

**§ 680.28**

**16 CFR Ch. I (1-1-17 Edition)**

ABC and XYZ companies” or by “the ABC banking and credit card companies and the XYZ insurance companies;”

(2) A list of the affiliates or types of affiliates whose use of eligibility information is covered by the notice, which may include companies that become affiliates after the notice is provided to the consumer. If each affiliate covered by the notice shares a common name, such as “ABC,” then the notice may indicate that it applies to multiple companies with the ABC name or multiple companies in the ABC group or family of companies, for example, by stating that the notice is provided by “all of the ABC companies,” “the ABC banking, credit card, insurance, and securities companies,” or by listing the name of each affiliate providing the notice. But if the affiliates covered by the notice do not all share a common name, then the notice must either separately identify each covered affiliate by name or identify each of the common names used by those affiliates, for example, by stating that the notice applies to “all of the ABC and XYZ companies” or to “the ABC banking and credit card companies and the XYZ insurance companies;”

(3) A general description of the types of eligibility information that may be used to make solicitations to the consumer;

(4) That the consumer previously elected to limit the use of certain information to make solicitations to the consumer;

(5) That the consumer’s election has expired or is about to expire;

(6) That the consumer may elect to renew the consumer’s previous election;

(7) If applicable, that the consumer’s election to renew will apply for the specified period of time stated in the notice and that the consumer will be allowed to renew the election once that period expires; and

(8) A reasonable and simple method for the consumer to opt out.

(c) *Timing of the renewal notice*—(1) *In general.* A renewal notice may be provided to the consumer either—

(i) A reasonable period of time before the expiration of the opt-out period; or

(ii) Any time after the expiration of the opt-out period but before solicitations that would have been prohibited by the expired opt-out are made to the consumer.

(2) *Combination with annual privacy notice.* If you provide an annual privacy notice under the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 *et seq.*, providing a renewal notice with the last annual privacy notice provided to the consumer before expiration of the opt-out period is a reasonable period of time before expiration of the opt-out in all cases.

(d) *No effect on opt-out period.* An opt-out period may not be shortened by sending a renewal notice to the consumer before expiration of the opt-out period, even if the consumer does not renew the opt out.

**§ 680.28 Effective date, compliance date, and prospective application.**

(a) *Effective date.* This part is effective January 1, 2008.

(b) *Mandatory compliance date.* Compliance with this part is required not later than October 1, 2008.

(c) *Prospective application.* The provisions of this part shall not prohibit you from using eligibility information that you receive from an affiliate to make solicitations to a consumer if you receive such information prior to October 1, 2008. For purposes of this section, you are deemed to receive eligibility information when such information is placed into a common database and is accessible by you.

**PART 681—IDENTITY THEFT RULES**

Sec.

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

681.2 Duties of card issuers regarding changes of address.

APPENDIX A TO PART 681—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

AUTHORITY: 15 U.S.C. 1681m(e); 15 U.S.C. 1681m(e)(4); 15 U.S.C. 1681c(h).

SOURCE: 72 FR 63771, Nov. 9, 2007, unless otherwise noted.

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

(a) *Scope.* This section applies to financial institutions and creditors that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681s(a)(1).

(b) *Definitions.* For purposes of this section, and Appendix A, 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 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

§ 681.2

16 CFR Ch. I (1–1–17 Edition)

(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 A of this part and include in its Program those guidelines that are appropriate.

[74 FR 22645, May 14, 2009, as amended at 77 FR 72715, Dec. 6, 2012]

§ 681.2 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in § 681.1(a) that issues a debit or credit card (card issuer).

(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:

(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 § 681.1 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.

[74 FR 22645, May 14, 2009]

APPENDIX A TO PART 681—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

Section 681.1 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 681.1(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 § 681.1 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 categories are appended as supplement A to this appendix A.

- (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(1) (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 website. 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:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with §681.1 of this part; 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 §681.1 of this part.

(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. 1681s–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 A*

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in appendix A of this part, 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 credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in §641.1(b) of this part.

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 external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or by other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

*Unusual Use of, or Suspicious Activity Related to, the Covered Account*

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

*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*

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

[72 FR 63771, Nov. 9, 2007, as amended at 74 FR 22646, May 14, 2009]

**PART 682—DISPOSAL OF CONSUMER REPORT INFORMATION AND RECORDS**

Sec.

682.1 Definitions.

682.2 Purpose and scope.

682.3 Proper disposal of consumer information.

682.4 Relation to other laws.

682.5 Effective date.

AUTHORITY: Pub. L. 108–159, sec. 216.

SOURCE: 69 FR 68697, Nov. 24, 2004, unless otherwise noted.

**§ 682.1 Definitions.**

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. 1681 *et seq.*

(b) “*Consumer information*” means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.

(c) “*Dispose,*” “*disposing,*” or “*disposal*” means:

(1) The discarding or abandonment of consumer information, or

(2) The sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.

**§ 682.2 Purpose and scope.**

(a) *Purpose.* This part (“rule”) implements section 216 of the Fair and Accurate Credit Transactions Act of 2003, which is designed to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information.

(b) *Scope.* This rule applies to any person over which the Federal Trade Commission has jurisdiction, that, for a business purpose, maintains or otherwise possesses consumer information.

**§ 682.3 Proper disposal of consumer information.**

(a) *Standard.* Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(b) *Examples.* Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples. These examples are illustrative only and are not exclusive or exhaustive methods for complying with the rule in this part.

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.

(3) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company’s operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company’s information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.

(4) For persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to