Ohio Administrative Code

Rule 3342-7-11 University policy regarding identity theft prevention.

Effective: March 1, 2015

(A) Policy statement. Kent state university developed this identity theft prevention program ("Program") pursuant to the implementation of Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The purpose of the act and this policy is to implement a university-wide identity theft prevention program. This program provides for the identification, detection, and response to patterns, practices and/or specific activities known as "red flags" that could indicate identity theft.

(B) Definitions. As used in this policy:

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

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

(3) "Covered account" includes:

(a) An account that the university offers or maintains that involves or is designed to permit multiple payments or transactions for students, faculty and staff, such as a credit card account, loan, phone accounts, utility accounts, checking accounts, or savings account;

(b) Any other account that the university offers or maintains for which there is a reasonably foreseeable risk to customers of identity theft;

(c) Covered accounts do not include stored value cards (such as laundry cards or dining hall prepaid cards) if the stored value cards do not require an electronic fund transfer from the card holders account held by the university for the purpose of transferring money between accounts or in exchange for money, property, goods, services or cash.

(4) "Identifying information" is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person or protected information including, but not limited to: name, address, telephone number, social security number, date of birth, government issued drivers license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, and/or credit card number.

(C) Scope.

This policy contains procedures to:

(1) Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the program;

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

(3) Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

(4) Ensure the program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from identity theft.

(D) Definitions. As used in this policy:

Identification of red flags. The university identifies the following red flags as potential indicators of fraud:

(1) Notifications and warning 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 an applicant;

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

(d) Receipt of a notice of address discrepancy in response to a credit report request; and

(e) Indication from a credit report of activity that is inconsistent with an applicant'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 student information; 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 student provides (example: inconsistent birth dates);

(b) Identifying information presented that is inconsistent with other sources of information (example: an address not matching an address on a loan application);

(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 (example: an invalid phone number or fictitious billing address);

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

(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; and

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

(4) Suspicious covered account activity or unusual use of account.

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

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

(c) Account used in a way that is not consistent with prior use;

(d) Mail sent to the student is repeatedly returned as undeliverable;

(e) Notice to the university that a student 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 student account information.

(5) Alerts from third-party.

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

(E) Procedures.

(1) Student enrollment. In order to detect red flags identified in this policy associated with the enrollment of a student, university personnel will utilize the following procedures, in addition to any other policies or procedures created internally, to obtain and verify the identity of the person opening or using the account.

(a) University personnel must require certain identifying information such as name, date of birth, academic records, home address or other identification; and

(b) University personnel must verify the students identity at time of issuance of student identification card.

(2) Existing accounts. In order to detect any of the red flags identified above for an existing covered account, university personnel will utilize the following procedures, in addition to any other policies or procedures created internally, to monitor transactions and information on an account.

(a) University personnel will verify the identification of students in person when in receipt of a request for information from the student or a third party;

(b) University personnel will verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and

(c) University personnel will verify changes in banking information given for billing and payment purposes.

(3) Responding to red flags. In the event university personnel detect any identified red flags, such personnel shall immediately contact his/her supervisor and take one or more of the following steps, depending on the degree of risk posed by the red flag:

(a) Continue to monitor a covered account for evidence of identity theft for a reasonable period of

time after such detection;

(b) Contact the student or applicant;

(c) Contact the office of security and access management in the division of information services to change any passwords or other security devices that permit access to covered accounts;

(d) Do not open a new covered account until the new red flag has been cleared;

(e) Provide the student with a new student identification number;

(f) Notify the appropriate office of origin for the record/account in which the red flag was detected;

(g) Notify law enforcement;

(h) In all cases, notify one of the following officials to assess whether attempted transaction was fraudulent or authentic;

(i) University registrar, for student account related issues;

(ii) University bursar, for university account related issues;

(iii) Director of admissions, for admission-related issues;

(iv) Vice president for information services, for university data related issues;

(v) Vice president for human resources, for employee account related issues;

(4) Preventive measures for identifying information. In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the university will take the following steps with respect to its internal operating procedures to secure identifying or protected information:

(a) Lock file cabinets, desk drawers, overhead cabinets, and any other storage space containing

documents with identifying or protected information;

(b) Ensure that its website is secure or provide notice when the website is no longer secure;

(c) Follow university policies for data security when transmitting identifying and/or protected information;

(d) Ensure complete and secure destruction of paper documents and computer filing containing student account information in accordance with the universitys record retention schedules;

(e) Ensure that university systems and computers accessing covered account information are password protected and virus definitions and protections are up-to-date;

(f) Avoid use of the social security number as an identifier.

(F) Program administration.

(1) Authority. Responsibility for developing, implementing and updating the red flag program is designated to the program administrator as appointed by the vice president for finance and administration.

(2) Training. At least annually, university personnel and/or office responsible for development, implementation, and administration of the procedures required by this policy shall be trained as necessary. Such attendance will be recorded for monitoring compliance and audit purposes. The report should include at a minimum any significant incidents involving identity theft and the university response, and recommendations for changes to the program and/or policy.

(3) Third-party service providers. It is the responsibility of the contracting department to ensure that the activities of all service providers and contractors are conducted in accordance with reasonable policies and procedures designed to protect, prevent, and mitigate the risk of identity theft. At a minimum, third-party service providers must meet the minimum requirements consistent with the red flag rules at 16 C.F.R. 681.

(4) Updates. The university shall update this policy periodically, when necessary, to reflect that changes in risks to covered account holders or to the safety and soundness of the university from identity theft, based on factors such as the experiences of the university with identity theft, changes in the methods of engaging in or preventing identity theft, and/or changes in the types of accounts that the university offers.