AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

to the scheduled termination date. Prices of refund and no-refund products may differ.

• Refund of fee paid in lump sum

[Applicable where the customer pays the fee in a single payment and the fee is added to the amount borrowed]

[Prohibited where the debt subject to the contract is a residential mortgage loan]

[Either:] (1) You may cancel [PRODUCT NAME] at any time and receive a refund; or (2) You may cancel [PRODUCT NAME] within __ days and receive a full refund; or (3) If you cancel [PRODUCT NAME] you will not receive a refund.

• Use of card or credit line restricted

[Applicable if the contract restricts use of card or credit line when customer activates protection]

If [PRODUCT NAME] is activated, you will be unable to incur additional charges on the credit card or use the credit line.

• Termination of [PRODUCT NAME]

[Either]: (1) You have no right to cancel [PRODUCT NAME]; *or* (2) You have the right to cancel [PRODUCT NAME] in the following circumstances: _____.

[And either]: (1) The bank has no right to cancel [PRODUCT NAME]; *or* (2)The bank has the right to cancel [PRODUCT NAME] in the following circumstances: _____.

• Eligibility requirements, conditions, and exclusions

There are eligibility requirements, conditions, and exclusions that could prevent you from receiving benefits under [PRODUCT NAME].

[Either]: (1) The following is a summary of the eligibility requirements, conditions, and exclusions. [The bank provides a summary of any eligibility requirements, conditions, and exclusions]; *or* (2) You may find a complete explanation of the eligibility requirements, conditions, and exclusions in paragraphs ___ of the [PRODUCT NAME] agreement.

PARTS 38–40 [RESERVED]

PART 41—FAIR CREDIT REPORTING

Subparts A–H [Reserved]

Subpart I—Proper Disposal of Records Containing Consumer Information

Sec.

41.80–41.82 [Reserved]
41.83 Proper disposal of records containing consumer information.

Subpart J—Identity Theft Red Flags

41.90 Duties regarding the detection, prevention, and mitigation of identity theft.
41.91 Duties of card issuers regarding changes of address.
41.92 Examples.

APPENDIXES A–I TO PART 41 [RESERVED]
APPENDIX J TO PART 41—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

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.

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 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); 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 §41.90 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 §41.90 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 J

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in appendix J 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 12 CFR 1022.82(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 63754, Nov. 9, 2007, as amended at 74 FR 22642, May 14, 2009; 76 FR 6688, Feb. 8, 2011; 79 FR 28401, May 16, 2014]

PART 42 [RESERVED]

PART 43—CREDIT RISK RETENTION

Subpart A—Authority, Purpose, Scope and Definitions

Sec.
43.1 Authority, purpose, scope, and reservation of authority.
43.2 Definitions.

Subpart B—Credit Risk Retention

43.3 Base risk retention requirement.
43.4 Standard risk retention.
43.5 Revolving pool securitizations.
43.6 Eligible ABCP conduits.
43.7 Commercial mortgage-backed securities.
43.8 Federal National Mortgage Association and Federal Home Loan Mortgage Corporation ABS.
43.9 Open market CLOs.
43.10 Qualified tender option bonds.

Subpart C—Transfer of Risk Retention

43.11 Allocation of risk retention to an originator.
43.12 Hedging, transfer and financing prohibitions.

Subpart D—Exceptions and Exemptions

43.13 Exemption for qualified residential mortgages.
43.14 Definitions applicable to qualifying commercial loans, qualifying commercial real estate loans, and qualifying automobile loans.
43.15 Qualifying commercial loans, commercial real estate loans, and automobile loans.
43.16 Underwriting standards for qualifying commercial loans.
43.17 Underwriting standards for qualifying CRE loans.
43.18 Underwriting standards for qualifying automobile loans.
43.19 General exemptions.
43.20 Safe harbor for certain foreign-related transactions.
43.21 Additional exemptions.
43.22 Periodic review of the QRM definition, exempted three-to-four unit residential mortgage loans, and community-focused residential mortgage exemption.

AUTHORITY: 12 U.S.C. 1 *et seq.*, 93a, 161, 1464, 1818, 5412(b)(2)(B), and 15 U.S.C. 78o-11.

SOURCE: 79 FR 77740, 77764, Dec. 24, 2014, unless otherwise noted.

Subpart A—Authority, Purpose, Scope and Definitions

§43.1 Authority, purpose, scope, and reservation of authority.

(a) *Authority.* This part is issued under the authority of 12 U.S.C. 1 *et seq.*, 93a, 161, 1464, 1818, 5412(b)(2)(B), and 15 U.S.C. 78o-11.

(b) *Purpose.* (1) This part requires securitizers to retain an economic interest in a portion of the credit risk for any asset that the securitizer, through the issuance of an asset-backed security, transfers, sells, or conveys to a third party. This part specifies the permissible types, forms, and amounts of credit risk retention, and it establishes