Cabrillo College
Identity Theft Prevention Program

Background

The Federal Trade Commission's Red Flags Rule (Section 114 of the Fair and Accurate Credit Transactions Act of 2003-16 C.F.R. -681.2) requires that every financial institution and creditor establish an "Identity Theft Program" tailored to its size, complexity and the nature of its operations. Cabrillo College is considered a creditor because we provide institutional and Perkins Loans to our students as well as allow them to defer payments of tuitions and fees for services rendered.

Purpose

The purpose of the Identity Theft Prevention Program is to detect, prevent and mitigate identity theft in connection with transactions that students, donors, friends, faculty and staff conduct with Cabrillo College. The program will provide policies and procedures to 1) identify and detect Red Flags, 2) respond to detected Red Flags and 3) ensure the program is updated from time to time to reflect changes in risk profiles.

Definitions

Identity Theft: Fraud committed using the identifying information of another person.

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

Covered Account: Any account the university maintains for students or employees that involves multiple payments or transactions, examples of these are: Perkins and Institutional Loans, student tuition accounts, staff computer loans.

Responsible Department: College department or office responsible for opening or maintaining the covered account.

Identifying Information: Any name or number that may be used, alone or in conjunction with any other information, to identify a person; this includes name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employee or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

Identification of Red Flags

The responsible department will evaluate the different ways its clients can open and access their covered accounts, i.e. internet, mail or physical presence. The following Red Flags can arise with the type of account access the college allows:

1. Notifications and warnings from credit reporting agencies. Red Flags in this category include:
    - report of fraud accompanying a credit report; notice of a credit freeze on a client or applicant
    - notice of an active alert for a client or applicant
    - indication from a credit report of activity that is inconsistent with a client or applicant's usual pattern of activity.
2. Suspicious documents; Red Flags in this category include:
    - identification documents or cards that appear to be forged or altered
    - identification documents or cards on which a person's photograph or physical description is not consistent with the person presenting the document

    - presentation of other documents with information that is not consistent with existing client information such as the person's signature; application for service that seems to have been altered or forged.
3. Suspicious personal identifying information; Red Flags in this category include:
    - identifying information such as birth date or address that is inconsistent with other information the client provides
    - identifying information presented that is consistent with found fraudulent activity such as an invalid phone number or fictitious billing address
    - social security number, address or phone number presented that is the same as those given by another customer
    - incomplete personal identifying information presented in an application.
4. Suspicious account activity or unusual use of account; Red Flags in this category include:
    - change of address requested for an account shortly followed by a request to change the account holder's name
    - payments stop coming in on an otherwise consistently up-to date account
    - mail sent to the account holder is repeatedly returned as undeliverable
    - notice to the college that a client is not receiving mail or email sent by the college
    - breach of the university's computer system
    - unauthorized access to or use of the client account information.
5. Alerts from others; the Red Flags in this category include:
    - notice to the college from a client, identity theft victim, law enforcement or other person that the college has opened or is maintaining a fraudulent account for a person engaged in identity theft.

Detecting Red Flags

In order to detect Red Flags in new accounts, the responsible department will take the following steps to obtain and verify the identity of the person opening the account:

- Require identifying information such as name, date of birth, residential or business address, principal place of business, driver's license, passport or other identification
- verify client's identity by comparing person to photo identity

- review documentation showing the existence of a business entity, i.e. state registration, license; and independently contact the client.

For existing accounts, before providing information, the responsible department personnel will verify the validity of the identification of the client and the validity of the client's request. Client's request may be made in person, via phone, fax, mail or email and can pertain to address changes, banking information changes, available balances, etc.

Preventing and Mitigating Identity Theft

In the event the responsible department's personnel detect or identify Red Flags and depending on the risk level of the identified flag, they will do one or a combination of the following steps:

1. Continue to monitor the account for further evidence of identity theft
2. Contact the client
3. Contact other college departments who may also need to take action on the incident
4. Change passwords or other security devices that permit access to account
5. Decline to open a new account
6. Close an existing account and/or open an account with a new number
7. Notify the responsible department's supervisor and the Identity Theft Prevention Program Committee to decide if law enforcement needs to be notified or if no further action is warranted under the particular circumstances

Protecting Client Identifying Information

In order to prevent the likelihood of identity theft occurring at the college, the responsible departments will add the following steps to their internal procedures:

1. Ensure that the college website is secure or provide clear notice to clients when the website is not secure due to technical difficulties

2. Ensure that department and personal computers' virus protection software is up to date
3. Ensure that the staff securely disposes of paper and electronic files containing clients' information
4. Ensure that department's computers are password protected and computer screens lock after a set reasonable period of time
5. Ensure that desks and computer screens are clear of client's information when meeting with other clients
6. Ensure that department personnel request only the last four digits of social security number, ITIN when clients submit requests via phone or email
7. Ensure that department personnel goes through the college security verification process (i.e. verify at least two of client's provided security questions and answers are consistent with data stored in the university computer system) when client calls or emails are received
8. Mail and email sensitive information only to client's address on file
9. Require and Keep only the identifying information that is necessary for their department's operation

Program Administration, Oversight and Updates

The Cabrillo College Identity Theft Prevention Program will be administered by a committee staffed by the following administrators or their designees: Registrar, Director of Information Technology, Financial Aid Director, Human Resources Director, and the Vice President of Administrative Services, who will function as the committee lead. The committee will meet on an annual basis during the summer (unless a need arises to meet sooner); the committee members will be responsible to a) conduct appropriate training of college employees in their area as to ensure consistence in the use of the identity protection measures described in this policy, b) review any staff reports regarding detection of Red Flags and the steps needed/used to prevent, mitigate or correct identity theft in those cases where it has been detected, and c) evaluate the college's experience with identity theft issues, risk changes in the clients and college profile to determine if those factors warrant changes to the program, its procedures or policies. Any changes to the program will need to be approved by the President's Cabinet.

Staff Training and Reporting

The expectation is that the Oversight Committee for the Identity Theft Prevention Program will conduct training on their respective areas to ensure that the responsible departments' personnel are implementing the program. The committee lead will provide copies of reports of identity theft incidents, program compliance and effectiveness to the Vice President of Administration.

Third Party Service Providers

From time to time the college contracts third party service providers to perform activities, i.e. payment processing, collection activities, monitoring and reporting, etc., in connection with covered accounts. When services are contracted, the responsible department will ensure the service provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

College departments implementing these contracts should ensure that the third party providers have identity theft prevention programs in place and obtain a copy of such policies and procedures. The agreement with those contractors should also require that the contractors report any Red Flags to the college for internal follow up.