Red Flag - Identity Theft Prevention

FT_IT_UT_45

Responsible Officer
Rick Snider
Responsible Office
IT
Last Revision
2019-12
Re-evaluation Date
2021

Policy Statement

Identity theft is a growing problem. This policy is implemented in an effort to protect the employees and students of CU from the dangers of identity theft. The theft of an employee's network credentials, for example, can expose CU to financial loss or financial penalties due to the compromise of protected personal data.

Rationale

In response to the growing threats of identity theft in the United States, Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended a previous law, the Fair Credit Reporting Act (FCRA). This amendment to FCRA charged the Federal Trade Commission (FTC) and several other federal agencies with promulgating rules regarding identity theft. On November 7, 2007, the FTC, in conjunction with several other federal agencies, promulgated a set of final regulations known as the "Red Flags Rule". Red Flags are potential indicators or warning signs of potential or actual identity theft or similar fraud. Any time a red flag, or a situation resembling a red flag, is apparent, it should be investigated for verification.

Policy Procedures

The following are examples of red flags, which should prompt the employee to investigate and report any problems to the IT department immediately.

I. Identification of Red Flags

A. Notifications and Warnings from Credit Reporting Agencies

- Report of fraud or active duty alert accompanying a credit report;
- Notice of credit freeze in response to a request for a consumer credit report; or
- Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity, such as:
    - A recent and significant increase in the volume of inquiries;
    - An unusual number of recently established credit relationships;
    - A material change in the use of credit, especially with respect to recently established credit relationships; or
    - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor

B. Suspicious Documents

- Identification document or card that appears to be altered or forged;
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
- Other information on the identification document is not consistent with information provided by the person opening a new covered account or customer presenting the identification; or
- 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);
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example:
    - The address on an application is the same as the address provided on a fraudulent application; or

    - The phone number on an application is the same as the number provided on a fraudulent application.
- A person fails to provide complete personal identifying information on an application when reminded to do so; or
- 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

- Shortly following the notice of a change of address for a covered account, the University receives a request to change the account holder's name;
- Payments stop on an otherwise consistently up-to-date account;
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account;
- The University is notified that the customer is not receiving paper account statements; or
- The University is notified of unauthorized charges or transactions in connection with a customer's covered account.

E. Alerts from Others

Notice to the University 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.

II. Detecting Red Flags

A. Student Enrollment

In order to detect any of the red flags identified above associated with the enrollment of a full-time student on campus, CU personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, academic records, home address or other appropriate identification; and
2. Verify the student's identity at the time of issuance of student identification card by review of driver's license or other government-issued photo identification.

For students enrolled in distance education or other programs that do not take place at the University's campus and for part-time students, CU will take reasonable steps to verify the identity of those students.

B. Existing Accounts

In order to detect any of the red flags identified above for an existing account, CU personnel will take the following steps to monitor transactions on an account:

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
2. 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
3. Verify changes in banking information given for billing and payment purposes.

III. Responding to Red Flags

Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the University from the effects of identity theft. The employee should inform his/her supervisor as soon as possible that he/she has detected an actual or potential red flag, or had identified a similar area of concern of identity theft. The supervisor should notify the CIOr and conduct any necessary inquiry to determine the validity of the red flag and shall take all appropriate steps to respond and mitigate identity theft depending on the nature and degree of risk posed by the red flag, including but not limited to the following examples:

- Continue to monitor an account for evidence of identity theft;
- Contact the employee or student;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account;
- Reopen an account with a new username;
- Notify law enforcement and the CIO; or
- Determine that no response is warranted under the particular circumstances.

In all situations where it is determined that a red flag has been positively identified, the office responsible for the account shall document what occurred, describe its review of the matter and any specific actions taken to mitigate the impact of the effects of the actual or potential identity theft discovered. Such documentation shall also include a description of any additional actions taken by the office (such as updating policies and procedures) in response to the identified red flag. The office shall provide a copy of those documents to the CIO and the Institutional Effectiveness office.

IV. Address Discrepancies

Any CU office that obtains and/or uses credit reports from a Consumer Reporting Agency must ensure that it has procedures in place concerning address discrepancies. Those procedures must enable the office to form a reasonable belief that the consumer report the office has obtained relates to the consumer about whom it requested the report. A notice of address discrepancy means that the office has received notice that the address in the credit report is substantially different from the address in the CU's file on the individual.

The office may reasonably confirm the accuracy of the consumer's address by:

1. Verifying the address with the individual;
2. Reviewing its own records (e.g., applications, change of address notification forms, other customer account records) to verify the address of the consumer;
3. Verifying the address through third-party sources; or
4. Using other reasonable means.