



Procedure 209-01 Identity Theft Prevention

Sponsor: Information Technology Services

Purpose

The Program is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program established procedures to:

1. Identify relevant red flags for covered accounts the College offers or maintains 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 flag that has been detected to prevent and mitigate identity theft.
4. Ensure the Program is updated periodically to reflect changes in risks to students and employees or to the safety and soundness of the creditor from identity theft.

The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Definitions

Covered Account is a consumer account that involves multiple payments or transactions in arrears such as a loan that is billed or payable monthly. This includes accounts where payments are deferred and made by a borrower periodically over time such as with a tuition or fee installment payment plan.

Creditor is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal or continuation of credit. Examples of activities that would indicate the College is acting as a creditor would include:

1. Participation in the Federal Direct Plus Loan program.
2. Participation in the Federal Direct Stafford Loan program.
3. Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester.
4. Emergency loans.

Personal Information is specific information that represents a legal or personal identity or that could result in public impersonation of identity or identity theft if such information were stolen or compromised. This would also consist of using information in combination with one or more data elements when either the name or elements are not encrypted or redacted. Sensitive personal information includes but may not be limited to the following:

1. Legal name (first, last, middle)
2. Full date of birth
3. SSN
4. Driver's License Number
5. Enterprise ID

6. Financial account number
7. Password
8. Home address
9. Gender
10. Race
11. Medical information
12. Payroll information

Red Flag is a pattern, practice or specific activity that indicates the existence of identity theft or possible attempted fraud via identity theft on covered accounts.

Security Incident is a collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

Procedure

Identification of Red Flags

In order to identify relevant red flags, CCC considers the types of accounts that it offers and maintains, the methods provided to open accounts, the methods provided to access accounts, as well as previous experiences with identity theft. The following categories are identified as red flags:

1. Alerts, notifications or warnings from a consumer reporting agency including fraud alerts, credit freezes or official notice of address discrepancies.
2. The presentation of suspicious documents such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application that appears to have been cut up, reassembled and photocopied.
3. The presentation of suspicious personal identifying information such as a photograph or physical description on the identification that is not consistent with the appearance of the student presenting the identification; discrepancies in address, Social Security Number, Student ID, or other information on file; an address that is a mail-drop, a prison, or is invalid, a phone number that is likely to be a pager or answering service; and/or failure to provide all required information.
4. Unusual use or suspicious account activity that would include material changes in payment patterns, notification that the account holder is not receiving mailed statement, or that the account has unauthorized charges.
5. A request to mail something to an address that is not on file.
6. Notice received from students, victims of identity theft, law enforcement, other persons regarding possible identity theft in connection with covered accounts.

Detection of Red Flags

The detection of red flags in connection with the opening of covered accounts and the processing of existing accounts can be made through internal controls such as:

1. Obtaining and verifying the identity of a person opening and using an account
2. Authenticating consumers
3. Monitoring transactions

4. Verifying the validity of change of information requests for existing covered accounts

Response to Red Flags

CCC's Identity Theft Prevention Program shall provide for appropriate responses to detected red flags in order to prevent and mitigate identity theft. This would include:

1. Monitoring covered accounts for evidence of identity theft
2. Denying access to a covered account until other information is available to eliminate the identified red flag, or close the existing covered account
3. Notifying the consumer
4. Changing any passwords, security codes or other security devices that permit access to a covered account
5. Closing an existing account
6. Reopening a covered account with a new account number
7. Determining if no response is warranted given the particular circumstances
8. Notifying law enforcement if suspected illegal activity

Security Incident Reporting

An employee who believes that a security incident has occurred shall immediately notify their appropriate supervisor and the Director of Information Technology Services. After normal business hours, notification shall be made to the college security office.

Service Providers Oversight

The College remains responsible for compliance with the Red Flag Rules even in instances where services are outsourced to a third party. The written agreement between CCC and the third-party service provider shall require the third party to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service activities. The written agreement must also indicate whether the service provider is responsible for notifying CCC of the detection of a Red Flag or if the service provider is responsible for implementing appropriate steps to prevent or mitigate identity theft.

Program Oversight

The Director of Information Technology Services shall exercise appropriate and effective oversight over the program and shall report regularly to the President and as needed to the District Governing Board. The program administrator shall be responsible for developing, implementing and updating the Program throughout the College district. The Director of Information Technology Services shall be responsible for ensuring the appropriate training of college and district employees, reviewing staff reports regarding the detection of Red Flags and implementing steps to identify, prevent and mitigate identity theft.

Program Updating

This Program will be periodically reviewed and updated to reflect changes in risks to students and employees and the soundness of the College from identity theft related to the noted covered accounts. At least once per fiscal year, the Director of Information Technology Services, Executive Vice President and Provost will consider the College's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the College maintains and changes in the College's business arrangements with other entities, as they relate to this program. After considering these factors, the College will determine whether changes to the Program, including the listing of red flags, are warranted. If warranted, the Program will be updated.

Staff Training

College staff responsible for implementing the program shall be trained either by or under the direction of the Director of Information Technology Services, Executive Vice President and Provost in the detection of red flags, and the responsive steps to be taken when a Red Flag is detected.

References

Federal Trade Commission Red Flags Rule

Procedure History

06/09/2010 New and approved by College Council

01/18/2011 Renumbered from 307-01

Legal Review

None