Clarkson College
Prepare to be the best.

POLICY:

Identity Theft Prevention

Purpose

The purpose of this program is to comply with a new federal mandate relating to identity theft. It requires creditors who have entered into business arrangements that meet the definition of "covered account" to establish an identity theft prevention program. Although we believe the risk of identity theft is low at Clarkson College, we believe implementation of a prevention program is in the best interest of our students and those that we serve.

Approval & Management; Program Administration; Training; Annual Report

The Board of Directors of Clarkson College has approved the identity theft prevention program. The Vice President of Operations has been given the responsibility by the Board for overall Program management and administration. S/he shall be responsible for the provision of appropriate identity theft training for relevant Clarkson College employees and for providing reports and periodic updates to senior management and to the Board on an annual basis. The annual report shall evaluate issues such as the effectiveness of the 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 response of Clarkson College, and any recommendations for material changes to 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
"Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

Identifying Information
"Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any

1. Name, social security number, date of birth, official state or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification;
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address or routing code; and
4. Telecommunication identifying information or access device (as defined in 18 USC1029(e)).

Account
"Account" means a continuing relationship established by a person with Clarkson College to obtain a product or service for personal, family, household, or business purposes. Account includes:

1. An extension of credit, such as the purchase of property or services involving a deferred payment, and
2. A deposit account.

Covered Account
"Covered Account" means:

1. An account that Clarkson College offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions. Examples could include credit or debit card accounts if the cards are issued by the institution, certain student loan accounts, telephone accounts, utility accounts, and accounts for the payment of tuition, fees or other charges over time; and

2. Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

Customer
"Customer" means a person that has a covered account with Clarkson College.

Red Flag
"Red Flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Service Provider
"Service Provider" means a person that provides a service directly to Clarkson College.

Transactions at Risk

Clarkson College has reviewed its transactions and has determined that the following are "covered accounts" and thus subject to the identity theft prevention policy: Student accounts being paid on payment plans.

Clarkson College has reviewed the guidelines that contain potential red flags in Appendix A to part 681 of Title 16 in the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. Clarkson College already has existing policies, procedures and other arrangements to ameliorate the risk to customers, with particular emphasis on those customers who are students or former students of identity theft. Clarkson College intends to utilize those current policies in addition to the new requirements of this identity theft prevention program.

1. Clarkson 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; and
    d. Our previous experience with identity theft.
2. Clarkson College will 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; and
    c. Applicable supervisory guidance.
3. Clarkson College will 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; and
    e. Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts.
4. Clarkson College will attempt to detect relevant red flags in connection with the opening of covered accounts and existing covered accounts, such as by:
    a. Obtaining identifying information about and verifying the identity of a person opening a covered account.
    b. Authenticating customers, monitoring transactions and verifying the validity of change of address requests in the case of existing covered accounts.

Red Flag Examples
The following are illustrative examples of red flags in connection with covered accounts:

5. Clarkson College will consider the following instances as red flags:

    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:

   (i) A recent and significant increase in the volume of inquiries;

   (ii) An unusual number of recently established credit relationships;

   (iii) A material change in the use of credit, especially with respect to recently established credit relationships; or

   (iv) An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

e. Documents provided for identification appear to have been altered or forged.

f. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

g. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

h. Other information on the identification is not consistent with readily accessible information that is on file with us.

i. An application appears to have been altered or forged, or given the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

j. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

   (i) The address does not match any address in the consumer report; or

   (ii) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

k. 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.

l. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by Clarkson College, such as;

   (i) The address on an application is the same as the address provided on a fraudulent application; or

   (ii) The telephone number on an application is the same as the phone number provided on a fraudulent application.

m. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Clarkson College such as

   (i) The address on an application is fictitious, a mail drop, or a prison; or

   (ii) The telephone number is invalid, or is associated with a pager or answering device.

n. The Social Security Number provided is the same as that submitted by other persons opening an account or is the same as other customers.

o. 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.

p. 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.

q. Personal identifying information provided is not consistent with personal identifying information that is on file at Clarkson College.

r. If Clarkson College uses challenge questions, the person opening the covered account or the customer 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 Covered Account

s. A covered account is used in a manner that is not consistent with established patterns of activity on the account, such as

   (i) Nonpayment when there is no history of late or missed payments;

   (ii) A material change in electronic funds transfer patterns in connection with a deposit account.

   (iii) 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.

t. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

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

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

v. Clarkson 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.

Response to Detected Red Flags

The program shall provide for appropriate responses to detected red flags in order to prevent and mitigate identity theft. The response of Clarkson College shall be commensurate with the degree of risk posed. Appropriate responses may include, but not be limited to:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the customer;
3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
4. Canceling the transaction;
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; or
9. Determining no response is warranted under the particular circumstances.

Updating the Program

The program shall be re-evaluated and updated periodically to reflect changes in risks to customers or the safety and soundness of Clarkson College based on factors such as:

1. The experiences of Clarkson College with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent and mitigate identity theft;
4. Changes in the types of accounts that Clarkson College offers or maintains; or
5. Changes in the business arrangements of Clarkson College, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

The reviews will include an assessment of which accounts are covered by the program and the risk of identity theft with respect to each type of covered account.

Oversight of Service Providers

It shall be the responsibility of Clarkson College to ensure that the activity of a service provider, who is engaged by Clarkson 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 Clarkson College and the federal law and regulations may be considered to be meeting these requirements.