2306 – Identity Theft

Summary

Barton Community College has developed this identity theft procedure pursuant to the Federal Trade Commission's Red Flags Rules.

Purpose

The procedure is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account. These procedures will aid in:

1. Identifying relevant red flags for covered accounts the college offers or maintains and incorporate those red flags into the procedure;

2. Detecting red flags that have been incorporated into the procedure;

3. Responding appropriately to any red flag that has been detected to prevent and mitigate identity theft; and

4. Ensuring the procedure is updated periodically to reflect changes in risks to students, employees, or to the safety and soundness of the College from identity theft.

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

Definitions

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

2. A Covered Account means (i) an account that a creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions or (ii) an account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft.

3. A red flag is a pattern, practice or specific activity that indicates the possible existence of identity theft.

4. Valid Photo ID - Driver's license, Passport, State or Federal Government, Military, Barton College photo ID.

5. Official Email - College sponsored email such as bartonccc.edu or bartoncougars.org.

6. Legal address – AD address as found in Banner.

College Covered Accounts

The College has identified the following covered accounts (student & employee related):

1. Federal Grants
2. Federal Student Loans
3. Federal Work Study
4. Federal Parent Loans
5. State Aid to Students
6. Institutional Aid
7. Other External Scholarships and Loans
8. Barton Student Accounts
9. Payroll

Risk Assessment

For the student related College administered covered accounts listed above, the existing risk is that a fraudulent request is made for a refund on an account with a credit balance. This is typically the result of a loan and/or direct payment. Since the College is solely responsible for issuing refunds on these accounts, the risk resides at the College level.

There is a potential risk to both student and employee payroll and the delivery of the funds to the individual that is owed the funds. Payroll procedures outline a number of options for the direction of funds that are owed to an employee.

The College will 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. However, the processes transacted by these providers represent funds owed to the College, mitigating the risk of theft to the account holders. Additionally, the College will take steps to review the Red Flag policies and procedures enacted by these providers.

Control Procedures

As noted above, the primary risk associated with the covered accounts relates to refunds and changes to student accounts and loan accounts. The following control procedures mitigate these risks, as well as other risks associated with identity theft:

1. Refunds & Requests to change information on an account:

    a. All refunds on student / employee's accounts that have a credit balance are either initiated by the college or must be initiated by the student / employee owning the account.

    b. A request for changes to the account may be initiated either in person (verified by a valid photo ID), or in writing from the student's / employee's official e-mail account.

    c. Phone requests will not be honored due to the difficulty in accessing the individual's identity.

2. Refund Check Distribution:

    a. Checks are paid and mailed to the legal name and legal address (AD Address Type) or other verified Address Type where the Source field contains PAWS, PERS, ENRL, APP, EMAL, HRDS within the Banner System or may be picked up in person.

    b. The student / employee must provide his/her valid photo ID when receiving the check in person.

    c. A student / employee may designate another individual to pick up their check, or request that the check be mailed to an address that is different from the address in Banner; however, this must be requested in writing and submitted either in person, with valid photo ID, or directly from the student's / employee's official email account.

3. Name Changes:

    a. Students / Employees must make any permanent name change by contacting the Enrollment Service's Office (students) or Human Resources Office (employees).

        i. Students - A change in a student's name requires that ~~the appropriate legal document, such as a marriage license or social security card, along with~~ a valid photo ID and a current Social Security Card be provided to Enrollment Services (mailed, emailed, faxed or in person).

        ii. Employees - A change in an employee's name requires that ~~either an original social security card, along with~~ a valid photo ID and a current Social Security Card~~, or a notarized copy of the original social security card to~~ be provided to Human resources (mailed, emailed, faxed or in person).

4. Address Changes:

    a. An individual may request a change in their legal address by one of the following methods:

        i. Submitting an address change request through the student's or employee's PAWs account.
        ii. In person (with valid photo ID).
        iii. By email from an official email address.
        iv. Faxing or mailing a change of address affidavit which has been signed, dated, and notarized.

5. Payroll Check Distribution:

    a. Full and Part time Employees may direct their payroll check to be direct deposited. The employee is to contact the Human Resources office to set up direct deposit.
    b. Full and Part time Employees may arrange with Human Resources to pick up payroll checks in person.
    c. Full and Part time employees can designate another individual to pick up their payroll check by requesting it in writing and then submitting the request to Human Resources either in person, with valid photo ID or directly from the employee's official email account.
    d. Student employee payroll checks will be available to be picked up by the student in the Business Office with the presentation of a valid photo ID.
    e. Students can designate another individual to pick up their payroll check by requesting it in writing and then submitting the request to the Business office either in person, with valid photo ID, or directly from the student's official email account.
    f. A valid photo ID is required whenever the identity of the individual picking up the check is not known.
    g. Payroll checks that are not picked up in person or direct deposited will be mailed to the legal address within the Banner System.

Red Flags

The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag is apparent, it should be investigated.

1. Documents provided for identification appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the individual presenting the identification;
3. Any request made from a non-official email address;
4. A request to mail something to an address not listed on file; and
5. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Response to Red Flags

The procedure provides appropriate responses to detect 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 or employee;
3. Change any passwords, security codes or other security devices that permit access to a covered account;
4. Notify law enforcement; or
5. Determine no response is warranted under the particular circumstances.

Oversight of the Procedure

Responsibility for developing, implementing and updating this procedure lies with the College's Dean of Administration. The Dean of Administration is responsible for the procedure administration, ensuring appropriate training of the College's staff on the procedure, reviewing any staff reports regarding the detection of red flags on the identified covered accounts 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 procedure.

Updating the Procedure

This procedure will be periodically reviewed and updated to reflect changes in risks to students, employees, and the soundness of the College from identity theft related to the noted covered accounts. At least once per fiscal year, the Dean of Administration 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 procedure. After considering these factors, the Dean of Administration will determine whether changes to the procedure, including the listing of red flags, are warranted. If warranted, the procedure will be updated.

Staff Training

College staff responsible for implementing the procedure shall be trained under the direction of the Dean of Administration or the Business Manager in the detection of red flags, and the responsive steps to be taken when a Red Flag is detected.

(Based on policy 1305; revised and approved by President on)