§ 391.22  
financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:
(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and
(ii) A deposit account.
(2) The term board of directors includes:
(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and
(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.
(3) Covered account means:
(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
(4) Credit has the same meaning as in 15 U.S.C. 1681a(c)(5).
(5) Creditor has the same meaning as in 15 U.S.C. 1681a(c)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.
(6) Customer means a person that has a covered account with a financial institution or creditor.
(7) Financial institution has the same meaning as in 15 U.S.C. 1681a(t).
(8) Identity theft has the same meaning as in 16 CFR 603.2(a).
(9) Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.
(10) Service provider means a person that provides a service directly to the financial institution or creditor.
(c) Periodic identification of covered accounts. Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:
(1) The methods it provides to open its accounts;
(2) The methods it provides to access its accounts; and
(3) Its previous experiences with identity theft.
(d) Establishment of an Identity Theft Prevention Program—(1) Program requirement. Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.
(2) Elements of the Program. The Program must include reasonable policies and procedures to:
(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Program;
(ii) Detect Red Flags that have been incorporated into the Program of the financial institution or creditor;
(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and
(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.
(e) Administration of the Program. Each financial institution or creditor that is required to implement a Program must provide for the continued
administration of the Program and must:
(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;
(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;
(3) Train staff, as necessary, to effectively implement the Program; and
(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) Guidelines. Each financial institution or creditor that is required to implement a Program must consider the guidelines in the appendix to this subpart and include in its Program those guidelines that are appropriate.

§ 391.23 Duties of card issuers regarding changes of address.

(a) Scope. This section applies to an issuer of a debit or credit card (card issuer) that is a State savings association whose deposits are insured by the Federal Deposit Insurance Corporation.

(b) Definitions. For purposes of this section:
(1) Cardholder means a consumer who has been issued a credit or debit card.
(2) Clear and conspicuous means reasonably understandable and designed to call attention to the nature and significance of the information presented.
(3) Address validation requirements. A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer’s debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:
(1)(i) Notifies the cardholder of the request:
(A) At the cardholder’s former address; or
(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and
(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or
(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to §391.22.
(d) Alternative timing of address validation. A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) Form of notice. Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

APPENDIX TO SUBPART C OF PART 391—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

Section 391.22 requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in §391.22(b)(3), to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of §391.22.

I. THE PROGRAM

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.
II. IDENTIFYING RELEVANT RED FLAGS

(a) Risk Factors. A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;
(2) The methods it provides to open its covered accounts;
(3) The methods it provides to access its covered accounts; and
(4) Its previous experiences with identity theft.

(b) Sources of Red Flags. Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;
(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and
(3) Applicable supervisory guidance.

(c) Categories of Red Flags. The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix.

(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.

III. DETECTING RED FLAGS

The Program’s policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(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. 5316(e) (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.

IV. PREVENTING AND MITIGATING IDENTITY THEFT

The Program’s policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer’s account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent Web site. Appropriate responses may include the following:

(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.

V. UPDATING THE PROGRAM

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(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.

VI. METHODS FOR ADMINISTERING THE PROGRAM

(a) Oversight of Program. Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:
Federal Deposit Insurance Corporation

(1) Assigning specific responsibility for the Program’s implementation;
(2) Reviewing reports prepared by staff regarding compliance with the financial institution or creditor’s Program and §391.22; and
(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) Reports. (1) In general. 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 §391.22.

(2) Contents of report. 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.

(c) Oversight of service provider arrangements. 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.

VII. OTHER APPLICABLE LEGAL REQUIREMENTS

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:
(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;
(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert; (c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681z–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and
(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix to Subpart C of Part 391

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in this Appendix, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

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 address discrepancy;
3. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
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.
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