Rock Valley College

Red Flag Identity Theft Prevention Program

RVC Administrative Procedure (2:10.060)

Program Adoption

Rock Valley College ("the College") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size and complexity of the College's operations and account systems, and the nature and scope of the College's activities, the Rock Valley College administration determined that this program was appropriate for the College.

Rock Valley College Identity Theft Prevention Program Requirement

Rock Valley College participates in the Direct Student Loan Program, offers institutional loans to students, and administers a tuition payment plan that allows qualified students to pay their tuition and fees throughout the semester. Therefore, the College is a creditor and student accounts are covered accounts subject to the Red Flags Rule which requires the College to develop and implement an identity theft prevention program.

The Red Flags Rule allows Rock Valley College to design and implement an identity theft prevention program that is appropriate to our size, complexity, and the nature of our operation. Programs must contain reasonable policies and procedures to:

- identify relevant "Red Flags" and incorporate them into the program
- detect the red flags that the program incorporates;
- respond appropriately to detected red flags to prevent and mitigate identity theft; and
- ensure that the program is updated periodically to reflect changes in risks.

Definitions and Program

A. Red Flags Rule Definitions Used in this Program

"Identity Theft" is a "fraud committed or attempted using the identifying information of another person without authority."

A **"Red Flag"** is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

A **“Covered Account”** is any account the College offers or maintains that involves or is designed to permit multiple payments or transactions and any other account that the College offers or maintains for which there is a reasonably foreseeable risk to the customer or to the safety and soundness of the College from identity theft. (Based on current practices of the College, the accounts referenced would include all student accounts, academic or financial, or accounts established through extensions of credit that are administered by the College.)

A **“Creditor”** is defined as someone who regularly extends, renews, or continues credit. Rock Valley College is considered a creditor due to our participation in the following activities:

- Offering a plan of payment or fees throughout the semester, rather than requiring full payment at the beginning of the semester.

“Program Administrator” is the individual designated with primary responsibility for oversight of the program. See Section VI below. “Personal information” is “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including: name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer’s Internet Protocol address, or routing code.

B. Identification of Covered Accounts

The College will periodically determine whether it maintains covered accounts by conducting risk assessment taking into account the methods it provides to open and access its accounts and its previous experience with identity theft.

C. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, the College is required to establish an “Identity Theft Prevention Program” tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts 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 Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students or college personnel or to the safety and soundness of the student or college personnel from Identity Theft.

Identifications of Red Flags

In order to identify relevant Red Flags, the College considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The College identifies the following Red Flags in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of an active-duty alert for an applicant;
4. Receipt of a notice of address discrepancy in response to a credit report request; and
5. Indication for a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic;
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
3. Other document with information that is not consistent with existing student or college personnel information; and
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the student or college personnel provides (example: inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on an application);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

5. Social security number presented that is the same as one given by another student or college personnel;
6. An address or phone number presented that is the same as that of another person and not within reason of being the same information;
7. A person fails to provide required personal identifying information on an application when reminded to do so; and
8. A person's identifying information is not consistent with the information that is on file for the student or college personnel (electronic or paper).

D. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the student or college personnel's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use.
4. Mail sent to the student or college personnel is repeatedly returned as undeliverable;
5. Notice to the College that student or college personnel is not receiving mail sent by the College;
6. Notice to the College that an account has unauthorized activity;
7. Breach in the College's computer system security; and
8. Unauthorized access to or use of student or college personnel account information.

E. Alerts from Others

Red Flag

1. Notice to the College from student or college personnel, 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

A. Student Enrollment

In order to detect any of the Red Flags identified above associated with the enrollment of a student, College personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

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

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing Covered Account, College personnel will take the following steps to monitor transactions on an account:

Detect

1. Verify the identification of students or college personnel 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 or college personnel a reasonable means of promptly reporting incorrect address changes (in accordance with the student or college personnel address change procedure); and
3. Verify reasons for changing banking information given for billing and payment purposes as processed through the payment plan system and are unsuccessful in changing the information through the system themselves.

C. Consumer ("Credit") Report Requests

In order to detect any of the Red Flags identified above for an employment, volunteer or any other position for which a credit or background report is sought, College personnel will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that the notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the university has reasonably confirmed is accurate.

Preventing and Mitigating Identity Theft

In the event College personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

1. Continue to monitor a Covered Account for evidence of Identity Theft;
2. Contact the student or college personnel as applicable per situation;
3. Reset any passwords or other security devices that permit access to Covered Accounts;
4. Provide the student or college personnel with a new student or college personnel identification number in person with proper identification;

5. Notify the Program Administrator for determination of the appropriate step(s) to take;
6. Notify law enforcement;
7. File or assist in filing a Suspicious Activities Report ("SAR"); or
8. Determine that no response is warranted under the particular circumstances.

Protect Student or College Personnel Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the College will take the following steps with respect to its internal operating procedures to protect student or college personnel identifying information:

1. Ensure that the College's website is secure or provide clear notice that the website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing student or college personnel account information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to Covered Account information are password protected;
4. Avoid use of social security numbers;
5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of student or college personnel information that are necessary for College purpose.

Program Administration

A. Oversight

Responsibility for developing, implementing and updating this Program lies with a Red Flag Identity Theft Committee ("Committee") for the College. Each representative from this committee will be responsible for ensuring appropriate training of their staff on the Program. The Director of Network Operations, as the Program Administrator, will review any staff reports regarding the detection of Red Flags 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 Program.

B. Staff Training and Reports

College staff responsible for implementing the Program shall be trained either by or under the direction of their department's representative on the Red Flag Identity Theft Committee in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. College staff shall be trained, as necessary, to effectively implement the Program. College employees are expected to notify their supervisor once they become aware of an incident of Identity Theft or of the College's failure to comply with this Program. At least annually or as otherwise requested by the Program Administrator, College staff responsible for development, implementation, and administration of the Program shall report to the Director of Network Operations on compliance with this Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

The College will utilize a training platform to provide departmental training as determined by administration.

C. Service Provider Arrangements

In the event the College engages a service provider to perform an activity in connection with one or more Covered Accounts, the College will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the College's Program and report any Red Flags to the College employee with primary oversight of the service provider relationship.

D. Non-Disclosure of Specific Practices

For the effectiveness of this Identity Theft Prevention Program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices may need to be limited to the Committee who developed this Program and to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be shared with other RVC employees or the public. The Executive Director of Finance shall inform the Committee and those employees with a need to know the information of those documents or specific practices, which should be maintained in a confidential manner.

E. Program Updates

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

F. Component Units of the College

As a component unit of the College, the Rock Valley College Foundation will adhere to the same Program as defined the College. The Foundation is considered a "creditor" in terms of offering a deferred payment method to donors for pledges receivable. A "covered account" is then created as multiple transactions or payments are then received through the Foundation's business operations. There is foreseeable identity theft risk in providing this option for donors, therefore, will require identifying, detecting, preventing, and mitigating red flags as defined in the College's Red Flag Program.

G. Red Flag Identity Theft Committee Members

The members of the Red Flag Identity Theft Committee are the Vice President of Finance CFO, Executive Director of Financial Services, Director of Records and Registration/Registrar, Executive Director of Financial Aid, Manager of Accounts Receivable, Executive Director of IT and the Dean of Enrollment Services.

Reference: Board Report 6594
Implemented: June 9, 2025
Revised: June 9, 2025