

Federal Deposit Insurance Corporation

§ 334.83

(a) *Act* means the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(b) *Affiliate* means any company that is related by common ownership or common corporate control with another company.

(c) [Reserved]

(d) *Company* means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e) *Consumer* means an individual.

(f)–(h) [Reserved]

(i) *Common ownership or common corporate control* means a relationship between two companies under which:

(1) One company has, with respect to the other company:

(i) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of a company, directly or indirectly, or acting through one or more other persons;

(ii) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of a company; or

(iii) The power to exercise, directly or indirectly, a controlling influence over the management or policies of a company, as the FDIC determines; or

(2) Any other person has, with respect to both companies, a relationship described in paragraphs (i)(1)(i) through (i)(1)(iii) of this section.

(j) [Reserved]

(k) *Medical information* means:

(1) Information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to:

(i) The past, present, or future physical, mental, or behavioral health or condition of an individual;

(ii) The provision of health care to an individual; or

(iii) The payment for the provision of health care to an individual.

(2) The term does not include:

(i) The age or gender of a consumer;

(ii) Demographic information about the consumer, including a consumer's residence address or e-mail address;

(iii) Any other information about a consumer that does not relate to the physical, mental, or behavioral health

or condition of a consumer, including the existence or value of any insurance policy; or

(iv) Information that does not identify a specific consumer.

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

(m) *State savings association* has the same meaning as in section 3(b)(3) of the Federal Deposit Insurance Act, 12 U.S.C. 1813(b)(3).

[70 FR 70685, Nov. 22, 2005, as amended at 72 FR 63760, Nov. 9, 2007; 80 FR 65919, Oct. 28, 2015]

Subparts B–H [Reserved]

Subpart I—Records Disposal

§§ 334.80–334.82 [Reserved]

§ 334.83 Disposal of consumer information.

(a) *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, as set forth in appendix B to part 364 of this chapter, prescribed pursuant to section 216 of the Fair and Accurate Credit Transactions Act of 2003 (15 U.S.C. 1681w) and section 501(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801(b)), to the extent the Guidelines are applicable to you.

(b) *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.

Subpart J—Identity Theft Red Flags

SOURCE: 72 FR 63761, Nov. 9, 2007, unless otherwise noted.

§ 334.90

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

(a) *Scope* This section applies to a financial institution or creditor that is an insured state nonmember bank, State savings association whose deposits are insured by the Federal Deposit Insurance Corporation, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers).

(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).

12 CFR Ch. III (1-1-23 Edition)

(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 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.

(11) *State savings association* has the same meaning as in section 3(b)(3) of the Federal Deposit Insurance Act, 12 U.S.C. 1813(b)(3).

(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;

Federal Deposit Insurance Corporation

§ 334.91

(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 63761, Nov. 9, 2007, as amended at 80 FR 65919, Oct. 28, 2015]

§ 334.91 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 an insured state non-member bank, state savings association whose deposits are insured by the Federal Deposit Insurance Corporation, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, or investment advisers).

(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) *State savings association* has the same meaning as in section 3(b)(3) of the Federal Deposit Insurance Act, 12 U.S.C. 1813(b)(3).

(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 § 334.90 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

Pt. 334, App. J

clear and conspicuous and provided separately from its regular correspondence with the cardholder.

[72 FR 63761, Nov. 9, 2007, as amended at 80 FR 65919, Oct. 28, 2015]

APPENDICES A–I TO PART 334 [RESERVED]

APPENDIX J TO PART 334—INTERAGENCY GUIDELINES ON IDENTITY THEFT DE- TECTION, PREVENTION, AND MITIGA- TION

Section 334.90 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in §334.90(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 §334.90 of this part.

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 cat-

12 CFR Ch. III (1–1–23 Edition)

egories are appended as Supplement A to this Appendix J.

(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. 5318(l) (31 CFR 1020.220); 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;