

A. Approval and Management; Program Administration; Training; Annual Report

The Vice-President of Administration and Finance or such other person that may be appointed from time to time by the President of the College (hereinafter, the "Program Administrator") is responsible for overall Program management and administration. The Program Administrator shall provide appropriate identity theft training for relevant LCCC employees and provide reports and periodic updates to the Program Administrative Committee of the College, as well as, the President and LCCC Board of Trustees on at least an annual basis.

The annual report shall identify and evaluate issues such as the effectiveness of the College's policies and procedures for addressing the risk of identity theft with respect to covered accounts, oversight of service providers, significant incidents involving identity theft and the College's response, and any recommendations for material changes to this policy or the

- 3) The presentation of suspicious personal identifying information, such as a suspicious address change
- 4) The unusual use of, or other suspicious activity related to, a Covered Account
- 5) Notices from customers, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts

D. Examples of Red Flags

Examples of Red Flags recognized by the College are listed in the Program document according to the following categories:

- 1) Notifications or warnings from a Consumer Reporting Agency.
- 2) Suspicious documents.
- 3) Suspicious personal identifying information.
- 4) Unusual use of, or suspicious activity related to, the Covered Account.
- 5) Notice from customers and others regarding possible identity theft in connection with Covered Accounts held by the college.

E. Detection of Red Flags

The college shall address the detection of Red Flags in connection with the opening of Covered Accounts and existing Covered Accounts according to Program guidance.

F. Response to Red Flags

The college shall respond quickly to prevent identity theft in accordance with steps listed in the Program document.

G. Oversight of Service Providers

The College will make reasonable efforts to ensure that the activity of a service provider engaged by the College to perform an activity in connection with Covered Accounts, is conducted with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. A service provider that maintains its own identity theft prevention program that is consistent with the policy of the College and the federal law and regulations may be considered to be meeting these requirements. An example of a major service provider could be an external entity that provides student loan administration, billing, reporting, etc.

H. Program Administration


Responsibility for developing, implementing and updating this Program lies with a Program Administrative Committee (Committee) for the College. The Committee is headed by the Program Administrator. Additional members of the committee will be appointed as necessary from departments within the College who deal with Covered Accounts or Sensitive Identifying Information within their departments. The Program Administrator will be responsible for ensuring appropriate training of College staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

I. Program Updates and Committee Report

The Committee will periodically review and update this Program to reflect changes in risks to students and the soundness of the College from Identity Theft. Updates will be reported at least annually to the President and the LCCC Board of Trustees in the Committee's report on the Identity Theft Prevention Program.

The annual report should address material matters related to the Program and evaluate issues such as:

- A. The effectiveness of the policies and procedures of the college in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements;
- B. Significant incidents involving identity theft and the college's response; and
- C. Recommendations for material changes to the Program.

Originator(s) Name(s)	Herry Andrews, Accounting Services Director	5/4/11
Approval by President's Cabinet		5/4/11
Approval by Board of Trustees	George McIlvaine, Acting Board Chair	6/16/10
Approval by President		6/17/10

In response to the growing threat of identity theft, the United States Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Public Law 108-159. This amendment to the Fair Credit Reporting Act charged the Federal Trade Commission with promulgating rules regarding identity theft. On November 7, 2007, the Federal Trade Commission promulgated the final rules, known as "Red Flag" rules, which had an effective date of November 1, 2008. 16 CFR 681. These rules, implementing sections 114 and 315 of FACTA, require the enactment of certain policies and procedures by the revised effective date of June 30, 2010. The rules apply to "financial institutions" and "creditors" with "covered accounts." A covered account is an "account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions," such as Laramie County Community College (LCCC) student accounts. Every affected college must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The program must be appropriate to the size and complexity of the college and the nature and scope of its activities. The program must incorporate the definition and charges the college with monitoring any such account for which there is a reasonably foreseeable risk of identity theft.

The purpose of the Red Flag Rules is to combat identity theft. Federal regulations require financial institutions and Creditors to implement a program to detect, prevent, and mitigate identity theft in connection with new and existing accounts.

The Vice President of Administration and Finance or such other person that may be appointed from time to time by the President of the College (hereinafter, the "Program Administrator") is responsible for overall Program management and administration. The Program Administrator shall provide appropriate identity theft training for relevant LCCC employees and provide reports and periodic updates to the Program Administrative Committee of the College, as well as, the President and LCCC Board of Trustees on at least an annual basis.

The annual report shall identify and evaluate issues such as the effectiveness of the College's policies and procedures for addressing the risk of identity theft with respect to covered accounts, oversight of service providers, significant incidents involving identity theft and the College's response, and any recommendations for material changes to this policy or the Program. As part of the review, Red Flags may be revised, replaced, or eliminated. Defining new Red Flags may also be appropriate.

- A. *Identity Theft* is a "fraud committed or attempted using the identifying information of another person without authority."
- B. *Red Flag* is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."
- C. *Covered Accounts* includes all employee and student accounts or loans that are administered by the College. Covered Accounts also include any account that involves or is designed to permit multiple payments or transactions.
- D. *Program Administrator* is the individual designated with primary responsibility for oversight of the program.
- E. *Program Administrative Committee* is a committee charged with updating this program, reporting *program* effectiveness, and assisting the program administrator in training of LCCC affected students, faculty and staff in program operation.
- F. *Sensitive Identifying Information* 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, email 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, student identification number, student bank routing and account number, central computer account name and password.

- A. Personal information upon enrollment, hire or contract:
 - 1) Social Security Number
 - 2) Date of birth
 - 3) Address
 - 4) Phone numbers
 - 5) Maiden name
 - 6) Student or employee number
 - 7) Government-issued ID numbers
 - 8) College systems account password
- B. Payroll Information – Same as Personal information along with:
 - 1) Paychecks
 - 2) Pay stubs
 - 3) Banking information
 - 4) Any document or electronic file containing salary information
- C. Medical Information for Employee or Student – Same as Personal information along with:
 - 1) Doctor names and claims
 - 2) Insurance claims
 - 3) Any personal medical information
- D. Credit Card Information, including:
 - 1) Credit card number (in part or whole)
 - 2) Credit card expiration date
 - 3) Cardholder name
 - 4) Cardholder address

- A. Laramie County Community College will consider the following risk factors in identifying Red Flags for Covered Accounts, if appropriate. The types of Covered Accounts we offer or maintain are:
- 1) The methods we provide to open Covered Accounts
 - 2) The methods we provide to access Covered Accounts
 - 3)

- 3) Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's Covered Account.
- 4) The College is notified that the customer is not receiving paper account statements.
- 5) The College is notified of unauthorized charges or transactions in connection with a customer's Covered Account.

E. Notice from Customers and Others Regarding Possible Identity Theft In Connection with Covered Accounts Held by the College

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.

The college shall address the detection of Red Flags in connection with the opening of Covered Accounts and existing Covered Accounts by:

- A. Obtaining identifying information about and verifying the identity of newly hired employees, newly enrolled students, etc.

The annual report should address material matters related to the Program and evaluate issues such as:

- A. The effectiveness of the policies and procedures of the college in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements;
- B. Significant incidents involving identity theft and the college's response; and
- C. Recommendations for material changes to the Program.