| RED FLAG / RESPONSE FORM – NEW ACCOUNTS | | | |
|---|---|---|---|
| Customer Name(s):<br>Account Number: | | Date: | |
| **Red Flag Category (indicate by number)** | **Procedure** | **Comments & Explanation:** | |
| Alerts & Notifications from the consumer report. | 1. Discuss information with customer.<br>2. If address discrepancy, apply CIP procedures<br>3. If suspected fraud, determine if you can accurately identify customer, if you are not able to identify the customer do not open the account, mark for Fraud review and send all documentation with denial. | Response(a-g): | |
| Suspicious Documents OR Suspicious Identifying Information | 1. Discuss observations with customer. If determined to be altered or forged do not proceed with the account.<br>2. If SSN provided has not been issued; is reported as a deceased person; ask for the original card or letter from the SSA. Also, run IRS.Gov TIN matching.<br>3. If SSN provided does not match the consumer report; or has multiple names tied to it: run IRS.Gov TIN matching. If it does not match, ask for the original card or letter from SSA.<br>4. If you cannot get satisfactory answer, deny the account. Mark for Fraud review, and send all documentation with denial. | Response(a-g): | |
| Unusual Use of, or Suspicious Activity Related to, the Covered Account | 1. Discuss activity with servicing officer.<br>2. Verify/check against original records or normal activity for the covered account.<br>3. Servicing officer contacts customer to discuss.<br>4. Submit copies to Fraud Department for review if applicable.<br>5. If customer notification, immediately notify Fraud Department for guidance and investigation. | Response(a-g): | |
| Notice From Customer, Victims of Identity Theft, or Law Enforcement of Possible Identity Theft | 1. Bank forms for ID Theft are located under the Compliance page of First Place.<br>2. Consider closing the account.<br>3. If requested, advise customer on information available to assist victims of ID Theft. Direct the customer to https://www.identitytheft.gov/<br>4. Submit copies to Fraud Department for investigation and guidance. | Response(a-g): | |
| **RED FLAG RESPONSES:**<br>a. Discussed with the customer, document customer's response.<br>b. Apply CIP procedures<br>c. Requested the original social security card or a letter from the SSA to verify the number (make a copy).<br>d. Conducted an IRS.Gov TIN match<br>e. Information was incorrectly entered to the consumer report. Verified accuracy with customer.<br>f. Gave customer FCRA and consumer report contact information.<br>g. Not proceeding with opening the account. | | | |
| Additional comments: | | | |
| Completed By - _____ Date: | | ☐ Request Fraud review. | |
| Fraud Department Review: | | Date: | |

Revision 8/1/2022

## Red Flags of Identity Theft (use identifying # on checklist)

***Alerts, Notifications or Warnings from a Consumer Reporting Agency***

1. Check Fraud is reported on the consumer report.
2. A consumer reporting agency provides a notice of address discrepancy, as defined in § 571.82(b) of this part.
3. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer.

***Suspicious Documents***

4. Documents provided for identification appear to have been altered or forged.
5. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
6. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
7. 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.
8. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

***Suspicious Personal Identifying Information***

9. 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 multiple names tied to it, has not been issued, or is listed on the Social Security Administration's Death Master File.
10. 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.
11. 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.
12. 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.
13. The SSN provided is the same as that submitted by other persons opening an account or other customers.
14. 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.
15. 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.
16. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
17. 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***

18. 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 for the addition of authorized users on the account.
19. 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).
20. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
21. The financial institution is notified that the customer is not receiving paper account statements.
22. The financial institution 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***

23. 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.