

## **Secure Opening Plus Requirements for the Identity Theft Red Flag Program**

Secure Opening Plus is a solution that assists financial institutions in obtaining identifying information and opening accounts quickly and efficiently with fewer human errors. In addition to the operational benefits, Secure Opening Plus has a number of compliance benefits, including:

- Giving institutions the flexibility to customize the account opening fields to reflect the institution's policies and procedures,
- Enabling the institution to mandate fields so account opening staff is required to complete them, and
- Giving institutions automated tools to meet their regulatory requirements, including the OFAC, Customer Identification Program ("CIP") and Identity Theft Red Flag Program requirements.

BANKCARS ID Analysis provides anti-fraud and identity theft solutions. This product works in conjunction with Secure Opening Plus to provide, in real time, the most robust and accurate identity verification and risk assessment available today. The main components of the solution are the searching and scoring capabilities. Using a given name and social security number of an applicant, ID Analysis searches through credit and non-credit databases containing billions of identity records. It then applies a scoring logic to determine the relevance of each matching record and yields an aggregate score to alert for any potential fraudulent identity, supporting and substantially enhancing your identity theft prevention efforts.

Secure Opening Plus is also supported by Metavante Regulatory Services, one of the nation's leading compliance advisors. The Metavante Regulatory Services team of experts will assist the institution in developing procedures to meet their CIP requirements and the address discrepancy requirements of the Identity Theft Red Flag Program requirements. Metavante Regulatory Services also assists institutions that utilize IQ Risk Assessor in customizing the program to meet their needs and level of risk. Metavante Regulatory Services can also assist the institution in developing its Identity Theft Red Flag Program through a consulting engagement. For more information about IQ Risk Assessor or Secure Opening Plus please contact Cosby Benton at 229-560-4411.

The grid below demonstrates how Secure Opening Plus and Metavante Regulatory Services can help an institution meet its Identity Theft Red Flag requirements. Solutions for the red flags are identified using the following color coding:

Supported by Secure Opening Plus	Blue
Supported by Secure Opening Plus with BANKCARS ID Analysis services	Green
Supported by Metavante Regulatory Services Procedures	Orange

Red Flag	How to Handle It
<i>Alerts, Notifications or Warnings from a Consumer Reporting Agency</i>	
1. A fraud or active duty alert is included with a consumer report.	The BANKCARS ID Analysis component of Secure Opening Plus can assist the institution with this flag.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.	The BANKCARS ID Analysis component of Secure Opening Plus can assist the institution with this flag.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in §222.82(b) of this part.	The BANKCARS ID Analysis component of Secure Opening Plus can assist the institution with this flag. In addition, the CIP report and the procedures that can be developed by Metavante Regulatory Services can assist bank staff in appropriately handling the red flag.
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: <ul style="list-style-type: none"> <li>a. A recent and significant increase in the volume of inquiries;</li> <li>b. An unusual number of recently established credit relationships;</li> <li>c. A material change in the use of credit, especially with respect to recently established credit relationships; or</li> </ul>	The BANKCARS ID Analysis component of Secure Opening Plus can assist the institution in identifying all three of these flags. For example, BANKCARS ID Analysis checks numerous databases to determine increases in inquiries, credit relationships, and material changes and provides a risk “score.”
d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.	The NCN database lists closed for cause and unpaid bad checks.

<i>Suspicious Documents</i>	
5. Documents provided for identification appear to have been altered or forged.	The ID reader reads the bar code or magnetic strip and allows the bank staff to compare the information on the front of the ID to determine forgeries or alterations.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.	This flag must be performed by bank staff.
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.	Same answer as #5, plus the CIP report checks various databases for accuracy of presented information.
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.	The institution will need manual procedures if it chooses to incorporate this flag into its Identity Theft Red Flag Program.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.	This flag must be performed by bank staff.

<i>Suspicious Personal Identifying Information</i>	
<p>10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:</p> <p>a. The address does not match any address in the consumer report; or</p> <p>b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.</p>	The CIP report will include an address history on the individual. In addition, the CIP report indicates inconsistencies in the address and social security number and provides the year of issuance for the social security number.
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.	Inconsistencies, such as a social security number that was issued for an individual with a different date of birth than what was provided by the customer, are identified in the CIP report.

*Suspicious Personal Identifying Information (Continued)*

<p>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:</p> <p>a. The address on an application is the same as the address provided on a fraudulent application; or</p> <p>b. The phone number on an application is the same as the number provided on a fraudulent application.</p>	<p>The institution will need manual procedures if it chooses to incorporate this flag into its Identity Theft Red Flag Program.</p>
<p>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:</p> <p>a. The address on an application is fictitious, a mail drop, or a prison; or</p> <p>b. The phone number is invalid, or is associated with a pager or answering service.</p>	<p>The CIP report will assist the institution with this flag.</p>
<p>14. The SSN provided is the same as that submitted by other persons opening an account or other customers.</p>	<p>The NCN database will identify where a social security number was used previously at the institution. In addition, the BANKCARS ID Analysis component can provide even more information by reporting where a social security number has been associated with other names.</p>
<p>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.</p>	<p>The CIP report will indicate where other individuals have opened accounts using the customer's address. The telephone number red flag is not supported by Secure Opening Plus.</p>
<p>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.</p>	<p>The institution can select which fields within Secure Opening Plus will be mandatory, which will prevent bank staff from opening an account without complete identification information. Otherwise, this flag must be performed by bank staff.</p>
<p>17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.</p>	<p>This flag must be performed by bank staff.</p>

*Suspicious Personal Identifying Information (Continued)*

<p>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.</p>	<p>This flag must be performed by bank staff.</p>
---	---

*Unusual Use of, or Suspicious Activity Related to, the Covered Account*

<p>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.</p>	<p>This flag must be performed by bank staff. Most institutions can use their existing systems, such as their core systems, to comply with this flag.</p>
<p>20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:</p> <ul style="list-style-type: none"> <li>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</li> <li>b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.</li> </ul>	<p>The institution will need manual procedures if it chooses to incorporate these flags into its Identity Theft Red Flag Program. Metavante Regulatory Services can assist the institution with such procedures in an Identity Theft Red Flag Program consulting engagement.</p>
<p>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:</p> <ul style="list-style-type: none"> <li>a. Nonpayment when there is no history of late or missed payments;</li> <li>b. A material increase in the use of available credit;</li> <li>c. A material change in purchasing or spending patterns;</li> <li>d. A material change in electronic fund transfer patterns in connection with a deposit account; or</li> <li>e. A material change in telephone call patterns in connection with a cellular phone account.</li> </ul>	<p>The institution will need manual procedures if it chooses to incorporate these flags into its Identity Theft Red Flag Program. Metavante Regulatory Services can assist the institution with such procedures in an Identity Theft Red Flag Program consulting engagement.</p>
<p>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).</p>	<p>This flag must be performed by bank staff. Most institutions can use their existing systems, such as their core systems, to comply with this flag.</p>

<i>Unusual Use of, or Suspicious Activity Related to, the Covered Account (Continued)</i>	
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.	This flag must be performed by bank staff.
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.	This flag must be performed by bank staff.
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.	This flag must be performed by bank staff.

<i>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</i>	
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.	This flag must be performed by bank staff.