



FACT ACT IDENTITY THEFT RED FLAGS

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A **fraud 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 provides a notice of **address discrepancy**.
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 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 account or customer presenting the identification.
8. Other information on the identification is **not consistent** with readily accessible **information that is on file**, 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**. *For example*:
 - a. The address does not match any address in the consumer report; or b. Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
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. *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.
13. Personal identifying information provided is of a type **commonly associated with fraudulent activity** as indicated by internal or third-party sources. *For example*:
 - a. The address on an application is fictitious, a mail drop, or 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 address or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
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**.
18. 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, a request for new, additional, or replacement checks, convenience checks, or cards, or for the addition of authorized users on the account is received.
20. A new **revolving credit account** is used in a manner commonly associated with known patterns of fraud. *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.
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; or d. A material change in electronic fund transfer patterns in connection with a deposit account.
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.
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** 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

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.