AUTHENTICATED,
OHIO LEGISLATIVE SERVICE
COMMISSION
DOCUMENT #270316

Ohio Administrative Code

Rule 3344-19-01 Identity theft prevention program and red flag compliance policy.

Effective: October 10, 2014

(A) Program adoption

Cleveland state university has developed this identity theft prevention program ("program") pursuant to the "Federal Trade Commission's Red Flags Rule," which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size of the university's operations and systems, and the nature and scope of its activities, the university has determined that this program is appropriate for Cleveland state university, and, therefore, adopted this program on July 23, 2009.

(B) Purpose

The university adopts this identity theft prevention program in an effort to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account," and to provide for continued administration of the program. This program shall include reasonable policies and procedures to:

(1) Identify patterns, practices, or specific activities ("red flags") that indicate the possible existence of identity theft with regard to new or existing covered accounts;

(2) Detect red flags that have been incorporated into the program;

(3) Respond appropriately to any red flags that are detected under the program;

(4) Ensure periodic updating of the program, including reviewing the accounts that are covered and the identified red flags that are part of the program; and

(5) Promote compliance with state and federal laws and regulations regarding identity theft protection.

(C) Definitions

(1) "Identity theft" refers to fraud committed or attempted using the identifying information of another person without authority.

(2) "Covered account" refers to any account the university offers or maintains primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions.

(3) "Red flag" refers to a pattern, practice or specific activity that indicates the possible existence of identity theft.

(4) "Identifying information" refers to any name that may be used, alone or in conjunction with any other information, to identify a specific person.

(D) Covered accounts

Cleveland state university has identified two types of accounts which are covered accounts administered by the university and are relevant to this policy:

(1) Deferred tuition payment plans

(2) Perkins loans

(E) Identification of relevant red flags

In order to identify relevant red flags, the university considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with identity theft. The following are relevant red flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

(1) Notifications and warnings from credit reporting agencies.

(a) Report of fraud accompanying a credit report

(b) Notice or report from a credit agency of a credit freeze on a customer or applicant

(c) Notice or report from a credit agency of an active duty alert for an applicant, and

(d) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

(2) Suspicious documents

(a) Identification document or card that appears to be forged, altered or inauthentic

(b) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document

(c) Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged), and

(d) Application for service that appears to have been altered or forged.

(3) Suspicious personal identifying information

(a) Identifying information presented that is inconsistent with other information the customer provides (for example, inconsistent birth date)

(b) Identifying information presented that is inconsistent with other sources of information (for example, an address not matching an address on a credit report)

(c) Identifying information presented that is the same as information shown on other applications that were found to be fraudulent

(d) Identifying information presented that is consistent with fraudulent activity (for example an invalid phone number or a fictitious billing address)

(e) Social security number presented that is the same as one given by another customer

(f) An address or phone number presented that is the same as that of another person

(g) A person fails to provide complete personal identifying information on an application when reminded to do so (note that by law, social security numbers are not required), and

(h) A person's identifying information is not consistent with the information that is on file for the customer.

(4) Suspicious account activity or unusual use of account

(a) Change of address for an account followed by a request to change the account holder's name

(b) Payment stop on an otherwise consistently up-to-date account

(c) Account used in a way that is not consistent with prior use (for example, very high activity level)

(d) Mail sent to the account holder is repeatedly returned as undeliverable

(e) Notice to the university that a customer is not receiving mail sent by the university

(f) Notice to the university that an account has unauthorized activity

(g) Breach in the university's computer system security, and

(h) Unauthorized access to or use of customer account information.

(5) Alerts from others

Notice to the university from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in identity theft.

(F) Detection of red flags

The program's general red flag detection practices are described in this document. Each college and/or department can develop and implement additional methods and protocols appropriate to meet the requirements of their senior management.

(1) New accounts. In order to detect any of the red flags identified above associated with the opening of a new account, university personnel will take the following steps to obtain and verify the identity of the person opening the account:

(a) Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification

(b) Verify the customer's identity (for example, review a student's viking card)

(c) Independently contact the customer.

(2) Existing accounts. In order to detect of the red flags identified above for an existing account, university personnel will take the following steps to monitor transactions with an account:

(a) Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email)

(b) Verify the validity of requests to change billing addresses (other than changes initiated on-line by the student/customer.)

(3) Specifically

(a) Participation in a payment plan. Deferred payment plan applications must be electronically signed and dated by the student. Initial payment must be received prior to enrollment in a deferred payment plan. Students in a "VA" student group are exempt from the payment requirement.

(b) Perkins loan. Application for a Perkins loan must be made electronically and will not be approved until the department of education's three point match (name, date of birth, social security number) are confirmed. Funds are applied against a student account, never disbursed directly to a student.

(G) Response

The program shall provide for appropriate responses to detected red flags to prevent and mitigate identity theft. The appropriate responses to the relevant red flags are as follows:

(1) Deny access to the covered account until other information is available to eliminate the red flag

(2) Contact the student

(3) Change any passwords, security codes or other security devices that permit access to a covered account

(4) Continue to monitor an account for evidence of identity theft

(5) Not open a new account

(6) Close an existing account

(7) Notify university police and law enforcement

(8) Determine no response is warranted under the particular circumstances.

(H) Training

All employees who process information related to a covered account shall receive training on the procedures outlined in this policy. Refresher training may be provided annually as needed.

(I) Oversight of the program

Responsibility for developing, implementing and updating this program lies with the vice president, business affairs and finance. The program administrator is the controller who will be responsible for day-to-day administration, ensuring appropriate training of university staff on the program, 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.

(J) Updating the program

This program will be periodically reviewed and updated to reflect changes in risks to students and the soundness of the university from identity theft. At least once per year in July, the program administrator will consider the university's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the university maintains and changes in the university's business arrangements with other entities. After considering these factors, the program administrator will determine whether changes to the program, including the listing of red flags, are warranted. If warranted, the program administrator will update the program.

(K) Oversight of service provider arrangements

(1) The university shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. The university will require, by contract, that service providers have such policies and procedures in place and report any red flags to the program administrator.

(2) Currently the university utilizes "ECSI" to administer the Perkins Loan repayment program. Students contact "ECSI" directly through its website or by telephone and provide personally identifying information to be matched to the records that the university has provided to "ECSI."