## Red Flags Rule

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Requirement | Control Effectiveness | Notes |
| B1 | Obtain approval of the initial written Program by the board of directors or a committee of the board, ensuring oversight of the development, implementation and administration of the Program, training staff, and overseeing service provider arrangements. |  |  |
|  | **Four Basic Elements of the Identity Theft Program** | | |
| E1 | Identity Theft Program must identify relevant Red Flags for covered accounts, including at least the following:  (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;  (2) The presentation of suspicious documents;  (3) The presentation of suspicious personal identifying information, such as a suspicious address change;  (4) The unusual use of, or other suspicious activity related to, a covered account; and  (5) 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. |  |  |
| E2 | Identity Theft Program must detect Red Flags that have been incorporated into the Program, through methods such as:  (a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and  (b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts. |  |  |
| E3 | Identity Theft Program must respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft. Examples of responses include:  (a) Monitoring a covered account for evidence of identity theft;  (b) Contacting the customer;  (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;  (d) Reopening a covered account with a new account number;  (e) Not opening a new covered account;  (f) Closing an existing covered account;  (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;  (h) Notifying law enforcement; or  (i) Determining that no response is warranted under the particular circumstances. |  |  |
| E4 | Identity Theft Program must be updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft. Examples of events that indicate an update is needed include:  (a) The experiences of the financial institution or creditor with identity theft;  (b) Changes in methods of identity theft;  (c) Changes in methods to detect, prevent, and mitigate identity theft;  (d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and  (e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements. |  |  |
|  | **Administering the Identity Theft Program** | | |
| A1 | Identity Theft Program includes oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management. This oversight includes:  (1) Assigning specific responsibility for the Program’s implementation;  (2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and  (3) Approving material changes to the Program as necessary to address changing identity theft risks. |  |  |
| A2 | Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 681.2 of this part. |  |  |
| A3 | The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management’s response; and recommendations for material changes to the Program. |  |  |
| A4 | Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider’s activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft. |  |  |