

§ 248.201

as our [investment adviser, investment company, transfer agent, and broker-dealer] affiliates, from marketing their products or services to you based on your personal information that we share with them. This information includes your [income], your [account history with us], and your [credit score].

- Your choice has expired or is about to expire.

To renew your choice to limit marketing for [x] more years, contact us [include all that apply]:

- By telephone: 1-877-###-####
- On the Web: *www.—.com*
- By mail: check the box and complete the form below, and send the form to:

[Company name]

[Company address]

Renew my choice to limit marketing for [x] more years.

A-4—MODEL FORM FOR RENEWAL NOTICE (JOINT NOTICE)—[RENEWING YOUR CHOICE TO LIMIT MARKETING]/[RENEWING YOUR MARKETING OPT OUT]

- The [ABC group of companies] is providing this notice.

- [Optional: Federal law gives you the right to limit some but not all marketing from the [ABC] companies. Federal law also requires us to give you this notice to tell you about your choice to limit marketing from the [ABC] companies.]

- You previously chose to limit the [ABC] companies, such as the [ABC investment adviser, investment company, transfer agent, and broker-dealer] affiliates, from marketing their products or services to you based on your personal information that they receive from other ABC companies. This information includes your [income], your [account history], and your [credit score].

- Your choice has expired or is about to expire.

To renew your choice to limit marketing for [x] more years, contact us [include all that apply]:

- By telephone: 1-877-###-####
- On the Web: *www.—.com*
- By mail: check the box and complete the form below, and send the form to:

[Company name]

[Company address]

Renew my choice to limit marketing for [x] more years.

A-5—MODEL FORM FOR VOLUNTARY “NO MARKETING” NOTICE—YOUR CHOICE TO STOP MARKETING

- [Name of Affiliate] is providing this notice.

- You may choose to stop all marketing from us and our affiliates.

17 CFR Ch. II (4–1–14 Edition)

- [Your choice to stop marketing from us and our affiliates will apply until you tell us to change your choice.]

To stop all marketing, contact us [include all that apply]:

- By telephone: 1-877-###-####
- On the Web: *www.—.com*
- By mail: check the box and complete the form below, and send the form to:

[Company name]

[Company address]

Do not market to me.

Subpart C—Regulation S-ID: Identity Theft Red Flags

SOURCE: 78 FR 23663, Apr. 17, 2013, unless otherwise noted.

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

(a) *Scope.* This section applies to a *financial institution* or *creditor*, as defined in the Fair Credit Reporting Act (15 U.S.C. 1681), that is:

(1) A broker, dealer or any other person that is registered or required to be registered under the Securities Exchange Act of 1934;

(2) An investment company that is registered or required to be registered under the Investment Company Act of 1940, that has elected to be regulated as a business development company under that Act, or that operates as an employees' securities company under that Act; or

(3) An investment adviser that is registered or required to be registered under the Investment Advisers Act of 1940.

(b) *Definitions.* For purposes of this subpart, and appendix A of this subpart, 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 a brokerage account, a *mutual fund* account (*i.e.*, an account with an open-end investment company), and an investment advisory account.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign financial institution or

Securities and Exchange Commission

§ 248.201

creditor, the managing official of that branch or agency; and

(ii) In the case of a financial institution or 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 brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; 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) *Identifying information* means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any—

(i) Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(ii) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(iii) Unique electronic identification number, address, or routing code; or

(iv) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

(9) *Identity theft* means a fraud committed or attempted using the identi-

fying information of another person without authority.

(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.

(12) *Other definitions.*

(i) *Broker* has the same meaning as in section 3(a)(4) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(4)).

(ii) *Commission* means the Securities and Exchange Commission.

(iii) *Dealer* has the same meaning as in section 3(a)(5) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(5)).

(iv) *Investment adviser* has the same meaning as in section 202(a)(11) of the Investment Advisers Act of 1940 (15 U.S.C. 80b-2(a)(11)).

(v) *Investment company* has the same meaning as in section 3 of the Investment Company Act of 1940 (15 U.S.C. 80a-3), and includes a separate series of the investment company.

(vi) Other terms not defined in this subpart have the same meaning as in the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(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

§ 248.202

17 CFR Ch. II (4-1-14 Edition)

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 A to this subpart and include in its Program those guidelines that are appropriate.

§ 248.202 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in §248.201(a) that issues a credit or debit card (card issuer).

(b) *Definitions.* For purposes of this section:

(1) *Cardholder* means a consumer who has been issued a *credit card* or *debit card* as defined in 15 U.S.C. 1681a(r).

(2) *Clear and conspicuous* means reasonably understandable and designed to call attention to the nature and significance of the information presented.

(3) Other terms not defined in this subpart have the same meaning as in the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*).

(c) *Address validation requirements.* A card issuer must establish and implement reasonable written 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 §248.201.

(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 be provided separately from its regular correspondence with the cardholder.

APPENDIX A TO SUBPART C OF PART 248—INTERAGENCY GUIDELINES ON IDENTITY THEFT DETECTION, PREVENTION, AND MITIGATION

Section 248.201 requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in §248.201(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 §248.201.

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 regulatory 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(l) (31 CFR 1023.220 (broker-dealers) and 1024.220 (mutual funds)); 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;
- (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 §248.201; 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 §248.201.

(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 to this subpart, 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 referenced in Sec. 605(h) of the Fair Credit Reporting Act (15 U.S.C. 1681c(h)).

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 means of accessing the account or for the addition of an authorized user on the account.

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

21. 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).

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

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

24. 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

25. 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.

PART 249—FORMS, SECURITIES EXCHANGE ACT OF 1934

Sec.

249.0-1 Availability of forms.

Subpart A—Forms for Registration or Exemption of, and Notification of Action Taken by, National Securities Exchanges

249.1 Form 1, for application for, and amendments to applications for, registration as a national securities exchange or exemption from registration pursuant to Section 5 of the Exchange Act.

249.10 Form 1-N for notice registration as a national securities exchange.

249.11 Form R31 for reporting covered sales and covered round turn transactions under section 31 of the Act.

249.25 Form 25, for notification of removal from listing and/or registration.

249.26 Form 26, for notification of the admission to trading of a substituted or additional class of security under Rule 12a-5 (§240.12a-5 of this chapter).

Subpart B—Forms for Reports To Be Filed by Officers, Directors, and Security Holders

249.103 Form 3, initial statement of beneficial ownership of securities.

249.104 Form 4, statement of changes in beneficial ownership of securities.

249.105 Form 5, annual statement of beneficial ownership of securities.

Subpart C—Forms for Applications for Registration of Securities on National Securities Exchanges and Similar Matters

249.208 [Reserved]

249.208a Form 8-A, for registration of certain classes of securities pursuant to sec-

tion 12(b) or (g) of the Securities Exchange Act of 1934.

249.208b-249.208c [Reserved]

249.210 Form 10 and Form 10-SB, general form for registration of securities pursuant to section 12 (b) or (g) of the Securities Exchange Act of 1934.

249.210b [Reserved]

249.218 Form 18, for foreign governments and political subdivisions thereof.

249.220f Form 20-F, registration of securities of foreign private issuers pursuant to section 12(b) or (g), annual and transition reports pursuant to sections 13 and 15(d), and shell company reports required under Rule 13a-19 or 15d-19 (§240.13a-19 or §240.15d-19 of this chapter).

249.240f Form 40-F, for registration of securities of certain Canadian issuers pursuant to section 12(b) or (g) and for reports pursuant to section 15(d) and Rule 15d-4 (§240.15d-4 of this chapter).

249.250 Form F-X, for appointment of agent for service of process by issuers registering securities on Form F-8, F-9, F-10 or F-80 (§239.38, 239.39, 239.40 or 239.41 of this chapter), or registering securities or filing periodic reports on Form 40-F (§249.240f of this chapter), or by any issuer or other non-U.S. person filing tender offer documents on Schedule 13E-4F, 14D-1F or 14D-9F (§240.13e-102, 240.14d-102 or 240.14d-103 of this chapter), or by any non-U.S. person acting as trustee with respect to securities registered on Form F-7 (§249.37 of this chapter), F-8, F-9, F-10 or F-80.

Subpart D—Forms for Annual and Other Reports of Issuers Required Under Sections 13 and 15(d) of the Securities Exchange Act of 1934

249.306 Form 6-K report of foreign issuer pursuant to Rules 13a-16 (§240.13a-16 of this chapter) and 15d-16 (§240.15d-16 of this chapter) under the Securities Exchange Act of 1934.

249.308 Form 8-K, for current reports.

249.308a Form 10-Q, for quarterly and transition reports under sections 13 or 15(d) of the Securities Exchange Act of 1934.

249.310 Form 10-K, for annual and transition reports pursuant to sections 13 or 15(d) of the Securities Exchange Act of 1934.

249.310b-249.310c [Reserved]

249.311 Form 11-K, for annual reports of employee stock purchase, savings and similar plans pursuant to section 15(d) of the Securities Exchange Act of 1934.

249.312 Form 10-D, periodic distribution reports by asset-backed issuers.

249.318 Form 18-K, annual report for foreign governments and political subdivisions thereof.

249.322 Form 12b-25—Notification of late filing.