FACTA Red Flags – Identity Theft Prevention

Lesson 1: Objectives

Upon completion of this course, you will be able to:

- Detect and appropriately respond to Red Flags to prevent and mitigate identity theft.

Introduction

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act or FACTA) requires that financial institutions and creditors have a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of an account or any existing account. Identity theft is fraud that is committed or attempted using a person's identifying information without authority. Any account which permits multiple payments or transactions and is primarily for personal, family, or household purposes, or in which there is a reasonably foreseeable risk from identity theft to customers or to the safety and soundness of an organization must be protected. The organization must identify patterns, practices, and specific activities that indicate the possible existence of identity theft, referred to as Red Flags, and train their employees on the detection and response to these Red Flags. Although FACTA applies specifically to financial institutions and creditors, every organization that handles customer accounts should be aware of the Red Flags that apply to its business.

Your organization provides oversight of its Identity Theft Prevention Program including the review of compliance reports, approval of changes, and oversight of service provider agreements, as applicable.

Lesson 2: Identity Theft Prevention Program

There are four basic elements of an Identity Theft Prevention Program: the identification of relevant Red Flags, detection of Red Flags, response to Red Flags to prevent and mitigate identity theft, and periodic updating.

Identification and Detection of Red Flags

In identifying relevant Red Flags for its accounts, an organization considers the types of accounts it offers or maintains, the methods it provides to open and access accounts, and its previous experiences with identity theft. Organizations also incorporate Red Flags from a variety of sources such as previous incidences of identity theft; methods of identity theft that change its risks; and supervisory guidance. Red Flags may also be identified through warnings received by consumer reporting agencies; the presentation

of suspicious documents or personal identifying information; the unusual use of an account; or a notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft. Each of these Red Flags will be explained in more detail in the following sections. You should be familiar with the Red Flags that are applicable to your organization so you can detect and respond appropriately when obtaining identifying information about, and verifying the identity of, a person opening an account or authenticating customers, monitoring transactions, and verifying the validity of change of address requests for existing accounts.

Alerts, notifications, or other warnings from a consumer reporting agency may indicate a Red Flag. For example,

- A fraud or active duty alert.
- A notice of credit freeze, address discrepancy, or an inconsistent pattern of activity when compared with the history and usual pattern of activity of a customer, 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; or
    - An account that was closed for cause or identified for abuse of account privileges.

The presentation of suspicious documents may indicate a Red Flag. For example,

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the customer.
- Other information on the identification is not consistent with information provided by the customer or with information that is on file with the organization, such as a signature card or check.
- An application appears to have been altered or forged or gives the appearance of having been destroyed and reassembled.

The presentation of suspicious personal identifying information by the customer may indicate a Red Flag. For example,

- Personal identifying information provided is not consistent with external information sources. For example, the address does not match the address on the consumer report; or the Social Security number has not been issued or is listed on the Social Security Administration’s Death Master File.

- Personal identifying information provided is not consistent with other information provided by the customer. For example, there is a lack of correlation between the Social Security number range and date of birth.
- Personal identifying information provided is associated with known fraudulent activity. For example, the address or phone number on the application is the same as the address or phone number provided on a fraudulent application.
- Personal identifying information provided is of a type commonly associated with fraudulent activity, such as a fictitious address, a mail drop, or a prison; or an invalid phone number or one that is associated with a pager or answering service.
- The Social Security number provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- The person opening the account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with information that is on file with the organization.
- The person opening the account or the customer cannot answer challenge questions or provide authenticating information beyond that which generally would be available from a wallet or consumer report.

The unusual use of, or other suspicious activity related to, an account may indicate a Red Flag. For example,

- Shortly following a notice of a change of address for an account, the organization receives a request for a new, additional, or replacement card or cell phone, or for the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:
    - The majority of available credit is used for cash advances or merchandise that is easily convertible to cash; or
    - The customer fails to make the first payment or makes an initial payment but no subsequent payments.
- An account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example,
    - A nonpayment when there is no history of late or missed payments;
    - A material increase in the use of available credit;
    - A material change in purchasing or spending patterns;

    - A material change in electronic fund transfer patterns in connection with a deposit account; or
    - A material change in telephone call patterns in connection with a cellular phone account.
- An account that has been inactive for a reasonably lengthy period of time is used.
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.
- The organization is notified that the customer is not receiving paper account statements.
- The organization is notified of unauthorized charges or transactions in connection with a customer's account.

Quiz Question:

Match the Red Flag to its example:

Alerts, notifications, or other warnings from a consumer reporting agency = *A notice of an inconsistent pattern of activity when compared with the history and usual pattern of activity of a customer.

The presentation of suspicious documents = *Documents provided for identification appear to have been altered or forged.

The presentation of suspicious personal identifying information by the customer = *The Social Security number provided is the same as that submitted by other persons opening an account or other customers.

The unusual use of, or other suspicious activity related to, an account = *An account that has been inactive for a reasonably lengthy period of time is used.

Lesson 3: Responding to Red Flags

It is critical that you respond appropriately to a detected Red Flag in order to prevent or mitigate identity theft. Your response should be in proportion with the risk of identity theft. Appropriate responses may include:

- Monitoring an account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to an account;
- Reopening an account with a new account number;

- Not opening a new account;
- Closing an existing account;
- Not attempting to collect on an account or not selling an account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is needed under the circumstances.

Quiz Question:

Select **all** of the responses that may be appropriate when a Red Flag is detected:

a. *Monitoring an account for evidence of identity theft.
b. *Contacting the customer.
c. *Changing any passwords, security codes, or other security devices that permit access to an account.
d. *Reopening an account with a new account number.
e. *Not opening a new account.
f. *Closing an existing account.
g. *Not attempting to collect on an account or not selling an account to a debt collector.
h. *Notifying law enforcement.
i. *Determining that no response is needed under the circumstances.

Lesson 4: Additional FACTA Requirements

FACTA requires credit and debit card issuers validate a change of address request when there is a request for additional or replacement cards within a short period of time from the original request. In these cases, a new card may not be issued unless the organization notifies the cardholder of the change of address request at the cardholder's former address or by any other agreed upon means of communication, and provides to the cardholder a reasonable means of promptly reporting an incorrect address change.

FACTA also requires organizations that request consumer reports have policies and procedures regarding a notice of address discrepancy by the consumer reporting agency and methods to determine whether the report belongs to the correct consumer. Methods may include comparing the information in the consumer report with the information the organization obtains and uses to verify the consumer's identity in accordance with Customer Information Program requirements; maintains in its own records, such as applications, change of address notifications, other customer account

records; or obtains from third-party sources. The organization may also verify the information in the consumer report with the consumer. The organization must give the consumer reporting agency an address for the consumer that the organization has reasonably confirmed is accurate.

Lesson 5: Updating the Identity Theft Prevention Program

Organizations should update its Identity Theft Prevention Program periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft, based on factors such as:

- The experiences of the organization with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that the organization offers or maintains; and
- Changes in the business arrangements of the organization.

Lesson 6: Conclusion

(NOTE: You may wish to display the contact information for the appropriate personnel within your organization.)

Employees must be able to detect and appropriately respond to Red Flags to prevent and mitigate identity theft. If you have any questions, contact the appropriate personnel within your organization.

Test Questions (10 questions Pre-Test or 5 questions Post-Test)

Pool 1 (6 or 3 questions)

MULTIPLE CHOICE

1. The four basic elements of an Identity Theft Prevention Program include:

    a. The identification and detection of Red Flags.
    b. The response to Red Flags.
    c. Periodic updating.
    d. All of the above.

2. In identifying relevant Red Flags, an organization considers:

    a. The types of accounts it offers or maintains.
    b. The methods it provides to open and access accounts.
    c. Its previous experiences with identity theft.
    d. All of the above.

3. Organizations incorporate Red Flags from a variety of sources such as:

    a. Previous incidences of identity theft.
    b. Methods of identity theft that change its risks.
    c. Supervisory guidance.
    d. All of the above.

4. Which of the following may indicate a Red Flag?

    a. Documents provided for identification appear to have been altered or forged.
    b. The photograph on the identification is not consistent with the appearance of the customer.
    c. The application appears to have been destroyed and reassembled.
    d. All of the above.

5. Which of the following may indicate a Red Flag?

    a. The person opening the account cannot answer challenge questions beyond that which generally would be available from a wallet or consumer report.

b. Personal identifying information provided is consistent with other information provided by the customer.
c. Personal identifying information provided is consistent with external information sources.
d. Personal identifying information provided is consistent with information that is on file with the organization.

6. Which of the following is an inappropriate response to a detected Red Flag?

a. Not opening a new account.
b. Verbally accusing the customer of identity theft.
c. Closing an existing account.
d. Determining that no response is needed under the circumstances.

Pool 2 (4 or 2 questions)

TRUE/FALSE

7. Identity theft is fraud that is committed or attempted using a person's identifying information without authority.

8. Red Flags are patterns, practices, and specific activities that indicate the possible existence of identity theft.

9. FACTA requires that financial institutions and creditors detect, prevent, and mitigate identity theft in connection with the opening of an account or any existing account.

10. Red Flags may be identified through warnings received by consumer reporting agencies.

11. Red Flags may be identified through the presentation of suspicious documents.

12. Red Flags may be identified through the presentation of suspicious personal identifying information by the customer.

13. Red Flags may be identified through the unusual use of an account.

14. Red Flags may be identified through a notice from a customer regarding possible identity theft.