PARTS 38–40 [RESERVED]

PART 41—FAIR CREDIT REPORTING

Subparts A–H [Reserved]

Subpart I—Proper Disposal of Records Containing Consumer Information

Subpart J—Identity Theft Red Flags

AUTHORITY: 12 U.S.C. 1 *et seq.*, 24(Seventh), 93a, 1462a, 1463, 1464, 1818, 1828, 1831p–1, 1881–1884, and 5412(b)(2)(B); 15 U.S.C. 1681m, 1681s, 1681t, and 1681w.

SOURCE: 69 FR 77616, Dec. 28, 2004, unless otherwise noted.

Subparts A–H [Reserved]

Subpart I—Proper Disposal of Records Containing Consumer Information

§§ 41.80–41.82 [Reserved]

§ 41.83 Proper disposal of records containing consumer information.

(a) *Definitions as used in this section.* (1) *Consumer* means an individual.

(2) *Federal savings association* means a Federal savings association or an operating subsidiary of a Federal savings association.

(3) *National bank* means a national bank, an operating subsidiary of a national bank, or a Federal branch or agency of a foreign bank.

(b) *In general.* Each national bank or Federal savings association must properly dispose of any consumer information that it maintains or otherwise possesses in accordance with the Interagency Guidelines Establishing Information Security Standards, as set forth in appendix B to 12 CFR part 30, to the extent that the bank or savings association is covered by the scope of the Guidelines.

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

(1) Require a national bank or Federal savings association 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.

[79 FR 28400, May 16, 2014]

Subpart J—Identity Theft Red Flags

SOURCE: 72 FR 63753, Nov. 9, 2007, unless otherwise noted.

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

(a) *Scope.* This section applies to a financial institution or creditor that is a national bank; a Federal savings association; a Federal branch or agency of a foreign bank; or an operating subsidiary of any of these institutions that is not a functionally regulated subsidiary within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(b) *Definitions.* For purposes of this section and appendix J, 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:

(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. 1681m(e)(4).

(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 12 CFR 1022.3(h).

(9) *Person* means any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency, or other entity.

(10) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(11) *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 appendix J of this part and include in its Program those guidelines that are appropriate.

[72 FR 63753, Nov. 9, 2007, as amended at 79 FR 28400, May 16, 2014]

§ 41.91 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 national bank; a Federal savings association; a Federal branch or agency of a foreign bank; or an operating subsidiary of any of these institutions that is not a functionally regulated subsidiary within the meaning of section 5(c)(5) of the Bank Holding Company Act of 1956, as amended (12 U.S.C. 1844(c)(5)).

(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) *Consumer* means an individual.

(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:

(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 § 41.90 of this part.

(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.

[72 FR 63753, Nov. 9, 2007, as amended at 79 FR 28401, May 16, 2014]

§ 41.92 Examples.

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

[79 FR 28401, May 16, 2014]

APPENDIXES A–I TO PART 41 [RESERVED]

APPENDIX J TO PART 41—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

Section 41.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 41.90(b)(3) of this part, 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 § 41.90 of this part.