Identity Theft Prevention Program

Red Flag Policy

Policy Overview

Clarkson College developed this Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This program was developed with oversight and approval of the Clarkson College Board of Directors. It is the policy of Clarkson College to comply with the procedures set forth below. Clarkson College shall implement a program to detect activities indicative of potential identity theft (i.e. "Red Flags") to prevent their occurrence. In the event identity theft does occur, Clarkson College shall quickly respond to mitigate harm.

Definitions

"Covered Account" means (i) an account that Clarkson College offers or maintains primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions and (ii) any other account that Clarkson College offers or maintains for which there is a reasonably foreseeable risk of identity theft to the customer (i.e. students and/or parents).

"Creditor" means any person or organization that extends, renews or continues credit, including the College who accepts multiple payments over time for services rendered.

"Identity Theft" is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else.

"Red Flag" means a pattern, practice or specific activity that could indicate identity theft.

"Red Flag Alert" means any mechanism or tool that makes all relevant employees aware that there may be a potential identity theft problem.

"Service Provider" means a vendor that provides services directly to Clarkson College related to Covered Accounts.

Covered Accounts

Covered accounts maintained by Clarkson College include but are not limited to the following:

- Student accounts
- Student loans.

Red Flags

Identifying Red Flags

Clarkson College shall identify and respond to Red Flags, which may indicate potential identity theft. Red Flags include but are not limited to the following:

1. Alerts, notifications or warnings from a consumer-reporting agency, including notices of credit freezes, notices of address discrepancies, and receipts of consumer reports showing patterns of activities that are inconsistent with the history and usual pattern and activity of the account holder.
2. Address discrepancies that cannot be explained. For example, changing an address more than once a year would not be considered a red flag action at Clarkson College when done through our authenticated site. However, it might constitute suspicious activity at a financial institution whose account holders do not change residences as often as college students.
3. Suspicious documents, including:
    a. photographs or physical descriptions that is inconsistent with the individual presenting the document;
    b. incomplete, altered, forged or inauthentic documents; or
    c. other personal identifying information that is inconsistent with information on file with Clarkson College.
4. Complaints or questions from students, guardians or customers about charges to a covered account for goods/services they claim were never received.
5. Suspicious activity related to Covered Accounts, including:
    a. unusual use of accounts that have been previously inactive for a lengthy period of time;
    b. mail being returned as undeliverable although transactions continue to be conducted in connection with the covered account; or
    c. unauthorized account changes or transactions.
6. Notice from customers, victims of identity theft, law enforcement authorities or other individuals regarding possible identity theft in connection with College Covered Accounts.

Response to Red Flag Detection(s)

Appropriate action should be taken when red flags are detected to confirm the identity of individuals when they open and/or access their covered accounts. The appropriate action(s) from the list that follows will depend on the particular covered account at issue and the relevant circumstances.

1. Appropriate personal identifying information (e.g., photo identification, date of birth, academic status, user name and password, address, etc.) shall be obtained from the individual account holder prior to issuing a new or replacement identification card, to opening a covered account or to allowing access to a covered account.
2. When certain changes to a covered account are made online, individuals holding covered accounts shall receive notification to confirm the change was valid and to provide instruction in the event the change is invalid.
3. Suspicious changes made to covered accounts that relate to an account holder's identity, administration of the account, or billing and payment information shall be verified.

Other actions will be taken by College personnel involved in the administration of covered accounts based on the covered account and the circumstances surrounding the detection of red flags. These actions may include one or more of the following:

1. Monitor a covered account for evidence of identity theft;
2. Contact individual account holder(s);
3. Request additional documentation from the individual account holder to verify identity;
4. Change passwords, security codes and other security devices permitting access to the covered account;
5. Close an existing covered account;
6. Notify law enforcement;
7. Take appropriate steps to modify the applicable process to prevent similar activity in the future;
8. Determine that no response is warranted under the particular circumstances.

Additional Program Information

Oversight of Service Providers

Clarkson College may contract with vendors to provide services related to Covered Accounts. The contracting department shall maintain written certification from the vendor stating it complies with FACTA Red Flag Rule regulations. The department shall investigate any service provider occurrences indicating a potential lack of compliance, and take any necessary actions to mitigate potential risk.

Program Education

All departments managing Covered Accounts shall provide education to current staff members and new hires on this policy and any internal department procedures created to implement it on an annual basis.

Program Updates

Clarkson College will periodically review and update this Program to reflect changes in risks to students and the soundness of the College from Identity Theft. In doing so, the College will consider its experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in College business arrangements with other entities. After considering these factors, the College will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the College will update the Program.

Privacy/Security Incident Response

In the event of a major incident involving identity theft, the Information Security Incident Response policy shall be followed (Policy IT-D4).

Responsible Party

Clarkson College Controller.