

Red Flag Rules

Identity Theft Prevention Program Training Guide



Why do you need training?

- The Federal Trade Commission (FTC) regulates financial transactions at VCCS.
- The FTC has defined VCCS as a *creditor*.
- The FTC has determined that all *creditors* must comply with the Red Flags regulation and by law must train certain respective employees that could come in contact with a “Red Flag”.

What will I gain from this?

- By completing this training module you will gain:
 - Knowledge of what is a Red Flag
 - Knowledge of what is a “covered account”
 - Knowledge of the different types of Red Flags and how they can present themselves
 - Knowledge of what to look for and where to look in detecting a Red Flag
 - Knowledge of what process to follow in case you should detect a Red Flag
 - Knowledge of whom to contact

So what is a Red Flag?

- In simple terms, a Red Flag is an indication or warning that a fraudulent transaction or event could be occurring as a result of identity theft.



Why is this needed?

- Identity thieves use personal identifying information to open new accounts and misuse existing accounts, creating havoc and fraud, costing consumers and businesses billions of dollars every year.
- Even though we continually put safeguards in place to prevent ID theft, criminals are becoming more sophisticated and educated everyday in obtaining this information fraudulently.
- The Red Flag regulation is designed to assist in detecting when ID theft might be happening and reduce its consequences. The Federal Government requires us to comply with this regulation.

What does the FTC say we must do?

According to the FTC, by law, we must be able to do the following:

- IDENTIFY areas of exposure to ID theft and what types of events within those areas could be interpreted as Red Flags – what to look for.
- DETECT when these Red Flag indicators might be present.

What does the FTC say we must do?

- PREVENT and MITIGATE the exposure of financial or personal loss to the VCCS and to the customer who might have been a victim of ID theft by investigating the detected Red Flags for actual fraud and responding quickly and appropriately if fraud does indeed exist.
- TRAIN our employees on how to accomplish all of this.

What is a “covered account”?

- A “covered account” is a customer account that has been identified as having the possibility of a Red Flag occurrence and must be monitored for the detection of a Red Flag.
- There are 2 types of covered accounts.
- The first type deals with **individuals**. Any account that allows an individual to pay for a service or product over time with multiple payments is considered a covered account. An example is an extended payment schedule for tuition costs.

What is a “covered account”?

- The second type deals with any **customer account** that allows small businesses or individuals to purchase products or services that are not paid in full at the time of the service or sale. These accounts could be considered covered accounts, depending upon the overall risk factors involved. As an example, this may apply to businesses that the VCCS provides services to every month, but only bills them at the end of the month.

Identity thieves may steal the following items:

- Address
- Telephone number
- Social Security card
- Date of birth
- Government issued driver's license or identification number
- Alien registration number
- Government passport number
- Employer or taxpayer identification number
- Individual identification number
- Computer's Internet Protocol address
- Bank or their financial account routing code
- Student identification number issued by VCCS

So we need to pay attention to them...

What should you look for?

- A Red Flag may indicate that identity theft has occurred and fraud could be in progress.
- Red Flags come in 5 categories...
 - Notifications and Warnings from Consumer Reporting Agencies
 - Suspicious Documents
 - Suspicious Personal Identifying Information
 - Suspicious Covered Account Activity or Unusual Use of Account
 - Alerts from Others

General Training – Notifications and Warnings from Consumer Credit Bureaus

■ Examples:

- A fraud alert has been included with a consumer credit report from a credit bureau.
- A notice or report from the credit bureau of an active duty alert for an applicant.
- A consumer credit bureau provides a notice of address discrepancy.
- A credit report of activity that is inconsistent with an applicant's usual pattern or activity, such as an increased number of accounts or inquires.

General Training – Suspicious Documents

Examples:

- Documents provided for identification that appear to be altered, forged or inauthentic.
- Photograph on ID does not match the appearance of the individual or does not look like the individual.
- Information on ID does not match the information provided by the person opening the account.
- Application appearing forged, altered, or destroyed and reassembled.

General Training - Suspicious Personal Identity Information

- Examples:
 - Information on an ID does not match any address in the consumer report.
 - The Social Security number has not been issued or appears on the Social Security Administration's Death Master File (a file of information associated with Social Security numbers of those who are deceased).
 - There is a lack of correlation between the Social Security number provided and the range for the date of birth.
 - Personal indentifying information that is provided is associated with known fraud activity.

General Training - Suspicious Personal Identity Information

■ Examples (cont.)

- A suspicious address is supplied, such as a mail drop or prison.
- A phone number associated with pagers or answering service is given.
- A duplicate Social Security number is provided that matches one submitted by another person opening an account or another customer with an existing account.
- Duplicate addresses or phone numbers that match others are supplied by a large number of applications.

General Training - Suspicious Personal Identity Information

- Examples (cont.)
 - The person opening the account is unable to supply identifying information when told that the application is incomplete.
 - The applicant's personal information is inconsistent with information already on file.
 - The person opening an account or an existing customer is unable to correctly answer challenge questions.

General Training – Suspicious Covered Account Activity

■ Examples:

- Shortly after a change of address on an account you receive a request for additional users of the account.
- You notice a drastic change in payment patterns, use of available credit, or spending patterns on an account.
- You notice that an account that has been inactive for a long time suddenly has lots of unusual activity.

General Training – Suspicious Covered Account Activity

■ Examples (cont.)

- You notice that mail that has been sent to a customer is repeatedly returned as undeliverable despite transactions continuing to occur on the account.
- You are notified that a customer is not receiving his/her account statements.
- You are notified of unauthorized charges or transactions on a customer's account.

General Training – Alerts from Others

■ Examples:

- Notice to the college from a student, 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.

General Training – Where can Red Flags be detected?

- The opening of a customer account, such as a student long term or short term loan or the activation of a campus card.
- The ongoing monitoring of one of these customer accounts for suspicious activities.
- General correspondence with a customer – written or verbal.
- Information received from Credit Agencies or Credit Bureaus that might lead you to be suspicious that there could be an identify theft problem.

General Training – How to Detect Red Flags

■ Examples:

- Verify identities when opening customer accounts or performing customer transactions.
- Monitor ongoing transactions of customer account, such as campus card transactions.
- Verify the validity of any change to address or bank routing information or other relevant information to a customer account.
- Watch for credit bureau report warnings.
- **BE AWARE** – identity fraud is all around us.

General Training – Prevent and Mitigate

- You need to act quickly.
- First consult the VCCS business and departmental procedures for individual departmental investigation instructions.
- Gather all related information and documentation associated with the situation.
- Escalate to a supervisor if your investigation does not eliminate the possibility that a fraud or ID theft may be occurring.
- If your investigation determines that the Red Flag is triggered by a normal and usual customer request or a general mistake, no action may be necessary – together than correcting the item in questions.

General Training – Prevent and Mitigate

- The supervisor will complete a Red Flag Suspicious Activities Report if the situation can not be resolved, or if it is determined that a possible fraud or ID theft may be occurring.
- The Suspicious Activities Report will be forwarded to the Program Administrator who is responsible for the operation of the VCCS Red Flag Program.
- If it is determined that a fraud or ID theft has actually been detected, then the owner of any comprised account **MUST** be notified by the Program Administrator.

General Training – Prevent and Mitigate

- Subsequent actions by the Program Administrator may include:
 - Notifying in writing the original customer/vendor/supplier/student of all ongoing investigations and outcomes
 - Notifying proper government or law enforcement entities and utilizing such for an ongoing investigation
 - Taking all actions required by law in handling a fraudulent account as defined by the FTC, the VCCS, and any local, state, or federal laws
 - Maintain all suspicious activities reports and pertinent information for reporting purposes and future references

General Correspondence

- All correspondence, written or verbal, both to and from a customer, vendor, or supplier, could indicate a red flag and possible ID fraud. The following are examples of such correspondence:
 - Mail sent to a customer/vendor/s supplier is repeatedly returned as undeliverable despite ongoing transactions on an active account.
 - You are notified that a customer/vendor/supplier is not receiving account statements or payments.
 - You are notified of unauthorized charges, transactions, or modifications on customer/vendor/supplier accounts.
 - You are notified that a fraudulent account for a person engaged in identity theft has been opened at VCCS.

Third Party Contracts

- All managers/supervisors must exercise appropriate and effective oversight of service provider or third party arrangements.
- There are certain service providers who may be the only ones that are able to detect Red Flags. Examples are debt collectors that may be hired to contact customers for outstanding debts. Another example could be an agency that collects payments for VCCS. These types of service providers must have a defined and implemented Red Flag Program and must certify as such to the VCCS via the contract agreement.

Third Party Contracts

- Examples within the VCCS of such service providers include, but are not limited to:
 - Financial Aid
 - Private collection agencies utilized by the VCCS for past due receivables

Student Accounts and Long Term Student Loans

- The following Red Flag could be detected when monitoring Student Accounts:
 - A request for withdrawal (drop all classes) when a refund is required shortly after a change of relevant information.

Student Accounts and Long Term Student Loans

- When dropping all classes or reducing the schedule such that a refund is warranted:
 - In order to process the request immediately, it must be done in person such that visual verification of the student is possible.
 - Two forms of ID should be utilized.
 - If it is not possible that the requesting student make the request in person, then a hold on any refunds should be placed for a period of time to ensure that a change of relevant information on the account has not erroneously occurred prior to the refund request.

Short Term Student Loans

- The following Red Flags could be detected when monitoring and processing Student Short Term Loans:
 - Presentation of suspicious documents when requesting a short term loan
 - Presentation of mismatched photo ID card
 - Request for an electronic disbursement immediately after a change of electronic routing information in the student's on line data base account.

Short Term Student Loans

- When distributing a short term loan the following must occur:
 - If the loan is from another department, a signed authorization form must be presented by the student. The department should have verified the identity of the student prior to approving.
 - Only the student authorized to receive the loan will be allowed to physically obtain the money. Third party authorization forms for individuals to receive another's loan proceeds will not be permitted.

Short Term Student Loans

- A government issued picture ID must be presented prior to any distribution of money and must be verified by the person administering the disbursement. If there seems to be an identification problem then a supervisor must be informed.
- Electronic disbursements will only be sent to the current banking information on file for the student. Care must be taken in determining if that information has recently been changed.

Credit Agency Reports

- In addition to Red Flags for covered accounts, any area that receives a notice from a consumer reporting agency or credit bureau that states the address furnished by the VCCS is different than that in the agency's files, must implement the following:
 - An investigation must occur to insure the report is for the person intended. This could include:
 - Verifying the address with the consumer about whom the report was requested
 - Reviewing existing records that may be already on file for this person
 - Verifying the address through a third party source
 - Using other reasonable means

Credit Agency Reports

- If the report is indeed for whom it was intended, the consumer must be contacted and informed of the address discrepancy.
- The Agency must be informed of the correct and verified address of the consumer.
- This includes employee, student, and customer accounts.
- Also, any 3rd party vendor or supplier that the college utilizes in obtaining or interpreting consumer reports must also certify via contract agreement that they have a Red Flag Policy and Program implemented.

Updates to the Red Flag Program

- The Red Flag Rules Committee has assessed various areas within the VCCS and has identified areas that contain covered accounts and defined Red Flags within these accounts.
- If you believe that there are other accounts that could qualify as covered accounts and should be included in the Red Flag Program, please contact the Program Administrator or any member of the Red Flag Rules Committee.
- Once a year (at a minimum), the program administrator of the Red policy will need to review and update to reflect changes in risks to students and the soundness of the colleges from identity theft. If warranted, the program will need to be updated.

Training

- The Program Administrator will train relevant staff to implement the identity theft prevention program effectively.

A Real Example of a Red Flag:

- High school student was notified by the college that her SSN already exist with another student at another college when she applied to take dual/concurrent classes at the college. The mother brought in daughter's original SS card and both showed ID. Mother stated she had been notified by her bank that another individual was using her daughter's SSN. Bank had made required security protection for her and she had reported this to local authority and credit bureaus. The other VCCS school was notified that we had official proof and they removed the SSN under the other person. The other person could not be reached to ask for proof per the other school since they had not attended that college in many years. The mother stated they were already aware of the name of the person and authorities were trying to find him but we didn't provide her the name. We also placed FERPA block on student's account so no 3rd party information would be given.

Contacts

- A Program Administrator should be assigned at each college from one of the following areas:
 - Financial Aid Office
 - Admissions & Records
 - Business Office