Laramie County Community College

Identity Theft Prevention Program

June 30, 2010

Background

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.

Purpose

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.

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 Program. As part of the review, Red Flags may be revised, replaced, or eliminated. Defining new Red Flags may also be appropriate.

Definitions

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

Red Flag is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

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.

Program Administrator is the individual designated with primary responsibility for oversight of the program.

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.

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.

Sensitive Information to be Protected

1. Personal information upon enrollment, hire or contract:
   a. Social Security Number
   b. Date of birth
   c. Address
   d. Phone numbers
   e. Maiden name
   f. Student or employee number
   g. Government-issued ID numbers
   h. College systems account password

2. Payroll Information – Same as Personal information along with:
   a. Paychecks
   b. Pay stubs
   c. Banking information
   d. Any document or electronic file containing salary information

3. Medical Information for Employee or Student – Same as Personal information along with:
   a. Doctor names and claims
   b. Insurance claims
   c. Any personal medical information

4. Credit Card Information, including:
    a. Credit card number (in part or whole)
    b. Credit card expiration date
    c. Cardholder name
    d. Cardholder address

Risk Assessment

1. Laramie County Community College will consider the following risk factors in identifying Red Flags for Covered Accounts, if appropriate:
    a. The types of Covered Accounts we offer or maintain
    b. The methods we provide to open Covered Accounts
    c. The methods we provide to access Covered Accounts
    d. Our previous experience with identity theft

2. Laramie County Community College will, from time to time, incorporate relevant Red Flags from sources such as:
    a. Incidents of identity theft that we have experienced or that have been experienced by other colleges and universities
    b. Methods of identity theft identified by us or other Creditors that reflect changes in identity theft risks
    c. Applicable supervisory guidance

3. Laramie County Community College will, from time to time, include relevant Red Flags from the following categories, if appropriate:
    a. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services
    b. The presentation of suspicious documents
    c. The presentation of suspicious personal identifying information, such as a suspicious address change
    d. The unusual use of, or other suspicious activity related to, a Covered Account
    e. Notices from customers, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts

Examples of Red Flags

The following instances are examples of Red Flags recognized by the College:

1. **Notifications or Warnings From a Consumer Reporting Agency**
    a. A fraud or active duty alert is included with a consumer report.
    b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
    c. A consumer reporting agency provides a notice of address discrepancy that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.
    d. 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 recent and significant increase in the volume of inquiries,
        2) An unusual number of recently established credit relationships, or
        3) A material change in the use of credit, especially with respect to recently established credit relationships.

2. **Suspicious Documents**
   a. Documents provided for identification appear to have been altered or forged.
   b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
   c. Other information on the identification is not consistent with information provided by the person opening a new Covered Account or customer presenting the identification.
   d. Other information on the identification is not consistent with readily accessible information that is on file with us.
   e. An application appears to have been altered or forged, or given the appearance of having been destroyed and reassembled.

3. **Suspicious Personal Identifying Information**
   a. Personal identifying information provided is inconsistent when compared against external information sources. For example:
      1) The address does not match any address in the consumer report; or
      2) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
   b. Personal identifying information is not consistent with other personal identifying information provided by the customer, such as a lack of correlation between the Social Security Number range and date of birth.
   c. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College, such as:
      1) The address on an application is the same as the address provided on a fraudulent application; or
      2) The telephone number on an application is the same as the phone number provided on a fraudulent application.
   d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College, such as:
      1) The address on an application is fictitious, a mail drop, or a prison; or
      2) The telephone number is invalid, or is associated with a pager or answering device.
   e. The Social Security Number provided is the same as that submitted by other persons opening an account or is the same as other customers.
   f. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or is the same or similar to other customers.
   g. The person opening the Covered Account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
   h. Personal identifying information provided is not consistent with personal identifying information that is on file at the College.

4. **Unusual Use of, or Suspicious Activity Related to, the Covered Account**
   a. Shortly following notice of a change of address for the Covered Account, the College receives a request for a new, additional, or replacement card.
   b. A new Covered Account is used in a manner commonly associated with known patterns of fraud, such as the customer failing to make the first payment or making an initial payment but no subsequent payments.

c. A Covered Account is used in a manner that is not consistent with established patterns of activity on the account, such as:
    1) Nonpayment when there is no history of late or missed payments,
    2) A material increase in the use of available credit, or
    3) A material change in purchasing or spending patterns.
d. A Covered Account that has been inactive for a reasonably lengthy period of time is used. Determining what is reasonably lengthy should take into consideration the type of account, the expected pattern of usage, and other factors which may be relevant.
e. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's Covered Account.
f. The College is notified that the customer is not receiving paper account statements.
g. The College is notified of unauthorized charges or transactions in connection with a customer's Covered Account.

5. <u>Notice from Customers and Others Regarding Possible Identity Theft In Connection with Covered Accounts Held by the College</u>

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.

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 by:

1. Obtaining identifying information about and verifying the identity of newly hired employees, newly enrolled students, etc.
2. Monitoring transactions through photo ID verification.
3. Requiring alternative identification method if photo ID appears to be altered or forged.
4. Rejecting any application for a service or transaction that appears to have been altered or forged.
5. Including assessment of Red Flags as part of the College's Internal Audit processes.

Response to Red Flags

The college shall respond quickly to prevent identity theft. **In all cases report Red Flags to Program Administrator.** Response may include:

1. Contacting owner of account in question by:
    a. A written letter
    b. Phone number on record
2. Denying access to the covered account until other information is available to eliminate the red flag.
3. Terminating transaction.
4. Changing any passwords, security codes, or other security devices that permits access to a Covered Account.
5. Reopening a Covered Account with a new account number.
6. Not opening a new Covered Account.
7. Closing an existing Covered Account.
8. Notifying and cooperating with appropriate law enforcement.
9. Determining no response is warranted under the particular circumstances.

In order to further prevent the likelihood of identity theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure.
2. Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information.
3. Ensure that office computers with access to Covered Account information are password protected.
4. Avoid use of social security numbers, except when necessary, and only by authorized individuals.
5. Ensure computer virus protection is up to date.
6. Require and keep only the kinds of student information that are necessary for College purposes.
7. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when unsupervised and/or secured behind a closed locked door at the end of the work day.
8. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded.
9. Any additional common sense steps deemed necessary by each department to protect against Identity Theft (example — privacy computer screens, etc.)
10. The College shall inquire that the activity of service providers to Covered Accounts is conducted with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

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.

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.

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:

1. 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;
2. Significant incidents involving identity theft and the college's response; and
3. Recommendations for material changes to the Program.