Policy: 4.16

Identity Theft Prevention (Red Flags)

Purpose

To establish an Identity Theft Prevention Plan and adopt the applicable requirements of 16 C.F.R. 681, a federal regulation issued by the Federal Trade commission (FTC) as part of the implementation of the Fair and Accurate Credit Transaction (FACT) Act of 2003 requiring that financial institutions and creditors implement written plans which provide for detection of and response to specific activities ("Red Flags") that could be related to damages from fraudulent activity of identity theft.

Definitions

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

Account: a continuing relationship established by a person with the College to obtain a product or service for personal, family, household or business purposes. The account includes an extension of credit, such as student tuition payment plan and other credit extended by the College and any of its departments or subunits to students, faculty, staff, and the campus community.

Consumer Reporting Agency: entities that collect and disseminate information about consumers to be used for credit evaluation and certain other purposes.

Covered Accounts: 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, including but not limited to:

- Credit account
- Loan account
- Prepaid card account

Any other account that the College 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 ligation risks.

Creditor: any departments, unit, subunit, or entity under the control of the College and its governing board of Trustees who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

Customer: student, faculty, staff, or any person from the campus community that has a covered account with the College

Credit: the right granted by a College to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase services and defer payment, thereto.

Prepaid Card: any card issued by the College to a customer for use in initiating an electronic payment from the prepaid balance credited to the prepaid card at the College, for the purpose of purchasing goods, meals, or services on campus or obtaining money.

Notice of Address Discrepancy: a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), 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.

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

- Name
- 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
- Unique electronic identification number
- Computer's internet protocol address or routing code

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

Service Provider: a person who provides a service directly to the College such as a food service provider.

Card Issuer: financial institution or creditor; in this case the College that issues a debit, credit, or prepaid card. College accounts that fall under this definition include:

- Federal Perkins Student Loans
- Tuition Payment Plans
- Institutional Accounts in CLM system
- Student, faculty, and staff ID cards that facilitate the holder to purchase items accessing a prepaid balance from said card

Policy Statement

Kansas City Kansas Community College (KCKCC; the College) will implement and provide for the continued administration of the plans in relation to:

- Identify patterns, practices, or specific "Red Flags" that indicate the possible existence of identity theft regarding new or existing covered accounts.
- Detect "Red Flags" that have been incorporated into the plan.
- Respond appropriately to any "Red Flags" that are detected under the Plan.
- Ensure periodic updating of the plan, including reviewing the accounts that are covered and the identified red flags that are part of the Plan.
- Promote compliance with state and federal laws and regulations regarding identity theft protection.

<u>Plan Responsibilities</u>

The Controller's Office is responsible for the administration of the Plan. Operational responsibility of the Plan includes but is not limited to, the oversight, development, implementation and administration of the Plan, approval of needed changes to the Plan, and implementation of needed changes.

The Plan Administrator will be responsible for ensuring appropriate training of the College staff on the Plan; the review of staff reports regarding the detection of "Red Flags" and, the steps for identifying, preventing, mitigating identity theft, determining which steps of prevention and mitigation should be taken, and considering periodic changes to the Plan.

The procedures as outlined in the Procedure Document will be periodically reviewed and updated to reflect changes in identity theft risks and technology. The Plan Administrator will consider the College's experiences with identity theft; changes in identity theft methods; changes in identity theft detection, mitigation and prevention methods; changes in types of accounts the College maintains; changes in the College's business arrangements with other entities, and any changes in legal requirements in the area of identity theft. After considering these factors, the plan Administrator will determine whether changes to the procedures, including the listing of "Red Flags", are warranted.

The Plan Administrator shall confer with all appropriate College personnel as necessary to ensure compliance with the plan. The Plan Administrator (Controller) shall regularly report through the College Risk Management Committee to the College Chief Financial Officer on the effectiveness of the plan and present any recommended changes for approval.

1) Application of Other Laws and College Policies

College personnel should make reasonable efforts to secure confidential information to the proper extent. Furthermore, this section should be read and applied in conjunction with the Family Education Rights and Privacy Act ("FERPA"), and other applicable laws and College policies.

2) Identification of "Red Flags"

Each College department which offers or maintains Covered Accounts will be responsible for managing and protecting information related to covered accounts. In order to identify relevant "Red Flags", the College considers the types of accounts that it offers and maintains, the methods it provides to open accounts, the methods it provides to access 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:

A. Notification and Warnings from Credit Reporting Agencies
   - Report of fraud accompanying a credit report.
   - Notice or report from a credit agency of a credit freeze on a customer or applicant.
   - Notice or report from a credit agency of an active-duty alert from an applicant.
   - Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents
   - Identification document or card that appears to be forged, altered on inauthentic.

- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document.
- Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged).
- Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information
   - Identifying information presented that is inconsistent with other information the customer provides *(example: inconsistent birth dates).*
   - Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report).
   - Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address).
   - Social security number presented that is the same as one given by another customer.
   - A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must **not** be required).
   - A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account
   - Change of address for an account followed by a request to change the account holder's name.
   - Payments stop on an otherwise consistently up-to-date account.
   - Account used in a way that is not consistent with prior use (example: very high activity).
   - Mail sent to the account holder is repeatedly returned as undeliverable.
   - Notice to the College that a customer is not receiving mail sent by the College.
   - Notice to the College that an account has unauthorized activity.
   - Breach in the College's computer system security.
   - Unauthorized access to or use of customer account information.

E. Alerts from Others
   - Notice to the College 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.

Board Approved: 05/18/2021