Red Flags 101
What It’s All About

Section’s 114 and 315 of the FACT Act were implemented in October 2007 and became effective January 1, 2008. These sections of the Fair and Accurate Credit Transaction Act, required financial institutions to establish a written program, develop policies and procedures and train appropriate personnel.

That’s You!!
Section 114 deals with the Red Flag Guidelines which are designed to help detect, prevent and mitigate Identity Theft issues that may arise during the course of business.

Section 315 deals with address discrepancies and steps that must be taken to reconcile the matter.
What It Means To You

- As an employee of this institution, it is essential that all the necessary steps are taken to protect our customer’s from Identity Theft and be there for them, should an instance of ID Theft occur.

How can you do this? Easy! Watch for the Red Flags and follow policies and procedures!
So, what are these Red Flags ???

- There are 26 Red Flags lumped in to 5 categories:
  - Alerts, Notifications or Warnings from a consumer reporting agency
  - Suspicious documents
  - Suspicious personal identifying information
  - Unusual use of , or suspicious activity related to the covered account
  - Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor
Alerts, Notifications or Warnings From a Consumer Reporting Agency

1 - A fraud alert or active duty alert is included with a consumer report.

2 – A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3 - A consumer reporting agency providing a notice of address discrepancy.
Alerts, Notifications or Warnings From a Consumer Reporting Agency

4 – A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
   a. A recent and significant increase in the volume of inquiries;
   b. An unusual number of recently established credit relationships;
   c. A material change in the use of credit, especially with respect to recently established credit relationships; or
   d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
Suspicious Documents

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

   a. The address does not match any address in the consumer report; or

   b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration’s Death Master File.
Suspicious Personal Identifying Information

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

   a. The address on an application is the same as the address provided on a fraudulent application; or

   b. The phone number on an application is the same as the number provided on a fraudulent application.
Suspicious Personal Identifying Information, continued...

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

   a. The address on an application is fictitious, a mail drop, or a prison; or
   b. The phone number is invalid, or is associated with a pager or answering service.
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
Suspicious Personal Identifying Information, continued…

16. The person opening the covered 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.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
Suspicious Personal Identifying Information, continued…

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
Unusual use of, or suspicious activity related to, the covered account.

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
Unusual use of, or suspicious activity related to, the covered account

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
   a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); Or
   b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
Unusual use of, or suspicious activity related to, the covered account, cont...

21. A covered 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;
   b. A material increase in the use of available credit;
   c. A material change in purchasing or spending patterns;
   d. A material change in electronic fund transfer patterns in connection with a deposit account; or
   e. A material change in telephone call patterns in connection with a cellular phone account.
Unusual use of, or suspicious activity related to, the covered account, cont…

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer’s covered account.
Unusual use of, or suspicious activity related to, the covered account, cont…

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer’s covered account.
Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
By now, you should be familiar with these red flags and the new policies and procedures that are in place to help this institution detect, prevent and mitigate Identity Theft.

Let’s Try Some Scenario's!
An individual comes to you and says they would like to open a new account. While getting the necessary documents needed to open the account, you notice that the photo on the drivers license differs greatly from the appearance of the person in front of you. This is considered a Red Flag. What should you do?

A. Ignore it. You’re sure everything is fine.
B. Turn to Bank procedure, as this is a indicator of possible ID Theft. Possible outcomes: SAR will be filed and the account will not be opened until the identity of the individual can be firmly determined.
Mr. Smith has been a long time customer of yours. He always pays his payments on time but this month, he appears on your late payment report.

Is this considered a Red Flag?

Yes! Mr. Smith’s normal pattern and practice has deviated and should not be taken lightly. Turn to policies and procedures for the appropriate steps to take. This may include contacting the customer and thoroughly documenting the conversation.
A consumer credit report is pulled for an applicant. The report states that there is an address discrepancy but you personally know the applicant and the address given is the correct one. Do you need to do anything?

Of course! It is your responsibility to report the correct address to the consumer credit reporting agency and document that you took the necessary steps to identify the correct address. This may involve completing a checklist on how the correct address was established. Policy and procedure should direct you explicitly.
Mr. Foster notifies you that he hasn’t been getting his statements lately. He states that it’s probably just the new mail carrier and not to worry; He’ll just take a print-out of his account.

He’s not worried. Should you be?  

YES!

This is considered a Red Flag and should be investigated. Perhaps Mr. Foster’s missing statements are due to his identity being stolen and not just the new mail carrier. Look to Bank policies and procedures for the necessary steps to take.
From the scenario’s provided, you can clearly see that Red Flags can affect all areas of the institution from the teller line to the closing table; from consumer to commercial customers.

Don’t be afraid to question something that doesn’t feel right. You may be saving someone from becoming the next victim of Identity Theft!