatives who collect demographic information.
	Authorized agencies to help in collection of accounts such as collection agencies and government agencies that assist with collections are provided with sensitive data.
	Breach of security with computer system and/or E-mail system.
Payment Process	Phone-in payments may have the risk of compromising banking information.
	Credit card information stored with the daily deposits,
	Accepting students' and other customers' checks that have financial and demographic information on them.

Detecting Red Flag/Identity Threats

1. The College collects, uses and/or discloses identifying information as permitted by the applicable laws and institutional policies and only in furtherance of legitimate college business.
2. Procedures should be in place to verify a person's identity when processing any activities such as bookstore transactions, and account payments/inquiries.
3. Receipt of notifications from service providers of red flag criteria (i.e., discrepancies in social security number to name, address differences, etc.) should be disseminated to proper personnel.
4. Receipt of notification of suspicious activity by student, law enforcement, or borrower should be disseminated to proper personnel.
5. The Department of Education randomly selects students for financial aid verification. These students are verified by financial aid staff.
6. Any report by an employee that laptops and/or computer equipment with sensitive data have been lost or stolen need to be addressed by proper personnel.
7. The College should appropriately process changes to sensitive information (i.e., record name changes, social security number changes, etc.).

8. The College should perform routine diagnostics on firewalls and the security of electronic data portals
9. Security scans should be done at regular intervals to detect any possible breaches.
10. The College must caution employees to be aware of their surroundings when talking with students or discussing a student with another College employee.

Preventing and Mitigating Identity Theft

1. **Employee Accounts**
    a. Documentation will be required to verify employee identity prior to processing for employment and/or payment. Any discrepancies of information should be addressed by College personnel through a verification process assuring the prospective employee is indeed who they claim to be.
2. **Forms, Document, and Records**
    a. Any form that requires a personal identifier must label input fields appropriately and avoid the use of social security numbers. Forms which require that SSNs be used under applicable state and federal laws are exempt.
    b. Identifying information may not be displayed on materials or documents that are widely seen by others without the knowledge of the person. Materials or documents may include but not limited to identification cards, badges, time cards, employee rosters, student rosters, bulletin board postings, grade postings, web sites, and other materials.
    c. Documents that include identifying information must be stored in a secure place. When possible, records containing identifying information, including back-ups, should be protected during storage by encrypting the numbers in electronic records or storing records in other media forms in locked cabinets.
    d. When possible, printed reports and other documents should not list identifying information. If identifying information needs to be included in printed documents, such documents should be accessible only to employees that require the information for the performance of their duties.
    e. Printed documents that contain identifying information must be disposed of by burning, pulverizing or shredding in an approved instrument when the documents are no longer needed or upon the expiration of their retention based on the applicable NCCCS Records, Retention and Disposition Schedule.
3. **Computers/Internet/E-mail/Mail**
    a. The storage of identifying information on local computers, laptops, portable devices or home/personal computers and/or electronic devices is prohibited unless specifically approved by the Chief Information Officer and appropriate Vice President.
    b. Transmission of identifying information is limited.
    c. Electronically stored information (files and records) that contain identifying information must be permanently deleted when they are no longer needed or upon the expiration of their retention based on the applicable NCCCS Record Retention and Disposition Schedule.
4. **Third Party**
    a. Employees may not intentionally communicate or otherwise make available to the general public a person's identifying information. Identifying information is strictly confidential. Students identifying information may not be disclosed except as permitted by FERPA.

b. Disclosures of identifying information to the College's vendors, contractors, or other external entities must be in accordance with College policy and/or state and federal laws.
c. In case of a court order, warrant, or subpoena for identifying information for an employee, the employee should immediately contact the Director of Human Resources; for a student the employee should contact the Registrar.
d. Third party agencies should make available to the College a listing of their policies and procedures for handling of accounts and the protection of sensitive data and promptly notify the College of any possible breaches. This includes, but is not limited to, agencies contracted by the College for handling of student reports/information, agencies contracted by the College for collection of accounts, the College's credit card merchant provider(s), and agencies who handle employee information for the College and/or employee's benefit. The College should also evaluate periodically methods of transferring sensitive data to third parties.

5. **FERPA (Family Educational Rights and Privacy Act)**
   a. See Student Records Policy. (Appendix A Student Handbook or Policy 601-02-07AP)
6. **Payment Card Data Security Standard Compliance**
   a. The College should remain PCI Compliant.
7. **Training of Staff**
   a. All employees with access to sensitive data should be trained and/or informed of risks and liabilities associated with data loss and/or theft and the responsibility that lie with each employee to keep sensitive data secure.
8. **Dean/Director Responsibilities**
   a. The Dean/Director is responsible for overseeing compliance and training for employees within their department related to the collection, use, disclosure, security, and disposal of identifying information.
   b. The Dean/Director will conduct a review as needed to identify relevant patterns, protocol, and specific forms of activity that signal possible red flags/ identity theft. Reviews, with the actions taken, should be maintained by the Dean/Director.
   c. The Dean/Director is responsible for ensuring the collection, use, storage and/ or disposal of identifying information in accordance with the state and federal laws.
   d. The Chief Information Officer will work with the appropriate Dean/Director or designee to limit access to records containing identifying information to employees that require the use of identifying information for the performance of their duties.

Responding to Detection of Red Flags/Identity Threats

1. Ask for validation and/or supplemental documentation/identification when a student's identity is in question.
2. Verify original student documents when a discrepancy is reported regarding social security number discrepancies to name and other issues regarding aged accounts.
3. Check credit card receipts when possible fraudulent charges are reported from a customer's bank statement.
4. Deny access to information or disable an account pending further investigation and resolution of suspicious activity.

5. Follow up on reported thefts which possibly involve the compromise of sensitive data.
6. Notify victims and proper authorities of possible identity theft.
7. Use all available media to disseminate information concerning an improper disclosure of sensitive information. The records of current students, former students, and employees should be considered when dissemination of the information concerns a breach.
8. It is the responsibility of any employee who believes that identifying information has been compromised to notify the Vice President of Administrative Services immediately. Following notification the Vice President of Administrative Services will begin the notification process as required by law.
9. Any inappropriate collection, use, disclosure and/or handling of identifying information by an employee my result in disciplinary action.

Update of Identity Theft Program

The College will evaluate and update as necessary the Identity Theft Prevention Program on an annual basis or as deemed appropriate by senior administration or other factors such as current issues, advances in technology, or other related policies.

Program Administration

1. **Program Oversight**
    a. The College designates the Vice President of Administrative Services to be responsible for the oversight, development, implementation, and administration of the Identity Theft Prevention Program.
2. **Staff Training**
    a. The College will ensure adequate staff training considering the needs of our faculty and staff, multiple records, and various locations through professional development, staff meetings, or other methods as established by Deans/ Directors.
3. **Oversight of Service Providers**
    a. Upon request the College will review the operating procedures of any service provider that will work with sensitive information from student and/or employees.

Policy Number: 306-02-10BP

Adopted: May 29, 2008

Amended: May 1, 2009; January 27, 2015

Download a PDF of this policy