§ 391.20  Examples.

The examples in this subpart are not exclusive. Compliance with an example, to the extent applicable, constitutes compliance with this subpart. Examples in a section illustrate only the issue described in the section and do not illustrate any other issue that may arise in this subpart.

§ 391.21  Disposal of consumer information.

(a) Scope. This section applies to State savings associations whose deposits are insured by the Federal Deposit Insurance Corporation (defined as “you”).

(b) In general. You must properly dispose of any consumer information that you maintain or otherwise possess in accordance with the Interagency Guidelines Establishing Information Security Standards, to the extent that you are covered by the scope of the Guidelines.

(c) Rule of construction. Nothing in this section shall be construed to:

(1) Require you to maintain or destroy any record pertaining to a consumer that is not imposed under any other law; or

(2) Alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

§ 391.22  Duties regarding the detection, prevention, and mitigation of identity theft.

(a) Scope. This section applies to a financial institution or creditor that is a State savings association whose deposits are insured by the Federal Deposit Insurance Corporation.

(b) Definitions. For purposes of this section and the appendix to subpart C of part 391, the following definitions apply:

(1) Account means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

for further information and assistance.\textsuperscript{14} The notice also should remind customers of the need to remain vigilant over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the institution. The notice should include the following additional items, when appropriate:

a. A recommendation that the customer review account statements and immediately report any suspicious activity to the institution;

b. A description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer’s consumer reports to put the customer’s creditors on notice that the customer may be a victim of fraud;

c. A recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted;

d. An explanation of how the customer may obtain a credit report free of charge; and

e. Information about the availability of the FTC’s online guidance regarding steps a consumer can take to protect against identity theft. The notice should encourage the customer to report any incidents of identity theft to the FTC, and should provide the FTC’s Web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and report suspected incidents of identity theft.\textsuperscript{15}

2. The Agencies encourage financial institutions to notify the nationwide consumer reporting agencies prior to sending notices to a large number of customers that include contact information for the reporting agencies.

C. Delivery of Customer Notice

Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by mail, or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

\textsuperscript{14} The institution should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance.

\textsuperscript{15} Currently, the FTC Web site for the ID Theft brochure and the FTC Hotline phone number are http://www.consumer.govidtheft and 1-877-IDTHEFT. The institution may also refer customers to any materials developed pursuant to section 151(b) of the FACT Act (educational materials developed by the FTC to teach the public how to prevent identity theft).
(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(r)(5).

(5) Creditor has the same meaning as in 15 U.S.C. 1681a(r)(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. 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.

(c) 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:

(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;