Identity Theft Red Flags Rules; Final Rule

Securities and Exchange Commission
17 CFR Part 248
Identity Theft Red Flags Rules; Final Rule
COMMODITY FUTURES TRADING COMMISSION

17 CFR Part 162
RIN 3038–AD14

SECURITIES AND EXCHANGE COMMISSION

17 CFR Part 248
[Release Nos. 34–69359, IA–3582, IC–30456; File No. S7–02–12]
RIN 3235–AL26

Identity Theft Red Flags Rules

AGENCY: Commodity Futures Trading Commission and Securities and Exchange Commission.

ACTION: Joint final rules and guidelines.

SUMMARY: The Commodity Futures Trading Commission ("CFTC") and the Securities and Exchange Commission ("SEC") (together, the "Commissions") are jointly issuing final rules and guidelines to require certain regulated entities to establish programs to address risks of identity theft. These rules and guidelines implement provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which amended the Fair Credit Reporting Act and directed the Commissions to adopt rules requiring entities that are subject to the Commissions' respective enforcement authorities to address identity theft. First, the rules require financial institutions and creditors to develop and implement a written identity theft prevention program designed to detect, prevent, and mitigate identity theft in connection with certain existing accounts or the opening of new accounts. The rules include guidelines to assist entities in the formulation and maintenance of programs that would satisfy the requirements of the rules. Second, the rules establish special requirements for any credit and debit card issuers that are subject to the Commissions' respective enforcement authorities, to assess the validity of notifications of changes of address under certain circumstances. 

DATES: Effective date: May 20, 2013; Compliance date: November 20, 2013.

FOR FURTHER INFORMATION CONTACT: CFTC: Sue McDonough, Counsel, at Commodity Futures Trading Commission, Office of the General Counsel, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581, telephone number (202) 418–5132, facsimile number (202) 418–5524, email smcdonough@cftc.gov; SEC: with regard to investment companies and investment advisers, contact Andrea Ottomaneli Magovern, Senior Counsel, Amanda Wagner, Senior Counsel, Thoreau Bartmann, Branch Chief, or Hunter Jones, Assistant Director, Office of Regulatory Policy, Division of Investment Management, (202) 551–6792, or with regard to brokers, dealers, or transfer agents, contact Brice Prince, Special Counsel, Joseph Furey, Assistant Chief Counsel, or David Blass, Chief Counsel, Office of Chief Counsel, Division of Trading and Markets, (202) 551–5550, Securities and Exchange Commission, 100 F Street NE., Washington, DC 20549–8549.


Table of Contents

I. Background
II. Explanation of the Final Rules and Guidelines
A. Final Identity Theft Red Flags Rules
  1. Which Financial Institutions and Creditors Are Required to Have a Program
  2. The Objectives of the Program
  3. The Elements of the Program
  4. Administration of the Program
B. Final Guidelines
  1. Section I of the Guidelines—Identity Theft Prevention Program
  2. Section II of the Guidelines—Identifying Relevant Red Flags
  3. Section III of the Guidelines—Detecting Red Flags
  4. Section IV of the Guidelines—Preventing and Mitigating Identity Theft
  5. Section V of the Guidelines—Updating the Identity Theft Prevention Program
  6. Section VI of the Guidelines—Methods for Administering the Identity Theft Prevention Program
  7. Section VII of the Guidelines—Other Applicable Legal Requirements
  8. Supplement A to the Guidelines
C. Final Card Issuer Rules
III. Related Matters
  A. Cost-Benefit Considerations (CFTC) and Economic Analysis (SEC)
  B. Analysis of Effects on Efficiency, Competition, and Capital Formation
  C. Paperwork Reduction Act
  D. Regulatory Flexibility Act
IV. Statutory Authority and Text of Amendments

I. Background

The growth and expansion of information technology and electronic communication have made it increasingly easy to collect, maintain, and transfer personal information about individuals. Advancements in technology also have led to increasing threats to the privacy and personal information of individuals. During recent decades, the federal government has taken steps to help protect individuals, and to help individuals protect themselves, from the risks of theft, loss, and abuse of their personal information.

The Fair Credit Reporting Act of 1970 ("FCRA"), as amended in 2003, required several federal agencies to issue joint rules and guidelines regarding the detection, prevention, and mitigation of identity theft for entities that are subject to their respective enforcement authorities (also known as "Red Flags").


A recent survey found that in 2012, over 5% of Americans were victims of identity fraud. See Javelin Strategy & Research, 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters (Feb. 2013), available at https://www.javelinstrategy.com/uploads/web_brochure/1303_R_2013IdentityFraudBrochure.pdf; see also Comment Letter of Tyler Krulla ("Tyler Krulla Comment Letter") (Apr. 27, 2012) ("In today’s technology driven world it is easier than ever for anyone to acquire and exploit someone’s identity and cause severe financial problems.").


of the Treasury, as described in section 1062 of that Act. On September 20, 2010, the Secretary of the Treasury designated July 21, 2011, as the transfer date. See Designated Transfer Date, 75 FR 57252 (Sept. 10, 2010).

12 The Commissions’ joint proposed rules and guidelines were published in the Federal Register on March 6, 2012. See Identity Theft Red Flags Rules, 77 FR 13450 (Mar. 6, 2012) (“Proposing Release”). For ease of reference, unless the context indicates otherwise, our general use of the terms “identity theft red flags rules” or “rules” in this release will refer to both the identity theft red flags rules and guidelines. In addition, unless the context indicates otherwise, the general use of these terms in this preamble and Section III of this release will refer to both the identity theft red flags rules and guidelines, and the card issuer rules (which are discussed in further detail later in this release).


14 See, e.g., Comment Letter of MarketCounsel (Apr. 25, 2012) (“MarketCounsel Comment Letter”) (“MarketCounsel supports the Commission’s attempt to help protect individuals from the risk of theft, loss, and abuse of their personal information through the Proposed Rule.”); Comment Letter of Erik Speicher (“Erik Speicher Comment Letter”) (Mar. 17, 2012) (“Identity theft is a major concern of all citizens. The effects and burdens associated with having ones [sic] identity stolen necessitate that such efforts be placed on the covered entities will better protect all of us from the possibility of having our identity stolen.”); Comment Letter of Lauren L. Mark (Mar. 12, 2012) (“I[requirement to implement an identity theft prevention plan and to verify change of personal information [have the [potential] to protect people]”).

15 See, e.g., Tyler Krulla Comment Letter; Lauren L. Comment Letter (“I agree with the proposed changes. With the market shifting to an IT based world, identity theft is increasing. Therefore, more stringent rules should be in place to protect those that may be affected.”).

16 See, e.g., Comment Letter of the Investment Adviser Association (May 7, 2012) (“IAA Comment Letter”) (requesting that the SEC and CFTC clarify the definition of “financial institution” and “creditor” and exclude clearing organizations from the categories of entities specifically mentioned in the scope section of the rule); Comment Letter of the Options Clearing Corporation (May 3, 2012) (“OCC Comment Letter”) (requesting that the SEC and CFTC clarify the definition of “creditor” and expressly exclude clearing organizations from the scope of the rule); Comment Letter of the Financial Services Roundtable and the Securities Industry and Financial Markets Association (May 2, 2012) (“FSR/SIFMA Comment Letter”) (requesting that the SEC and CFTC clarify the definition of “creditor” and “financial institution” and “covered account,” and that the SEC and CFTC specifically define the types of accounts that would qualify as covered accounts).
II. Explanation of the Final Rules and Guidelines

A. Final Identity Theft Red Flags Rules

Sections 615(e)(1)(A) and (B) of the FCRA, as amended by the Dodd-Frank Act, require that the Commissions jointly establish and maintain guidelines for “financial institutions” and “creditors” regarding identity theft, and adopt rules requiring such institutions and creditors to establish reasonable policies and procedures for the implementation of those guidelines. Under the final rules, a financial institution or creditor that offers or maintains “covered accounts” must establish an identity theft red flags program designed to detect, prevent, and mitigate identity theft. To that end, the final rules discussed below specify: (1) Which financial institutions and creditors must develop and implement a written identity theft prevention program (“Program”); (2) the objectives of the Program; (3) the elements that the Program must contain; and (4) the steps financial institutions and creditors need to take to administer the Program.

1. Which Financial Institutions and Creditors Are Required To Have a Program

The “scope” subsections of the rules generally set forth the types of entities that are subject to the Commissions’ identity theft red flags rules. Under these subsections, the rules apply to entities over which Congress recently granted the Commissions enforcement authority under the FCRA. The Commissions’ scope provisions are similar to those contained in the rules adopted by the Agencies, which limit the rules’ scope to entities that are within the Agencies’ respective enforcement authorities.

As noted above, the CFTC’s “scope” subsection “applies to financial institutions and creditors that are subject to” the CFTC’s enforcement authority under the FCRA. The CFTC’s proposed definitions of “financial institution” and “creditor” describe the entities to which its identity theft red flags rules and guidelines apply. In the Proposing Release, the CFTC defined “financial institution” as having the same meaning as in section 603(1) of the FCRA. In addition, the CFTC’s proposed definition of “financial institution” also specified that the term includes any futures commission merchant (“FCM”), retail foreign exchange dealer (“RFED”), commodity trading advisor (“CTA”), commodity pool operator (“CPO”), introducing broker (“IB”), swap dealer (“SD”), or major swap participant (“MSP”) that directly or indirectly holds a transaction account belonging to a consumer. Similarly, in the CFTC’s proposed definition of “creditor,” the CFTC applies the definition of “creditor” from 15 U.S.C. 1681m(e)(4) to any FCM, RFED, CTA, CPO, IB, SD, or MSP that “regularly extends, renew, or continues credit; regularly arranges for the extension, renewal, or continuation of credit; or in acting as an assignee of an original creditor, participates in the decision to extend, renew, or continue credit.”

The CFTC has determined that the final identity theft red flags rules apply to these entities because of the increased likelihood that these entities open or maintain covered accounts, or pose a reasonably foreseeable risk, or to the safety and soundness of the financial institution or creditor, from identity theft. This approach is consistent with the general scope of part 162 of the CFTC’s regulations.

One commenter suggested that the CFTC follow the SEC’s approach and simply cross-reference the FCRA definition of “financial institution” and the FCRA definition of “creditor” as amended by the Red Flag Program Clarification Act of 2010 (“Clarification Act”) rather than including named entities in the definition. The commenter argued that cross-referencing the FCRA definitions, as amended by the Clarification Act, rather than including specific types of entities that are subject to the CFTC’s enforcement authority in the definitions of “financial institution” and “creditor,” would be more consistent with the SEC’s and the Agencies’ regulations and would allow the agencies to easily adapt to any changes to the FCRA over time.

After considering these concerns, the CFTC has concluded that if it were to follow the SEC’s approach and simply cross-reference the FCRA definitions of “financial institution” and “creditor,” the general scope provisions of 17 CFR part 162 would still apply and specify that part 162 applies to FCMs, RFEDs, CTAs, CPOs, IBs, MSPs, and SDs. As a practical matter, a cross-reference to the FCRA definitions of “financial institution” and “creditor” would not change the result because under the general scope provisions of part 162, the CFTC’s identity theft red flags rules would still apply to the same list of entities. As a result, the CFTC believes that it should retain the same definition of “financial institution” and “creditor” contained in the Proposing Release.

The SEC’s “scope” subsection provides that the final rules apply to a financial institution or creditor, as defined by the FCRA, that is: 

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

• An investment company that is registered or required to be registered under the Investment Company Act of 1940 (“Investment Company Act”); 

(except brokers, dealers, persons providing insurance, investment companies, and investment advisers); 

• 12 CFR 17.90(a) (stating that the NCUA’s red flags rule “applies to a financial institution or creditor that is a federal credit union”). 

• 12 CFR 134.90(a) (stating that the FIDC’s red flags rule “applies to a financial institution or creditor that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities 

32 § 162.30(a); see also supra note 24.

33 See 15 U.S.C. 1681a(l) (defining “financial institution” to include certain banks and credit unions, and “any other person that, directly or indirectly, holds a transaction account (as defined in Section 196(b) of the Federal Reserve Act belonging to a consumer”). Section 196(b) of the Federal Reserve Act defines a transaction account as “a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders or withdrawal, telephone transfers, or other similar items for the purpose of making payments or transferring third parties or others.” 12 U.S.C. 461(b)(1)(C). 

• 12 CFR 134.90(a) (stating that the FDIC’s red flags rule “applies to a financial institution or creditor that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities.


36 The commenter also noted that the CFTC’s proposed definition of “creditor” would include certain entities such as CPOs and CTAs—entities that do not extend credit.

37 See 12 CFR 134.90(a). 

38 See 12 CFR 134.90(a).

39 See 12 CFR 134.90(a) (stating that the FIDC’s red flags rule “applies to a financial institution or creditor that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities.

40 As noted above, the CFTC’s “scope” subsection “applies to financial institutions and creditors that are subject to” the CFTC’s enforcement authority under the FCRA. The CFTC’s proposed definitions of “financial institution” and “creditor” describe the entities to which its identity theft red flags rules and guidelines apply. In the Proposing Release, the CFTC defined “financial institution” as having the same meaning as in section 603(1) of the FCRA. In addition, the CFTC’s proposed definition of “financial institution” also specified that the term includes any futures commission merchant (“FCM”), retail foreign exchange dealer (“RFED”), commodity trading advisor (“CTA”), commodity pool operator (“CPO”), introducing broker (“IB”), swap dealer (“SD”), or major swap participant (“MSP”) that directly or indirectly holds a transaction account belonging to a consumer. Similarly, in the CFTC’s proposed definition of “creditor,” the CFTC applies the definition of “creditor” from 15 U.S.C. 1681m(e)(4) to any FCM, RFED, CTA, CPO, IB, SD, or MSP that “regularly extends, renew, or continues credit; regularly arranges for the extension, renewal, or continuation of credit; or in acting as an assignee of an original creditor, participates in the decision to extend, renew, or continue credit.”

The CFTC has determined that the final identity theft red flags rules apply to these entities because of the increased likelihood that these entities open or maintain covered accounts, or pose a reasonably foreseeable risk, or to the safety and soundness of the financial institution or creditor, from identity theft. This approach is consistent with the general scope of part 162 of the CFTC’s regulations.

(except brokers, dealers, persons providing insurance, investment companies, and investment advisers); 

• 12 CFR 17.90(a) (stating that the NCUA’s red flags rule “applies to a financial institution or creditor that is a federal credit union”). 

• 12 CFR 134.90(a) (stating that the FIDC’s red flags rule “applies to a financial institution or creditor that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities.

32 § 162.30(a); see also supra note 24.

33 See 15 U.S.C. 1681a(l) (defining “financial institution” to include certain banks and credit unions, and “any other person that, directly or indirectly, holds a transaction account (as defined in Section 196(b) of the Federal Reserve Act belonging to a consumer”). Section 196(b) of the Federal Reserve Act defines a transaction account as “a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders or withdrawal, telephone transfers, or other similar items for the purpose of making payments or transferring third parties or others.” 12 U.S.C. 461(b)(1)(C). 

• 12 CFR 134.90(a) (stating that the FIDC’s red flags rule “applies to a financial institution or creditor that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities.


36 The commenter also noted that the CFTC’s proposed definition of “creditor” would include certain entities such as CPOs and CTAs—entities that do not extend credit.

37 See 12 CFR 134.90(a). 

38 See 12 CFR 134.90(a).
development company ("BDC") under that Act, or that operates as an employees' securities company ("ESC") under that Act; or

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

The types of entities listed by name in the scope section are the registered entities regulated by the SEC that are most likely to be financial institutions or creditors, i.e., brokers or dealers ("broker-dealers"); investment companies; and, investment advisers.

The scope section also includes any other entities that are registered or are required to register under the Exchange Act. Some types of entities required to register under the Exchange Act, such as nationally recognized statistical rating organizations ("NRSROs"), self-regulatory organizations ("SROs"), municipal advisors, and municipal securities dealers, are not listed by name in the scope section because they may be less likely to qualify as financial institutions or creditors under the FCRA. Nevertheless, if any entity of a type not listed qualifies as a financial institution or creditor, it is covered by the SEC's rules. The scope section does not include entities that are not themselves registered or required to register with the SEC (with the exception of certain non-registered investment companies that nonetheless are regulated by the SEC), even if they register securities under the Securities Act of 1933 or the Exchange Act, or report information under the federal securities laws.

The SEC received four comment letters arguing that it should specifically exclude certain entities from the scope of the rules. These commenters recommended that the scope section exclude registered investment advisers, clearing organizations, SROs, municipal securities dealers, municipal advisors, or NRSROs. The commenters argued that these entities are not likely to be financial institutions or creditors under the FCRA. Nevertheless, if any entity of a type not listed qualifies as a financial institution or creditor, the SEC believes that such an entity should be subject to the SEC's rules, and did not state that Regulation S–AM applies to any brokers or dealers, municipal advisors, or NRSROs. The commenters argued that these entities may be subject to the SEC's rules, because such a list could confuse entities that are on the list but do not qualify as financial institutions or creditors.

We appreciate these concerns, and seek to minimize potential unnecessary burdens on regulated entities. As we acknowledge above, the entities that are not listed in the rule's scope section may be less likely to qualify as financial institutions or creditors under the FCRA, e.g., because they do not hold transaction accounts for consumers. The Dodd-Frank Act required the SEC to adopt identity theft red flags rules with respect to persons that are "subject to the jurisdiction of the Securities and Exchange Commission." Expressly excluding from certain requirements of the rules any entities that are registered with the SEC, are subject to the SEC's enforcement authority, and are covered by the scope of the rules likely would not effectively implement the purposes of the Dodd-Frank Act and the FCRA, which are described in this release. In addition, we continue to believe that specifically listing in the scope section the entities that are likely to be subject to the rules—if they qualify as financial institutions or creditors—will provide useful guidance to those entities in determining their status under the rules. Therefore, we are adopting the scope section of the rules as proposed.

i. Definition of Financial Institution

As discussed above, the Commissions' final red flags rules apply to "financial institutions" and "creditors." As in the proposed rules, the Commissions are defining the term "financial institution" in the final rules by reference to the definition of the term in section 603(t) of the FCRA. That section defines a financial institution as an "organization that is engaged in the business of extending credit, making loans, purchasing or otherwise acquiring loans, or taking other loans as collateral in the ordinary course of business." 15 U.S.C. 1681s(b)(1)(G).

42/See supra note 37 and accompanying text. For further discussion of the extent to which investment advisers, which are specifically listed in the rules' scope section, may qualify as financial institutions or creditors, see infra notes 55–60 and 73–76 and accompanying text.

43/See supra note 37 and accompanying text. For further discussion of the extent to which investment advisers, which are specifically listed in the rules' scope section, may qualify as financial institutions or creditors, see infra notes 55–60 and 73–76 and accompanying text.

44/See supra note 37 and accompanying text. For further discussion of the extent to which investment advisers, which are specifically listed in the rules' scope section, may qualify as financial institutions or creditors, see infra notes 55–60 and 73–76 and accompanying text.

45/See supra note 37 and accompanying text. For further discussion of the extent to which investment advisers, which are specifically listed in the rules' scope section, may qualify as financial institutions or creditors, see infra notes 55–60 and 73–76 and accompanying text.

46/See supra note 37 and accompanying text. For further discussion of the extent to which investment advisers, which are specifically listed in the rules' scope section, may qualify as financial institutions or creditors, see infra notes 55–60 and 73–76 and accompanying text.
financial institution to include certain banks and credit unions, and “any other person that, directly or indirectly, holds a transaction account (as defined in section 19(b) of the Federal Reserve Act) belonging to a consumer.” 49 Section 19(b) of the Federal Reserve Act defines “transaction account” to include an “account on which the * * * account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others.” 50 Section 603(c) of the FCRA defines “consumer” as an individual; 51 thus, to qualify as a financial institution, an entity must hold a transaction account belonging to an individual. The following are illustrative examples of an SEC-regulated entity that could fall within the meaning of the term “financial institution” because it holds transaction accounts belonging to individuals: (i) A broker-dealer that offers custodial accounts; (ii) a registered investment company that enables investors to make wire transfers to other parties or that offers check-writing privileges; and (iii) an investment adviser that directly or indirectly holds transaction accounts and that is permitted to direct payments or transfers out of those accounts to third parties. 52

A few commenters raised concerns about the SEC’s statements in the Proposing Release regarding the possibility that some investment advisers could be financial institutions under certain circumstances. These commenters argued that investment advisers generally do not “hold” transaction accounts, thus meaning that they would not be financial institutions under the definition. 53 One commenter requested that we state that investment advisers who are authorized to withdraw assets from investors’ accounts to pay bills, or otherwise direct payments to third parties, on behalf of investors do not “indirectly” hold such accounts and therefore are not financial institutions. 54 The SEC has concluded otherwise. As described below, some investment advisers do hold transaction accounts, both directly and indirectly, and thus may qualify as financial institutions under the rules as we are adopting them. As discussed further in Section III of this release, SEC staff anticipates that the following examples of circumstances in which certain entities, particularly investment advisers, may qualify as financial institutions may lead some of these entities that had not previously complied with the Agencies’ rules to now determine that they should comply with Regulation S-ID. 55 Investment advisers who have the ability to direct transfers or payments from accounts belonging to individuals to third parties upon the individuals’ instructions, or who act as agents on behalf of the individuals, are susceptible to the same types of risks of fraud as other financial institutions, and individuals who hold transaction accounts with these investment advisers bear the same types of risks of identity theft and loss of assets as consumers holding accounts with other financial institutions. If such an adviser does not have a program in place to verify investors’ identities and detect identity theft red flags, another individual may deceive the adviser by posing as an investor. The red flags program of a bank or other qualified custodian 56 that maintains physical custody of an investor’s assets would not adequately protect individuals holding transaction accounts with such advisers, because the adviser could give an order to withdraw assets, but at the direction of an impostor. 57 Investors who entrust their assets to registered investment advisers that directly or indirectly hold transaction accounts should receive the protections against identity theft provided by these rules.

For instance, even if an investor’s assets are physically held with a qualified custodian, an adviser that has authority, by power of attorney or otherwise, to withdraw money from the investor’s account and direct payments to third parties according to the investor’s instructions would hold a transaction account. However, an adviser that has authority to withdraw money from an investor’s account solely to deduct its own advisory fees would not hold a transaction account, because the adviser would not be making the payments to third parties. 58 Registered investment advisers to private funds also may directly or indirectly hold transaction accounts. 59 If an individual invests money in a private fund, and the adviser to the fund has the authority, pursuant to an arrangement with the private fund or the individual, to direct such individual’s investment proceeds (e.g., redemptions, distributions, dividends, interest, or other proceeds related to the individual’s account) to third parties, then that adviser would indirectly hold a transaction account. For example, a private fund adviser would hold a transaction account if it has the authority to direct additional redemption proceeds to other persons upon instructions received from the investor. 60

ii. Definition of Creditor

The Commissions’ final definitions of “creditor” refer to the definition of...
“creditor” in the FCRA as amended by the Clarification Act.61 The FCRA now defines “creditor,” for purposes of the red flags rules, as a creditor as defined in the Equal Credit Opportunity Act62 (“ECOA”) (i.e., a person that regularly extends, renewes or continues credit, makes those credit arrangements) that “regularly and in the course of business advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.”63 The FCRA excludes from this definition a creditor that “advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person.”64

The CFTC’s definition of “creditor” includes certain entities (such as FCMs and CTAs) that regularly extend, renew, or continue credit or make those credit arrangements.65 The proposed definition applies the definition of “creditor” from 15 U.S.C. 1681m(e)(4) to “any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, swap dealer, or major swap participant that regularly extends, renewes, or continues credit; regularly arranges for the extension, renewal, or continuation of credit; or in acting as an assignee of an original creditor, participates in the decision to extend, renew, or continue credit.”66 One commenter stated that the proposed definition was overly broad and unclear because it did not appear to include derivative clearing organizations (“DCOs”) such as the Options Clearing Corporation, while the SEC’s definition could be read to include DCOs, and recommended that DCOs be explicitly excluded from the definition.67 The commenter further requested that the Commissions specifically exclude DCOs from the scope of the Proposed Rules.

As the commenter noted, the CFTC’s definition of “creditor” excludes DCOs because DCOs are not included on the list of entities that may qualify as creditors under the rule. Under the proposed CFTC rules, a “creditor” includes any entity that takes advances of the exception in the definition to advance funds on behalf of a person for expenses incidental to a service provided by the creditor to the person.68 Our final rules do not treat investment advisers differently than any other entity under the definition of “creditor.”69 An investment adviser could potentially qualify as a creditor if it “advances funds” to an investor that are not for expenses incidental to services provided by that adviser. For example, a private

63 See § 162.30(b)(5) (CFTC); § 248.201(b)(5) (SEC); see also supra note 31.

64 Section 702(e) of the ECOA defines “creditor” to mean “any person who regularly extends, renewes, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.” 15 U.S.C. 1691(a).

65 The Commissions are defining “credit” by reference to its definition in the FCRA. See § 162.30(b)(4) (CFTC); § 248.201(b)(4) (SEC). That definition refers to the definition of credit in the ECOA, which defines “credit” as “the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.” The Agencies define credit in the same manner in their identity theft red flags rules. See, e.g., 16 CFR 681.1(b)(4) (FTC) (defining “credit” as having the same meaning as in 15 U.S.C. 1691(a)(5), which defines “credit” as having the same meaning as in section 702 of the ECOA).

66 15 U.S.C. 1681m(e)(4)(A)(ii). The FCRA defines a “creditor” also to include a creditor as defined in the ECOA that “regularly and in the ordinary course of business (i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction; (ii) furnishes information to a consumer reporting agency * * * in connection with a credit transaction * * *” 15 U.S.C. 1681m(1)(4)(A)(ii). The Clarification Act does not define the extent to which the advancement of funds for expenses would be considered “incidental” to services rendered by the creditor. The legislative history indicates that the Clarification Act was intended to ensure that lawyers, doctors, and other small businesses that may advance funds to pay for services such as expert witnesses, or that may bill in arrears for services provided, should not be considered creditors under the red flags rules. See 156 Cong. Rec. S3288–9 (daily ed. Nov. 30, 2010) (statements of Senators Thune and Dodd).

67 See § 162.30(b)(7).

68 OCC Comment Letter.

69 See § 162.10(b).

70 See proposed § 248.201(b)(5).
broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties. The Commissions are defining an “account” as 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.” The CFTC’s definition specifically includes an extension of credit, such as the purchase of property or services involving a deferred payment. The SEC’s definition includes, as examples of accounts, “a brokerage account, a mutual fund account (i.e., an account with an open-end investment company), and an investment advisory account.”

In the Proposing Release, the Commissions noted that “entities that adopt red flags Programs would focus their attention on ‘covered accounts’ for indicia of possible identity theft.” In response to this statement, one commenter recommended revising the definition of “covered account” such that entities that adopt red flags Programs would focus particularly on protecting various types of information provided by customers, rather than focusing on particular categories of accounts. The Commissions have decided not to revise the definition of “covered account” as suggested by this commenter, because the Commissions believe that by focusing the rules on the types of accounts that might pose a reasonably foreseeable risk of identity theft, financial institutions and creditors are best able to protect the information that customers provide in the course of holding these accounts. Moreover, the current definition and scope of the term “covered account” are similar to the provisions of the other Agencies’ identity theft red flags rules. As discussed below, the Commissions believe that the final rules’ terms should be defined as the Agencies defined them in their respective final rules, where appropriate, to foster consistent regulations.

Two commenters argued that insurance company separate accounts are unlikely to be covered accounts because they are not established for personal, family, or household purposes and do not pose a reasonably foreseeable risk of identity theft. They contended that insurance company separate accounts are investment vehicles underlying variable life and annuity insurance products, and generally individual customers do not have a direct relationship with these accounts. One of the commenters requested that the definition of “covered account” specifically exclude insurance company separate accounts. The commenter noted that because third parties and customers do not have direct access to insurance company separate accounts, there is little risk of identity theft in these accounts.

The final rules require all financial institutions and creditors to assess whether they offer or maintain covered accounts. Although, as discussed above, some commenters suggested that insurance company separate accounts may not qualify as covered accounts under the definition, the final rule does not exclude insurance company separate accounts from the definition of “covered account” because it would be impracticable to provide an exhaustive list of account types that are not covered accounts. Similarly, one commenter requested that the SEC list all of the types of accounts that would be “covered accounts” under the rules. The rules provide examples of covered accounts, but we cannot anticipate all of the types of accounts that could be covered accounts. Any list that attempts to encompass all types of covered accounts would likely be under-inclusive and would not take into account future business practices. The

78 However, a private fund adviser would not qualify as a creditor solely because its private funds regularly borrow money from third-party credit facilities pending receipt of investor contributions, as the definition of “creditor” does not include “indirect” creditors.

79 To be a financial institution, an entity must hold a transaction account with at least one “consumer” (defined as an “individual” in 15 U.S.C. 1681a(b)), or, once an entity is a financial institution, it must periodically determine whether it offers or maintains “covered accounts” to or on behalf of its customers, which may be individuals or business entities. Sections 162.30(b)(1)(i) (CFTC) and 248.201(b)(1) (SEC) define “customer” to mean a person that has a covered account with a financial institution or creditor. The Commissions are including this definition for two reasons. First, this definition is the same as the definition of “customer” in the Agencies’ final rules. Second, because the definition uses the term “person,” it includes types of business entities (e.g., small businesses) that could be victims of identity theft. 15 U.S.C. 1681a(b).

Although the definition of “customer” is broad, not every account held by or offered to a customer will be considered a covered account, as the identification of covered accounts under the identity theft red flags rules is based on a risk-based determination. See infra notes 95–100 and accompanying text.

80 See § 248.201(b)(3)(i).

81 See § 248.201(b)(3)(i).

82 See supra note 8, at 63721.

83 See § 162.30(b)(3)(ii).

84 For example, an institution that holds only accounts for personal, family, or household purposes that permit multiple payments. The rule’s requirement that a financial institution or creditor periodically determine whether it holds covered accounts is designed to require that these entities re-evaluate whether they in fact hold any covered accounts. See infra notes 95 and 96 and accompanying text.

85 See infra note 93 and accompanying text.

86 Comment Letter of Kenneth Orgoglioso (May 7, 2012); FSR/SIFMA Comment Letter.

87 See id. (“Further, third parties, including customers, do not have direct access to Separate Accounts, which means that the types of identity theft risks anticipated by the proposed Red Flags Rules are essentially nonexistent.”).

88 For example, an institution that holds only business accounts may decide later to offer accounts for personal, family, or household purposes that permit multiple payments. The rule’s requirement that a financial institution or creditor periodically determine whether it holds covered accounts is designed to require that these entities re-evaluate whether they in fact hold any covered accounts. See infra notes 95 and 96 and accompanying text.
definition of “covered account” is deliberately designed to be flexible to allow the financial institution or creditor to determine which accounts pose a reasonably foreseeable risk of identity theft and protect them accordingly. Therefore, we are adopting the definitions of “account” and “covered account” as they were proposed.

The identity theft red flags rules also define several other terms as the Agencies defined them in their final rules, where appropriate, to foster consistent regulations. In addition, terms that the SEC’s rules do not define have the same meaning they have in FCRA.

iv. Determination of Whether a Covered Account Is Offered or Maintained

As under the proposed rules, under the final rules, each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As part of this periodic determination, a financial institution or creditor must conduct a risk assessment that takes 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. A financial institution or creditor should consider whether, for example, a reasonably foreseeable risk of identity theft may exist in connection with accounts it offers or maintains that may be opened or accessed remotely or through methods that do not require face-to-face contact, such as through email or the Internet, or by telephone. In addition, if financial institutions or creditors offer or maintain accounts that have been the target of identity theft, they should factor those experiences into their determination. The Commissions anticipate that entities will be able to demonstrate that they have complied with applicable requirements, including their recurring determinations regarding covered accounts.

The Commissions acknowledge that some financial institutions or creditors regulated by the Commissions do not offer or maintain accounts for personal, family, or household purposes, and engage predominantly in transactions with businesses, where the risk of identity theft is minimal. In these instances, the financial institution or creditor may determine after a preliminary risk assessment that the accounts it offers or maintains do not pose a reasonably foreseeable risk to customers or to its own safety and soundness from identity theft, and therefore it does not need to develop and implement a Program because it does not offer or maintain any “covered accounts.” Alternatively, the financial institution or creditor may determine that only a limited range of its accounts present a reasonably foreseeable risk to customers, and therefore may decide to develop and implement a Program that applies only to those accounts or types of accounts.

3. The Elements of the Program

The final rules set out the four elements that financial institutions and creditors must include in their Programs. These elements are being adopted as proposed and are identical to the elements required under the Agencies’ final identity theft red flags rules.

First, the final rules require a financial institution or creditor to develop a Program that includes reasonable policies and procedures to identify relevant red flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those red flags into the Program.

rules. See, e.g., §162.30(d)(1)(CFTC) and §248.201(d)(1)(SEC) (program requirements).

101 See §162.30(d)(1) (CFTC) and §248.201(d)(1) (SEC).

102 See §162.30(d)(2) (CFTC) and §248.201(d)(2) (SEC).

103 See 2007 Adopting Release, supra note 8, at 63726–63730.

104 §162.30(b)(10) (CFTC) and §248.201(b)(10) (SEC) define “red flag” to mean a pattern, practice, or specific activity that indicates the possible existence of identity theft.

105 §162.30(b)(2)(i)(CFTC) and §248.201(b)(2)(i)(SEC). The board of directors, appropriate committee thereof, or designated senior management employee may determine that a Program designed by a parent, subsidiary, or affiliated entity is also appropriate for use by the financial institution or creditor. In making such a decision,

Continued
singing out specific red flags as mandatory or requiring specific policies and procedures to identify possible red flags, this first element provides financial institutions and creditors with flexibility in determining which red flags are relevant to their businesses and the covered accounts they manage over time. The list of factors that a financial institution or creditor should consider (as well as examples) are included in Section II of the guidelines, which appear at the end of the final rules.\footnote{See Section II.B.2 below.}

Given the changing nature of identity theft,\footnote{See § 248.201(d)(2)(i) (SEC).} the Commissions believe that this element allows financial institutions or creditors to respond and adapt to new forms of identity theft and the attendant risks as they arise.

Second, the final rules require financial institutions and creditors to have reasonable policies and procedures to detect the red flags that the Program incorporates.\footnote{See § 248.201(d)(2)(ii) (SEC).} This element does not provide a specific method of detection. Instead, section III of the guidelines provides examples of various means to detect red flags.\footnote{See § 248.201(d)(2)(iii) (SEC).}

Third, the final rules require financial institutions and creditors to have reasonable policies and procedures to respond appropriately to any red flags that they detect.\footnote{See § 248.201(d)(2)(iv) (SEC).} This element incorporates the requirement that a financial institution or creditor assess whether the red flags that are detected evidence a risk of identity theft and, if so, determine how to respond appropriately based on the degree of risk. Section IV of the guidelines sets out a list of aggravating factors and examples that a financial institution or creditor should consider in determining the appropriate response.\footnote{See § 248.201(b)(2) (SEC).}

Finally, the rules require financial institutions and creditors to have reasonable policies and procedures to periodically update the Program (including the red flags determined to be relevant), to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.\footnote{See § 162.30(e) (CFTC) and § 248.201(e) (SEC). As discussed above, financial institutions and creditors are required to determine which red flags are relevant to their businesses and the covered accounts they offer or maintain. The Commissions are requiring a periodic update, rather than immediate or continuous updates, to be parallel with the identity theft red flags rules of the Agencies and to avoid unnecessary regulatory burdens. Section V of the guidelines provides a set of factors that should cause a financial institution or creditor to update its Program.\footnote{See § 248.201(a)(1)(C) (SEC).} We received no comment on the proposed elements of Programs and are adopting them as proposed.}

4. Administration of the Program

The final rules provide direction to financial institutions and creditors regarding the administration of Programs as a means of enhancing the effectiveness of those Programs.\footnote{See § 248.201(b)(2)(i) (SEC).} First, the final rules require that a financial institution or creditor obtain approval of the initial written Program from either its board of directors, an appropriate committee of the board of directors, or if the entity does not have a board, from a designated senior management employee.\footnote{See § 248.201(b)(2)(ii) (SEC).} This requirement highlights the responsibility of the board of directors in approving a Program. One commenter asked us to clarify that an entity that already has an existing Program in place, in compliance with the other Agencies’ rules, need not have the board reapprove the Program to comply with this requirement.\footnote{See § 248.201(b)(2)(iii) (SEC).}

We agree that if a financial institution or creditor already has a Program in place, the board is not required to reapprove the existing Program in response to this requirement, provided the Program otherwise meets the requirements of the final rules.

Second, the final rules provide that financial institutions and creditors must involve the board of directors, an appropriate committee thereof, or a designated senior management employee in the oversight, development, implementation, and administration of the Program.\footnote{See § 248.201(e) (SEC).} The designated senior management employee who is responsible for the oversight of a broker-dealer’s, investment company’s or investment adviser’s Program may be the entity’s chief compliance officer.\footnote{See § 248.201(e) (SEC).} Third, the final rules provide that financial institutions and creditors must train staff, as necessary, to effectively implement their Programs.\footnote{See § 248.201(e)(4) (SEC).}

Finally, the rules provide that financial institutions and creditors must exercise appropriate and effective oversight of service provider arrangements.\footnote{See § 248.201(e)(5) (SEC).} The Commissions believe that it is important that the rules address service provider arrangements so that financial institutions and creditors remain legally responsible for compliance with the rules, irrespective of whether such financial institutions and creditors outsource their identity theft red flags detection, prevention, and mitigation operations to a service provider.\footnote{See § 248.201(e)(6) (SEC).} The final rules do not prescribe a specific manner in which appropriate and effective oversight of service provider arrangements must occur. Instead, the requirement provides flexibility to financial institutions and creditors in maintaining their service provider arrangements, while making clear that such institutions and creditors are still required to fulfill their legal compliance obligations.\footnote{See § 248.201(e)(7) (SEC).} We received no comments on the substance of this aspect of the proposal and are adopting the requirements related to the administration of Programs as proposed.
B. Final Guidelines

As amended by the Dodd-Frank Act, section 615(e)(1)(A) of the FCRA provides that the Commissions must jointly "establish and maintain guidelines for use by each financial institution and each creditor regarding identity theft with respect to account holders at, or customers of, such entities, and update such guidelines as often as necessary."123 Accordingly, the Commissions are jointly adopting guidelines in an appendix to the final identity theft red flags rules that are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of the rules. These guidelines are substantially similar to the guidelines adopted by the Agencies.

The final rules require each financial institution or creditor that is required to implement a Program to consider the guidelines and include in its Program those guidelines that are appropriate.124 The Program needs to contain reasonable policies and procedures to fulfill the requirements of the final rules, even if a financial institution or creditor determines that one or more guidelines are not appropriate for its circumstances. We received no comment on the guidelines, and the Commissions are adopting them as proposed.

1. Section I of the Guidelines—Identity Theft Prevention Program

Section I of the guidelines makes clear that a financial institution or creditor may incorporate into its Program, 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. An example of such existing policies, procedures, and other arrangements may include other policies, procedures, and arrangements that the financial institution or creditor has developed to prevent fraud or otherwise ensure compliance with applicable laws and regulations.

2. Section II of the Guidelines—Identifying Relevant Red Flags

Section II(a) of the guidelines sets out several risk factors that a financial institution or creditor must consider in identifying relevant red flags for covered accounts, as appropriate. These risk factors are: (i) The types of covered accounts a financial institution or creditor offers or maintains; (ii) the methods it provides to open or access its covered accounts; and (iii) its previous experiences with identity theft. Thus, for example, red flags relevant to one type of covered account may differ from those relevant to another type of covered account. Under the guidelines, a financial institution or creditor also should consider identifying as relevant those red flags that directly relate to its previous experiences with identity theft.

Section II(b) of the guidelines sets out examples of sources from which financial institutions and creditors should derive relevant red flags. As discussed in the Proposing Release, this section of the guidelines does not require financial institutions and creditors to incorporate relevant red flags strictly from these sources. Instead, financial institutions and creditors must consider them when developing a Program.

Section II(c) of the guidelines identifies five categories of red flags that financial institutions and creditors must consider including in their Programs, as appropriate:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- Presentation of suspicious documents, such as documents that appear to have been altered or forged;
- Presentation of suspicious personal identifying information, such as a suspicious address change;
- Unusual use of, or other suspicious activity related to, a covered account; and
- 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.

Supplement A to the guidelines includes a non-comprehensive list of examples of red flags from each of these categories.

3. Section III of the Guidelines—Detecting Red Flags

Section III of the guidelines provides examples of policies and procedures that a financial institution or creditor must consider including in its Program’s policies and procedures for the purpose of detecting red flags. As discussed in the Proposing Release, entities that are currently subject to the Agencies’ identity theft red flags rules,125 the federal customer identification program ("CIP") rules126 or other Bank Secrecy Act rules,127 the Federal Financial Institutions Examination Council’s guidance on authentication,128 or the Interagency Guidelines Establishing Information Security Standards129 may already be engaged in detecting red flags. These entities may wish to integrate the policies and procedures already developed for purposes of complying with these rules and standards into their Programs. However, such policies and procedures may need to be supplemented.130

4. Section IV of the Guidelines—Preventing and Mitigating Identity Theft

Section IV of the guidelines states that a Program’s policies and procedures should provide for appropriate responses to the red flags that a financial institution or creditor has detected, that are commensurate with the degree of risk posed by each red flag. In determining an appropriate response, under the guidelines, a financial institution or creditor is required to consider aggravating factors that may heighten the risk of identity theft.

Section IV of the guidelines also provides several examples of appropriate responses. These examples are identical to those included in the Agencies’ final guidelines. Financial institutions and creditors also may consider adopting measures to prevent and mitigate identity theft that are not listed in the guidelines.

5. Section V of the Guidelines—Updating the Identity Theft Prevention Program

Section V of the guidelines includes a list of factors on which a financial institution or creditor could base the periodic updates to its Program. These factors are: (i) The experiences of the financial institution or creditor with identity theft; (ii) changes in methods of

---

124 See § 162.30(f) (CFTC) and § 248.201(f) (SEC).
125 See supra note 8.
126 See, e.g., 31 CFR 1023.220 (broker-dealers), 1024.220 (mutual funds), and 1026.220 (futures
128 See, e.g., 31 CFR 1023.220 (broker-dealers), 1024.220 (mutual funds), and 1026.220 (futures
129 See 31 CFR 103.130 (anti-money laundering programs for mutual funds).
132 For example, the CIP rules were written to implement section 326 [31 U.S.C. 5318(l)] of the USA PATRIOT Act (Pub. L. 107–56 (2001)), and certain types of “accounts,” “customers,” and products are exempted or treated specially in the CIP rules because they pose a lower risk of money laundering or terrorist financing. Such special treatment may not be appropriate to accomplish the broader objective of detecting, preventing, and mitigating identity theft.
identity theft; (iii) changes in methods to
detect, prevent, and mitigate identity
thief; (iv) changes in the types of
accounts that the financial institution or
creditor offers or maintains; and (v)
changes in the business arrangements of
the financial institution or creditor,
including mergers, acquisitions,
alliances, joint ventures, and service
provider arrangements.

6. Section VI of the Guidelines—
Methods for Administering the Identity
Theft Prevention Program

Section VI of the guidelines provides
additional guidance for financial
institutions and creditors to consider in
administering their Programs. These
guideline provisions are substantially
identical to those prescribed by the
Agencies in their final guidelines.

i. Oversight of Identity Theft Prevention
Program

Section VI(a) of the guidelines states
that oversight by the board of directors,
an appropriate committee of the board,
or a designated senior management
employee should include: (i) Assigning
specific responsibility for the Program’s
implementation; (ii) reviewing reports
prepared by staff regarding compliance
by the financial institution or creditor
with the final rules; and (iii) approving
material changes to the Program as
necessary to address changing identity
theft risks.

ii. Reporting to the Board of Directors

Section VI(b) of the guidelines states
that 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 senior
management employee, at least
annually, on compliance by the
financial institution or creditor with
the final rules. In addition, section VI(b)
of the guidelines provides that the report
should address material matters related
to the Program and evaluate issues such
as recommendations for material
changes to the Program.131

iii. Oversight of Service Provider
Arrangements

Section VI(c) of the guidelines provides
that 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. As discussed in
the Proposing Release, the
Commissions believe that these
guidelines make clear that a service
provider that provides services to
multiple financial institutions and
creditors may do so in accordance with
its own program to prevent identity
theft, as long as the service provider’s
program meets the requirements of the
identity theft red flags rules.

Section VII of the guidelines includes,
as an example of how a
financial institution or creditor may
 comply with this provision, that 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. In
those circumstances, the Commissions
eXpect that the contractual arrangements
would include the provision of
sufficient documentation by the service
provider to the financial institution or
creditor to enable it to assess
compliance with the identity theft red
flags rules.

7. Section VII of the Guidelines—Other
Applicable Legal Requirements

Section VII of the guidelines identifies
other applicable legal requirements from
the FCRA and USA PATRIOT Act that
financial institutions and creditors
should keep in mind when developing,
implementing, and administering their
Programs.

8. Supplement A to the Guidelines

Supplement A to the guidelines
provides illustrative examples of red
flags that financial institutions and
creditors are required to consider
incorporating into their Programs, as
appropriate. These examples are
substantially similar to the examples
identified in the Agencies’ final
guidelines. The examples are organized
under the five categories of red flags that
are set forth in section II(c) of the
guidelines.

The Commissions recognize that some
of the examples of red flags may be
more reliable indicators of identity theft,
while others are more reliable when
detected in combination with other red
flags. The Commissions intend that
Supplement A to the guidelines be
flexible and allow a financial institution
or creditor to tailor the red flags it
chooses for its Program to its own
operations. Although the final rules do
not require a financial institution or
creditor to justify to the Commissions
failure to include in its Program a
specific red flag from the list of
examples, a financial institution or
creditor has to account for the overall
effectiveness of its Program, and ensure
that the Program is appropriate to the
entity’s size and complexity, and to the
nature and scope of its activities.

C. Final Card Issuer Rules

Section 615(e)(1)(C) of the FCRA
provides that the CFTC and SEC must
"prescribe regulations applicable to card
issuers to ensure that, if a card issuer
receives notification of a change of
address for an existing account, and
within a short period of time (during at
least the first 30 days after such
notification is received) receives a
request for an additional or replacement
card for the same account, the card
issuer may not issue the additional or
replacement card, unless the card issuer
applies certain address validation
procedures."132 Accordingly, the
Commissions are adopting rules that set
out the duties of card issuers regarding
changes of address.133 These rules are
similar to the final card issuer rules
adopted by the Agencies.134 The rules
apply only to a person that issues a
debit or credit card ("card issuer") and
that is subject to the enforcement
authority that issue debit or credit cards
as also discussed in the
Proposing Release, the CFTC is not aware of any
entities subject to its enforcement
authority that issue debit or credit cards
and, as a matter of practice, believes that
it is highly unlikely that CFTC-regulated
entities would issue debit or credit
cards. As also discussed in the
Proposing Release, the SEC understands
that a number of entities within its
enforcement authority issue cards in
partnership with affiliated or
unaffiliated banks and financial
institutions, but that these cards are
generally issued by the partner bank,
and not by the SEC-regulated entity. The
SEC therefore expects that no entities
within its enforcement authority will be
subject to the card issuer rules.

131 The other issues referenced in the guideline are: (i) 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; (ii) service
provider arrangements; and (iii) significant
incidents involving identity theft and
management’s response.

133 See § 162.32 (CFTC) and § 248.202 (SEC).
134 See, e.g., 16 CFR 681.3 (FTC).
135 See supra Section II.A.1.
III. Related Matters

A. Cost-Benefit Considerations (CFTC) and Economic Analysis (SEC)

CFTC

Section 15(a) of the CEA \(^{136}\) requires the CFTC to consider the costs and benefits of its actions before promulgating a regulation under the CEA or issuing certain orders. Section 15(a) further specifies that the costs and benefits shall be evaluated in light of the following five broad areas of market and public concern: (1) Protection of market participants and the public; (2) efficiency, competitiveness, and financial integrity of futures markets; (3) price discovery; (4) sound risk management practices; and (5) other public interest considerations. The CFTC considers the costs and benefits resulting from its discretionary determinations with respect to the section 15(a) considerations.\(^{137}\) In the paragraphs that follow, the CFTC summarizes the proposal and comments to the same before considering the costs and benefits of the final rule in light of the 15(a) considerations.

Cost-Benefit Considerations of Identity Theft Red Flags Rules

Background and Proposal. As discussed above, section 1088 of the Dodd-Frank Act transferred authority over certain parts of FCRA from the Agencies to the CFTC and the SEC for entities they regulate. On February 28, 2012, the CFTC, together with the SEC, issued proposed rules to help protect investors from identity theft by ensuring that FCMs, IBs, CPOs, and other CFTC-regulated entities create programs to detect and respond appropriately to red flags.\(^{138}\) The proposed rules, which were substantially similar to rules adopted in 2007 by the FTC and other federal financial regulatory agencies, would require CFTC-regulated entities to adopt written identity theft programs that include reasonable policies and procedures to: (1) Identify relevant red flags; (2) detect the occurrence of red flags; (3) respond appropriately to the detected red flags; and (4) periodically update their programs. The proposed rules also included guidelines and examples of red flags to help regulated entities administer their programs.

In its proposed consideration of costs and benefits pursuant to CEA section 15(a), the CFTC stated that section 162.30 should not result in any significant new costs or benefits because it generally reflects a statutory transfer of enforcement authority from the FTC to the CFTC. The CFTC requested comment on all aspects of its proposed consideration of costs and benefits.

Comments. The CFTC received two comments on its consideration of the costs and benefits of the joint proposal. These two commenters were divided on the reasonableness of the Commissions’ estimated costs of compliance. In a letter focused on the SEC’s proposed regulations (which are, of course, substantially similar to the CFTC’s proposed regulations), one commenter stated that because Regulation S–ID “is substantially similar to” the existing FTC rules and guidelines, broker-dealers should not bear “any new costs in coming into compliance with proposed Regulation S–ID.” Another commenter further stated that “broker-dealers should already have in place a program that complies with the FTC rule. While firms will need to update some of their procedures to reflect the SEC’s new responsibility for the oversight of the application of this rule, many of the changes would be cosmetic and grammatical in nature.”\(^{139}\) In marked contrast, another comment letter, submitted on behalf of the Financial Services Roundtable (“FSR”) and the Securities Industry and Financial Markets Association (“SIFMA”), stated that the “consensus of our members is that the estimated compliance costs for the proposed Rules are extremely low and unrealistic.”\(^{140}\)

The FSR/SIFMA Comment Letter also stated that the FSR and SIFMA members estimated that the initial compliance burden to implement the rules would average 2,000 hours for each line of business conducted by a “large, complex financial institution,” noting that the estimate would vary based on the number of “covered accounts” for each line of business. In addition, this comment letter also stated that continuing compliance monitoring for such an institution would average 400 hours annually. They did not provide any data or information from which the CFTC could replicate its estimates.

The FSR/SIFMA Comment Letter also stated that “financial institutions with an existing Red Flags program would experience an incremental burden due to reassessing the scope of the ‘covered accounts’ and reevaluating whether a business activity would be defined as a ‘financial institution’ or as a ‘creditor’ for purposes of the Agencies’ Rules.”\(^{142}\)

The letter did not attribute a time estimate to this “incremental burden.” Finally, the FSR/SIFMA Comment Letter contended that the Commissions’ “estimated compliance costs further fail to consider the cost to third-party service providers, many of which may be required to implement an identity theft program even though they are not financial institutions or creditors.”\(^{143}\)

CFTC Response to Comments Regarding Costs and Benefits. In considering the costs and benefits of the final rules, the CFTC stated that each CFTC-regulated entity covered by the final rules is already in existence and acting in compliance with the law, including the FTC’s identity theft rules.\(^{144}\) Under this assumption, the CFTC believes, as one of the commenters did,\(^{145}\) that entities will incur few if any new costs in complying with the CFTC’s regulations because they are largely unchanged in terms of scope and substance from the FTC’s rules. The CFTC believes that the costs of compliance for such entities may actually decrease as a result of the additional guidance provided in this rulemaking. Without such guidance from the CFTC, entities might incur the costs of seeking advice from third parties. With respect to the comment that CFTC-regulated entities will experience an “incremental burden” in reassessing covered accounts and determining whether their activities fall within the scope of the rules,\(^{146}\) the CFTC notes that the FTC’s identity theft rules also include the requirement to periodically reassess covered accounts, and thus costs associated with this requirement are not new costs.

With regard to the estimate in the FSR/SIFMA Comment Letter that a “large, complex financial institution” would incur 2,000 hours of “initial compliance burden,”\(^{147}\) the CFTC is unaware of any such institution that is not already in compliance with the FCRA and the FTC’s rules. But even if such a large, complex financial institution exists and is not already in compliance with FCRA and the FTC’s rules, the “initial burden” that such an entity would incur is largely attributable to the FCRA, as amended by the Dodd-Frank Act. As discussed above,

---

\(^{136}\) 7 U.S.C. 19(a).

\(^{137}\) Id.

\(^{138}\) See NSCP Comment Letter.

\(^{139}\) See FSR/SIFMA Comment Letter.

\(^{140}\) Id.

\(^{141}\) See NSCP Comment Letter.

\(^{142}\) See FSR/SIFMA Comment Letter.

\(^{143}\) Id.

\(^{144}\) As discussed above, the final rules implement a shift in oversight of identity theft rules for CFTC-regulated entities from the FTC to the CFTC. The rules do not contain new requirements, nor do they substantially expand the scope of the FTC’s rules. Most entities should already be in compliance with the FTC’s existing rules, which the FTC began enforcing on January 1, 2011.

\(^{145}\) See NSCP Comment Letter.

\(^{146}\) See supra note 142 and accompanying text.

\(^{147}\) See FSR/SIFMA Comment Letter.
Congress mandated that the CFTC promulgate rules to bring its regulated entities into compliance with FCRA, and the CFTC has elected to do so in a manner that imposes minimal incremental cost on CFTC-regulated entities. In response to the comments concerning the costs to “third-party service providers,” the CFTC stresses these costs have already been taken into account, as CFTC-regulated entities that have outsourced identity theft detection, prevention, and mitigation operations to affiliates or third-party service providers have effectively shifted a burden that the CFTC-regulated entities otherwise would have carried themselves.

One commenter also stated that since it maintains no covered accounts and has no plans to, it should be specifically excluded from the scope of the rules to avoid any potential that it would be subject to the requirements of the final rules. According to this commenter, to include it within the scope of the final rules would require it needlessly to incur compliance costs associated with periodically reassessing whether they maintain any covered accounts and documenting the same.148

The majority of the per-entity costs associated with the final rules would be incurred by those financial institutions and creditors that maintain covered accounts.149 Additionally, even if financial institutions and creditors do not currently maintain, or intend to maintain, covered accounts, such entities must nevertheless periodically assess whether they maintain covered accounts, as certain accounts may be deemed to be “covered accounts” if reasonably foreseeable identity theft risks are associated with these accounts.150 Moreover, the CFTC reiterates that the final rules do not contain any new requirements or significantly expand the scope of the pre-existing FTC rules. Therefore, no financial institutions or creditors, regardless of whether they maintain covered accounts, should incur any additional costs other than the costs already being incurred under the previous regulatory framework.

Consideration of Costs and Benefits in Light of CEA Section 15(a). As discussed above, the Dodd-Frank Act shifted enforcement authority over CFTC-regulated entities that are subject to section 615(e) of the FCRA from the FTC to the CFTC. Section 615(e) of the FCRA, as amended by the Dodd-Frank Act, requires that the CFTC, jointly with the Agencies and the SEC, adopt identity theft red flags rules. To carry out this requirement, the CFTC is adopting section 162.30, which is substantially similar to the identity theft red flags rules adopted by the Agencies in 2007.

Section 162.30 will shift oversight of identity theft rules of CFTC-regulated entities from the FTC to the CFTC. These entities should already be in compliance with the FTC’s existing identity theft red flags rules, which the FTC began enforcing on January 1, 2011. Because section 162.30 is substantially similar to those existing rules, these entities should not bear any significant costs in coming into compliance with section 162.30. The new regulation does not contain new requirements, nor does it expand the scope of the rules significantly. The new regulation does contain examples and minor language changes designed to help guide entities within the CFTC’s enforcement authority in complying with the rules, which the CFTC expects will mitigate costs of compliance. Moreover, section 162.30 would not impose any significant new costs on new entities since any newly-formed entities would already be covered under the FTC’s existing rules.

In the analysis for the Paperwork Reduction Act of 1995 (“PRA”) below, the staff identified certain initial and ongoing hour burdens and associated time costs related to compliance with section 162.30. However, these costs are not new costs, but are current costs associated with compliance with the Agencies’ existing rules. CFTC-regulated entities will incur these hours and costs regardless of whether the CFTC adopts section 162.30. Therefore, these costs would be transferred from the Agencies’ PRA allotment to the CFTC. No new costs should result from the adoption of section 162.30.

These existing costs related to section 162.30 would include, for newly-formed CFTC-regulated entities, the one-time cost for financial institutions and creditors to conduct initial assessments of covered accounts, create a Program, obtain board approval of the Program, and train staff.151 The existing costs would also include the ongoing cost to periodically review and update the Program, report periodically on the Program, and conduct periodic assessments of covered accounts.152

The benefits related to adoption of section 162.30, which already exist in connection with the Agencies’ identity theft red flags rules, would include a reduction in the risk of identity theft for investors (consumers) and cardholders, and a reduction in the risk of losses due to fraud for financial institutions and creditors. It is not practicable for the CFTC to estimate with precision a dollar value associated with the benefits that will inure to the public from the adoption of section 162.30, as the quantity or value of identity theft

---

148 See OCC Comment Letter.
149 See infra notes 151 and 152.
150 See supra notes 95–100 and accompanying text.

---

\[ \text{based on the following calculations: } 354 \times 12 \text{ hours} = $4,248; 566 + 17 = $1,122; 40,000 \times x = \frac{5,770}{2} = $2,885,000. \]

As discussed in the PRA analysis, CFTC staff estimates that there are 702 CFTC-regulated entities that newly form each year and that would fall within the definitions of “institution” or “creditor.” Of these 702 entities, 54 entities would maintain covered accounts. See infra note 168 and text following note 168. CFTC staff estimates that 2 hours of internal counsel’s time would be spent conducting an initial assessment to determine whether they have covered accounts and whether they are subject to the proposed rule (or 702 entities). The cost associated with this determination is $497,016 based on the following calculation: $354 \times 2 = $708; 708 + 702 = $1,496,016. CFTC staff estimates that 54 entities would bear the remaining specified costs for a total cost of $683,748 (54 \times 12,662 = $683,748). See SFIMA’s Office Salaries in the Securities Industry 2011.

Staff also estimates that in response to Dodd-Frank, there will be approximately 125 newly registered SDs and MSPs. Staff believes that each of these SDs and MSPs will be a financial institution or creditor with covered accounts. The additional cost of these SDs and MSPs is $1,671,250 (125 \times 13,370 = $1,671,250).

CFTC staff estimates that the ongoing burden of compliance would include 2 hours to conduct periodic assessments of covered accounts, 4 hours to periodically review and update the Program, and 4 hours to prepare and present an annual report to the board, for a total of 8 hours. CFTC staff estimates that, of the 8 hours incurred, 7 hours would be spent by internal counsel at an hourly rate of $354 and 1 hour would be spent by the board of directors as a whole, at an hourly rate of $4,000, for a total hourly cost of $6,000. This estimate is based on the following calculations rounded to two significant digits: $354 \times 7 \text{ hours} = $2,478; $4,000 \times 1 \text{ hour} = $4,000; $2,478 + $4,000 = $6,478 = $6,000.

As discussed in the PRA analysis, CFTC staff estimates that 2,946 existing CFTC-regulated entities would be financial institutions or creditors, of which 260 maintain covered accounts. CFTC staff estimates that 2 hours of internal counsel’s time would be spent conducting periodic assessments of covered accounts and that all financial institutions or creditors subject to the proposed rule (2,946 entities) would bear this cost for a total cost of $2,100,000 based on the following calculations rounded to two significant digits: $354 \times 2 = $708; $708 = \frac{2,100,000}{2} = $1,050,000. CFTC staff estimates that 260 entities would bear the remaining specified ongoing costs for a total cost of $1,500,000 (260 \times 5,770 = $1,500,000).
deterred or prevented is not knowable. The CFTC, however, recognizes that the cost of any given instance of identity theft may be substantial to the individual involved. Joint adoption of identity theft red flags rules in a form that is substantially similar to the Agencies’ identity theft red flags rules might also benefit financial institutions and creditors because entities regulated by multiple federal agencies could comply with a single set of standards, which would reduce potential compliance costs. As is true of the Agencies’ generally similar red flags rules, the CFTC has designed section 162.30 to provide financial institutions and creditors significant flexibility in developing and maintaining a Program that is tailored to the size and complexity of their business and the nature of their operations, as well as in satisfying the address verification procedures.

Accordingly, as previously discussed, section 162.30 should not result in any significant new costs or benefits, because it merely reflects a statutory transfer of enforcement authority from the FTC to the CFTC, does not include any significant new requirements, and does not include new entities that were not previously covered by the Agencies’ rules.

Section 15(a) Analysis. As stated above, the CFTC is required to consider costs and benefits of proposed CFTC action in light of (1) protection of market participants and the public; (2) efficiency, competitiveness, and financial integrity of futures markets; (3) price discovery; (4) sound risk management practices; and (5) other public interest considerations. These rules protect market participants and the public by detecting, preventing, and mitigating identity theft, an illegal act that may be costly to them in both time and money. Because, however, these rules create no new requirements — rather, as explained above, the CFTC is adopting rules that reflect requirements already in place — the impact of the rules on the protection of market participants and the public will remain the same. The Commission is not aware of any effect of these rules on the efficiency, competitiveness, and financial integrity of futures markets.

The existing costs related to section 162.32 would include a reduction in the risk of identity theft for cardholders, and a reduction in the risk of losses due to fraud for card issuers. However, it is not practicable for the CFTC to estimate with precision the dollar value associated with the benefits that will accrue to the public from these card issuer rules. As true of the Agencies’ card issuer rules, the CFTC has designed section 162.32 to provide card issuers significant flexibility in developing and maintaining a Program that is tailored to the size and complexity of their business and the nature of their operations.

Accordingly, as previously discussed, the card issuer rules should not result in any significant new costs or benefits, because they generally reflect a statutory transfer of enforcement authority from the FTC to the CFTC, do not include any significant new requirements, and do not include new entities that were not previously covered by the Agencies’ rules.

Section 15(a) Analysis. As stated above, the CFTC is required to consider costs and benefits of proposed CFTC action in light of (1) protection of market participants and the public; (2) efficiency, competitiveness, and financial integrity of futures markets; (3) price discovery; (4) sound risk management practices; and (5) other public interest considerations. These rules protect market participants and the public by detecting, preventing, and mitigating identity theft, an illegal act that may be costly to them in both time and money. Because, however, these rules create no new requirements — rather, as explained above, the CFTC is adopting rules that reflect requirements already in place — the impact of the rules on the protection of market participants and the public will remain the same. The Commission is not aware of any effect of these rules on the efficiency, competitiveness, and financial integrity of futures markets.

153 According to the Javelin 2011 Identity Fraud Survey Report, consumer costs (the average out-of-pocket dollar amount victims pay) increased in 2010. See Javelin 2011 Identity Fraud Survey Report (2011). The report attributed this increase to new account fraud, which showed longer periods of misuse and detection and therefore more dollar losses associated with it than any other type of fraud. Notwithstanding the increase in cost, the report stated that the number of identity theft victims has decreased in recent years. Id.

154 See id.
SEC

The SEC is sensitive to the costs and benefits imposed by its rules. As discussed above, the Dodd-Frank Act shifted enforcement authority over SEC-regulated entities subject to section 615(e) of the FCRA from the Agencies to the SEC. Section 615(e) of the FCRA, as amended by the Dodd-Frank Act, requires that the SEC, jointly with the Agencies and the CFTC, adopt identity theft red flags rules and guidelines. To carry out this requirement, the SEC is adopting Regulation S–ID, which is substantially similar to the identity theft red flags rules and guidelines adopted by the Agencies in 2007, and whose scope covers the same categories of SEC-regulated entities that were covered under the Agencies’ red flags rules.

Regulation S–ID requires a financial institution or creditor that is subject to the SEC’s enforcement authority and that offers or maintains covered accounts to develop, implement, and administer a written identity theft prevention Program. A financial institution or creditor must design its Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. A financial institution or creditor must take certain steps to comply with the requirements of the identity theft red flags rules, including training staff, providing annual reports to the board of directors, an appropriate committee thereof, or a designated senior management employee, and, if applicable, oversight of service providers.

Section 615(e)(1)(C) of the FCRA singles out change of address notifications sent to credit and debit card issuers as a possible indicator of identity theft, and requires the SEC to prescribe regulations concerning such notifications. Accordingly, the card issuer rules in this release set out the duties of card issuers regarding changes of address. The card issuer rules apply only to SEC-regulated entities that issue credit or debit cards. The card issuer rules require a card issuer to comply with certain address validation procedures in the event that such issuer receives a notification of a change of address for an existing account, and within a short period of time (during at least the first 30 days after it receives such notification) receives a request for an additional or replacement card for the same account. The card issuer may not issue the additional or replacement card unless it complies with those procedures. The procedures include: (1) Notifying the cardholder of the request either at the cardholder’s former address, or by any other means of communication that the card issuer and the cardholder have previously agreed to use; or (2) assessing the validity of the change of address in accordance with established policies and procedures.

The baseline we use to analyze the economic effects of Regulation S–ID is the identity theft red flags regulatory scheme administered by the Agencies. Regulation S–ID, as discussed above, implements the transfer of oversight of identity theft red flags rules for SEC-regulated entities from the Agencies to the SEC. Entities that qualify as a financial institution or creditor and offer or maintain covered accounts should already have existing identity theft red flags Programs. Regulation S–ID does not contain new requirements, nor does it expand the scope of the Agencies’ rules to include new entities that the Agencies’ rules did not previously cover. Regulation S–ID does contain examples and minor language changes designed to help guide entities within the SEC’s enforcement authority in complying with the rules. Because Regulation S–ID is substantially similar to the Agencies’ rules, the entities within its scope should not bear new costs in coming into compliance with Regulation S–ID.

Costs

The costs of complying with section 248.201 of Regulation S–ID include both ongoing costs and initial, one-time costs. These are the same costs that were associated with the requirements of the Agencies’ red flags rules, and these costs will continue to apply after the adoption of the SEC’s identity theft red flags rules (section 248.201 of Regulation S–ID). The ongoing costs include the costs to periodically review and update the Program, report on the Program, and conduct assessments of covered accounts. All entities that qualify as financial institutions or creditors and that maintain covered accounts will bear the costs of including entities subject to Regulation S–ID should already bear, and will continue to bear, the ongoing costs.

Initial, one-time costs relate to the initial assessments of covered accounts, creation of a Program, board approval of the Program, and the training of staff. New entities will bear these costs.

156 See, e.g., NSCP Comment Letter (“Because proposed Regulation S–ID is substantially similar to [the Agencies’] existing rules and guidelines, broker-dealer firms should not bear any new costs in coming into compliance with proposed Regulation S–ID.”). As previously indicated, the SEC staff understands that a number of investment advisers may not currently have identity theft red flags Programs. See supra note 53 and infra notes 186 and 190. Thus, the costs in this release may lead some of these entities to determine that they should comply with Regulation S–ID. Although the costs and benefits of Regulation S–ID discussed below would be new to these entities, the costs would result not from Regulation S–ID but instead from the entities’ recognition that these rules and the previously-existing rules apply to them. In that regard, the initial, one-time costs of Regulation S–ID could be up to $756 for each investment adviser that qualifies as a financial institution or creditor, and additional one-time costs of $13,885 for each such investment adviser that maintains covered accounts. See infra notes 158 and 159. Not all investment advisers will bear the full extent of these costs, however, as some may already have in place certain identity theft protections. And, the guidance in this release could have the benefit of reducing identity theft. See infra discussion of benefits in Part III.A. of this release.

157 See infra note 182 and accompanying text.

158 Unless otherwise stated, all cost estimates for personnel time are derived from SIFMA’s Management & Professional Earnings in the Securities Industry 2011, modified to account for an 1800-hour work-year and multiplied by 5.35 to account for bonuses, entity size, employee benefits, and overhead. The estimates in this release, both for salary rates and numbers of entities affected, have been updated from those in the Proposing Release to reflect recent SIFMA management and professional salary data.

SEC staff estimates that the ongoing burden of compliance will include 2 hours to conduct periodic assessments of covered accounts, 2 hours to periodically review and update the Program, and 4 hours to prepare and present an annual report to the board, for a total of 8 hours. SEC staff estimates that, of the 8 hours incurred, 7 hours will be spent by internal counsel at an hourly rate of $378 and 1 hour will be spent by the board of directors as a whole, at an hourly rate of $180, for a total of $1,320 for each hour of $7146 per entity. This estimate is based on the following calculations: $378 × 7 hours = $2646; $4500 × 1 hour = $4500; $2646 + $4500 = $7146. The cost estimate for the board of directors is derived from estimates made by SEC staff regarding typical board size and compensation that is based on information received from fund representatives and publicly available sources.

As discussed in the PRA analysis, SEC staff estimates that 10,339 existing SEC-regulated entities will be financial institutions or creditors under Regulation S–ID, and approximately 90%, or 9305, of these entities will maintain covered accounts. See infra notes 190 and 191 and accompanying text. SEC staff estimates that 2 hours of internal counsel’s time will be spent conducting periodic assessments of covered accounts and that a financial institutions or creditors subject to the rule (or 10,339 entities) will bear this cost for a total cost of $7,816,284 based on the following calculations: $378 × 2 × 10,339 = $7,816,284. SEC staff estimates that 9305 entities will bear the remaining specified ongoing costs for a total cost of $59,458,950 (9305 × ($378 × 5) + ($4500 × 1)) = $59,458,950.

159 SEC staff estimates that the incremental one-time burden of compliance includes 2 hours to conduct initial assessments of covered accounts, 25 hours to develop and obtain board approval of a Program, and 4 hours to train staff. SEC staff estimates that, of the 31 hours incurred, 12 hours will be spent by internal counsel at an hourly rate of $378, 17 hours will be spent by administrative personnel at an estimated hourly rate of $7146, and 2 hours will be spent by the board of directors at an estimated hourly rate of $180. The total cost estimate is $71,460.
As discussed above, the final rules require financial institutions and creditors to tailor their Programs to the size and complexity of the entity and to the nature and scope of the entity’s activities. Ongoing and one-time costs will therefore depend on the size and complexity of the SEC-regulated entity. Entities may already have other policies and procedures in place that are designed to reduce the risks of identity theft for their customers. The presence of other related policies and procedures could reduce the ongoing and one-time costs.160

Two commenters agreed with the SEC that the substantial similarity of Regulation S–ID to the Agencies’ rules should minimize any compliance costs for entities that have previously complied with the Agencies’ rules,160 and another commenter stated that the benefits of reduced risk of identity theft would outweigh the costs associated with the rules.161 Another commenter raised concerns with the cost estimates in the Proposing Release, and argued that actual costs of compliance could be much greater than estimated.162 This commenter provided hour burden estimates for large, complex financial institutions that were significantly higher than the estimates made for those entities in the Proposing Release. Additionally, the commenter stated that the Commissions’ estimated compliance costs did not consider the costs to third-party service providers that may be required to implement an identity theft red flags Program, even though they are not financial institutions or creditors. The commenter also noted, however, that burdens placed upon the entities currently complying with the Agencies’ rules would be the same burdens that each of these entities already incurs in regularly assessing whether it maintains covered accounts and evaluating whether it falls within the rules’ scope. We note that the commenter who suggested that significantly higher hour burdens would be associated with the rules focused on large, complex financial institutions. Regulation S–ID requires each financial institution and creditor to tailor its Program to its size and complexity, and to the nature and scope of its activities. Our estimates take into account the hour burdens for small financial institutions and creditors, which we understand, based on discussions with industry representatives, to be significantly less than the estimates provided by this commenter. We also note that costs to service providers have already been taken into account, as SEC-regulated entities that have outsourced identity theft detection, prevention, and mitigation operations to service providers have already effectively shifted a burden that the SEC-regulated entities otherwise would have carried themselves.163 As mentioned above, the costs of Regulation S–ID are not new, and existing entities should already have identity theft red flags Programs and bear the ongoing costs associated with Regulation S–ID.

The existing costs related to the card issuer rules (section 248.202 of Regulation S–ID) include the cost for card issuers to establish policies and procedures that assess the validity of a change of address notification submitted shortly before a request for an additional or replacement card and, before issuing an additional or replacement card, either notify the cardholder at the previous address or through another previously agreed-upon form of communication, or alternatively assess the validity of the address change through existing policies and procedures. As discussed in the PRA analysis, SEC staff does not expect that any SEC-regulated entities will be subject to the card issuer rules.164

In the PRA analysis below, the staff identifies certain ongoing and initial hour burdens and associated time costs related to compliance with Regulation S–ID. These hour burdens and costs are consistent with those associated with the requirements of the Agencies’ existing rules.

Benefits

The benefits related to adoption of Regulation S–ID, which already exist in connection with the Agencies’ identity theft red flags rules, include a reduction in the risk of identity theft for investors (consumers) and cardholders, and a reduction in the risk of losses due to fraud for financial institutions and creditors. The SEC is the federal agency best positioned to oversee the financial institutions and creditors subject to its enforcement authority because of its experience in overseeing these entities. Adoption of Regulation S–ID therefore may have the added benefit of increasing entities’ adherence to their identity theft red flags Programs, thus further reducing the risk of identity theft for investors. As is true of the Agencies’ identity theft red flags rules, the SEC has designed Regulation S–ID to provide financial institutions, creditors, and card issuers significant flexibility in developing and maintaining a Program that is tailored to the size and complexity of their business and the nature of their operations, as well as in satisfying the address verification procedures. Many of the benefits and costs discussed are difficult to quantify, in particular when discussing the potential reduction in the risk of identity theft. The SEC staff cannot quantify the benefits of the potential reduction in the risk of identity theft because of the uncertainty of its effect on customer behavior. Therefore, we discuss much of the benefits qualitatively but, where possible, the SEC staff attempted to quantify the costs.

Alternatives

In analyzing the costs and benefits that could result from the implementation of Regulation S–ID, the
SEC also considered the costs and benefits of any plausible alternatives to the final rules as set forth in this release. As discussed above, section 615(e) of the FCRA, as amended by the Dodd-Frank Act, requires that the SEC, jointly with the Agencies and the CFTC, adopt identity theft red flags rules and guidelines that are substantially similar to those adopted by the Agencies. The rules the SEC promulgates should achieve a similar outcome with respect to the reduction in the risk of identity theft as the rules of other Agencies. Alternatives to the identity theft red flags rules that would achieve a similar outcome may impose additional costs, especially for those entities that would need to alter existing Programs to conform to a new set of rules. The SEC does provide additional guidance in this release to better enable entities to determine whether they fall within the rules’ scope. Although the SEC could have provided different guidance with this release, the SEC believes that the release provides sufficient guidance to enable entities to determine whether they need to adopt identity theft red flags Programs. Lastly, for the reasons discussed above, the SEC is not exempting certain entities from certain requirements of the identity theft red flags rules. The SEC believes that if an entity determines that it is a financial institution or a creditor that offers or maintains covered accounts, then the risk of identity theft that the rules are designed to address is present. Under such circumstances, we believe that the benefits of the rules justify the costs to the financial institution or creditor subject to the rules and, therefore, no exemptions are appropriate.

**B. Analysis of Effects on Efficiency, Competition, and Capital Formation**

Section 3(f) of the Exchange Act and section 2(c) of the Investment Company Act require the SEC, whenever it engages in rulemaking and must consider or determine if an action is necessary, appropriate, or consistent with the public interest, to consider, in addition to the protection of investors, whether the action would promote efficiency, competition, and capital formation. In addition, section 23(a)(2) of the Exchange Act requires the SEC, when making rules under the Exchange Act, to consider the impact the rules may have upon competition. Section 23(a)(2) of the Exchange Act prohibits the SEC from adopting any rule that would impose a burden on competition that is not necessary or appropriate in furtherance of the purposes of the Exchange Act.\(^{164}\)

As discussed in the cost-benefit analysis above, Regulation S–ID will carry out the requirement in the Dodd-Frank Act that the SEC adopt rules governing identity theft protections, pursuant to section 615(e) of the FCRA with regard to entities that are subject to the SEC’s enforcement authority. This requirement was designed to transfer regulatory oversight of identity theft red flags rules for SEC registered entities from the Agencies to the SEC. Regulation S–ID is substantially similar to the identity theft red flags rules adopted by the Agencies in 2007, and does not contain new requirements. The entities covered by Regulation S–ID should already be in compliance with existing identity theft red flags rules.

For the reasons discussed above, Regulation S–ID should have a negligible effect on efficiency, competition, and capital formation because it does not include new requirements and does not include new entities that were not previously covered by the Agencies’ rules.\(^{165}\) The SEC thereby finds that, pursuant to Exchange Act section 23(a)(2), the adoption of Regulation S–ID would not result in any burden on competition, efficiency, or capital formation that is not necessary or appropriate in furtherance of the purposes of the Exchange Act.

\(^{164}\) See infra Section IV (setting forth statutory authority under, among other things, the Exchange Act and Investment Company Act for rulemakings).

\(^{165}\) See infra note 182 (discussing the entities that the SEC staff considers to be financial institutions in landmark rulemakings with industry representatives and a review of applicable law, will fall within the scope of Regulation S–ID). The SEC staff understands, however, that a number of investment advisers may not currently have identity theft red flags Programs. See supra note 55. The guidance in this release regarding situations in which certain SEC-regulated entities could qualify as financial institutions or creditors should not produce any significant effects. These entities may experience a negligible increase to business efficiency due to the industry-specific guidance in this release regarding the types of activities that could cause an entity to fall within the scope of Regulation S–ID. The guidance should also have a negligible effect on capital formation. Prior to Regulation S–ID, investors preferring to base their capital allocations on the existence of identity theft red flags Programs could have allocated capital with entities adhering to the Agencies’ rules. The guidance therefore should have a negligible effect on the amount of capital allocated for investment purposes. In addition, all entities that conclude based on this guidance that they are subject to the final rules will be subject to the same requirements, and experience the same costs and benefits, as all other entities currently adhering to the Agencies’ existing rules. The guidance therefore should have a negligible effect on competition.

**C. Paperwork Reduction Act**

**CFTC**

Provisions of sections 162.30 and 162.32 contain collection of information requirements within the meaning of the PRA. The CFTC submitted the proposal to the Office of Management and Budget (“OMB”) for review and public comment, in accordance with 44 U.S.C. 3507(d) and 5 CFR 1320.11. The title for this collection of information is “Part 162 Subpart C—Identity Theft.” Responses to this new collection of information are mandatory.

1. Information Provided by Reporting Entities/Persons

Under part 162, subpart C, CFTC regulated entities—which presently would include approximately 260 CFTC registrants\(^{166}\) plus 123 new CFTC registrants pursuant to Title VII of the Dodd-Frank Act\(^{167}\)—are required to develop, design, and implement reasonable policies and procedures to identify relevant red flags, and potentially to notify cardholders of identity theft risks. In addition, CFTC-regulated entities are required to: (i) Collect information and keep records for the purpose of ensuring that their Programs met requirements to detect, prevent, and mitigate identity theft in...
connection with the opening of a covered account or any existing covered account; (ii) develop and implement reasonable policies and procedures to identify, detect and respond to relevant red flags, as well as periodic reports related to the Program; and (iii) from time to time, notify cardholders of possible identity theft with respect to their covered accounts, as well as assess the validity of those accounts.

These burden estimates assume that CFTC-regulated entities already comply with the identity theft red flags rules jointly adopted by the FTC with the Agencies, as of January 1, 2011. Consequently, these entities may already have in place many of the customary protections addressing identity theft and changes of address required by these regulations.

Burden means the total time, effort, or financial resources expended by persons to generate, maintain, retain, disclose or provide information to or for a federal agency. Because compliance with identity theft red flags rules jointly adopted by the FTC with the Agencies may have occurred, the CFTC estimates the time and cost burdens of complying with part 162 to be both one-time and ongoing burdens. However, any initial or one-time burdens associated with compliance with part 162 would apply only to newly-formed entities, and the ongoing burden to all CFTC-regulated entities.

i. Initial Burden

The CFTC estimates that the one-time burden of compliance with part 162 for its regulated entities with covered accounts would be: (i) 25 hours to develop and obtain board approval of a Program; (ii) 4 hours for staff training; and (iii) 2 hours to conduct an initial assessment of covered accounts, totaling 31 hours. Of the 31 hours, the CFTC estimates that 15 hours would involve internal counsel, 14 hours expended by administrative assistants, and 2 hours by the board of directors in total, for those newly-regulated entities.

The CFTC estimates that approximately 702 FCMS, CTAs and CPOs would need to conduct an initial assessment of covered accounts. As noted above, the CFTC estimates that approximately 125 newly registered SDs and MSPs would need to conduct an initial assessment of covered accounts. The total number of newly registered CFTC registrants would be 827 entities. Each of these 827 entities would need to conduct an initial assessment of covered accounts, for a total of 1,654 hours. Of these 827 entities, CFTC staff estimates that approximately 179 of these entities may maintain covered accounts. Accordingly, the CFTC estimates the one-time burden for these 179 entities to be 5,191 hours, for a total burden among newly registered entities of 6,845 hours.

ii. Ongoing Burden

The CFTC staff estimates that the ongoing compliance burden associated with part 162 would include: (i) 2 hours to periodically review and update the Program, review and preserve contracts with service providers, and review and preserve any documentation received from such providers; (ii) 4 hours to prepare and present an annual report to the board; and (iii) 2 hours to conduct periodic assessments to determine if the entity offers or maintains covered accounts, for a total of 8 hours. The CFTC staff estimates that of the 8 hours expended, 7 hours would be spent by internal counsel, and 1 hour would be spent by the board of directors as a whole.

The CFTC estimates that approximately 3,071 entities may maintain covered accounts, and that they would be required to periodically review their internal guidelines, as required to be considered if they comply with these rules, for a total of 6,142 hours for these entities. Of these 3,071 entities, the CFTC estimates that approximately 385 maintain covered accounts, and thus would need to incur the additional burdens related to complying with the rule, for a total of 2,310 hours. The total ongoing burden for all CFTC registrants is 8,452 hours.

The CFTC estimates that the one-time burden of compliance with the proposed rules, and the ongoing burden for all CFTC registrants is 8,452 hours.

SEC: Provisions of sections 248.201 and 248.202 contain “collection of information” requirements within the meaning of the PRA. In the Proposing Release, the SEC solicited comment on the collection of information requirements. The SEC also submitted the proposed collections of information to the OMB for review in accordance with 44 U.S.C. 3507(d) and 5 CFR 1320.11. The title for this collection of information is “Part 248, Subpart C—Regulation S-ID.” In response to this submission, the OMB issued control number 3239–0692. Responses to the new collection of information provisions are mandatory, and the information, when provided to the SEC in connection with staff examinations or investigations, is kept confidential to the extent permitted by law.

1. Description of the Collections

Under Regulation S–ID, SEC-regulated entities are required to develop and implement reasonable policies and procedures to identify, detect and respond to relevant red flags and, in the case of entities that issue credit or debit cards, to assess the validity of, and communicate with cardholders regarding, address changes. Section 248.201 of Regulation S–ID includes the following “collections of information” by SEC-regulated entities that are financial institutions or creditors if the entity maintains covered accounts: (1) Creation and periodic updating of a Program that is approved by the board of directors, an appropriate committee thereof, or a designated senior management employee; (2) periodic staff reporting on compliance with the identity theft red flags rules and guidelines, as required to be considered by section VI of the guidelines; and (3) training of staff to implement the Program. Section 248.202 of Regulation S–ID includes the following “collections of information” by SEC-regulated entities that are credit or debit card issuers: (1) Establishment of policies and procedures that assess the validity of
of a change of address notification if a request for an additional or replacement card on the account follows soon after the address change; and (2) notification of a cardholder, before issuance of an additional or replacement card, at the previous address or through some other previously agreed-upon form of communication, or alternatively, assessment of the validity of the address change request through the entity’s established policies and procedures.

SEC-regulated entities that must comply with the collections of information required by Regulation S–ID should already be in compliance with the identity theft red flags rules that the Agencies jointly adopted in 2007.176 The requirements of those rules are substantially similar and comparable to the requirements of Regulation S–ID.177

In addition, SEC staff understands that most SEC-regulated entities that are financial institutions or creditors may otherwise have in place many of the protections regarding identity theft and changes of address that Regulation S–ID requires because they are usual and customary business practices that they engage in to minimize losses from fraud. Furthermore, SEC staff believes that many of them are likely to have already effectively implemented most of the requirements as a result of having to comply (or an affiliate having to comply) with other, existing statutes, regulations and guidance, such as the federal CIP rules implementing section 326 of the USA PATRIOT Act,178 the Interagency Guidelines Establishing Information Security Standards that implement section 501(b) of the Gramm-Leach-Bliley Act (GLBA),179 section 216 of the FACT Act,180 and guidance issued by the Agencies or the Federal Financial Institutions Examination Council regarding information security, authentication, identity theft, and response programs.181

SEC staff estimates of time and cost burdens represent the one-time burden of complying with Regulation S–ID for newly-formed SEC-regulated entities, and the ongoing costs of compliance for all SEC-regulated entities.182 SEC staff estimates also attribute all burdens to entities that are directly subject to the requirements of the rulemaking. An entity directly subject to Regulation S–ID that outsources activities to a service provider is, in effect, shifting to that service provider the burden that it would otherwise have carried itself. Under these circumstances, the burden is, by contract, shifted from the entity that is directly subject to Regulation S–ID to the service provider, but the total amount of burden is not increased.

Thus, service provider burdens are already included in the burden estimates provided for entities that are directly subject to Regulation S–ID. The time and cost estimates made here are based on conversations with industry representatives and on a review of comments received on the proposed rules as well as the estimates made in the regulatory analyses of the identity theft red flags rules previously issued by the Agencies.

2. Section 248.201 (Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft)

The collections of information required by section 248.201 apply to SEC-regulated entities that are financial institutions or creditors.183 As stated above, SEC staff expects that SEC-regulated entities should already have incurred initial or one-time burdens associated with compliance with Regulation S–ID because they should already be in compliance with the substantially identical requirements of the Agencies’ identity theft red flags rules.184 Any initial or one-time burden estimates associated with compliance with section 248.201 of Regulation S–ID apply only to newly-formed entities. The ongoing burden estimates apply to all SEC-regulated entities that are financial institutions or creditors. Existing entities subject to Regulation S–ID should already bear, and will continue to be subject to, this burden. In the Proposing Release, the SEC solicited comment on its estimates of the burdens associated with the collections of information required by section 248.201; one commenter raised concerns with the estimates in the Proposing Release, arguing that actual burdens could be greater than estimated.185

i. Initial Burden

SEC staff estimates that the one-time burden of compliance with section 248.201 for SEC-regulated financial institutions and creditors with covered accounts is: (i) 236 hours to develop and obtain board approval of a Program; (ii) 4 hours to train staff; and (iii) 2 hours to conduct an initial assessment of covered accounts, for a total of 31 hours. SEC staff estimates that, of the 31 hours incurred, 12 hours will be spent by internal counsel, 17 hours will be spent by administrative assistants, and 2 hours will be spent by the board of directors as a whole for newly-formed entities.

SEC staff estimates that approximately 668 SEC-regulated financial institutions and creditors are newly formed each year.186 Each of these 668 entities will need to conduct an initial assessment of covered accounts, for a total of 1336 hours.187 Of these 668 entities, SEC staff estimates that approximately 90% (or respect to the Agencies’ identity theft red flags rules). Because the requirements of Regulation S–ID are substantially identical to the requirements of the Agencies’ identity theft red flags rules, the SEC staff took the Agencies’ PRA analysis into account in estimating the regulatory burdens of Regulation S–ID.

Based on a review of new registrations typically filed with the SEC each year, SEC staff estimates that approximately 900 investment advisers, 231 broker-dealers, 139 investment companies, and 1 ESC typically apply for registration with the SEC or otherwise are newly formed each year, for a total of 1271 entities that could be financial institutions or creditors. Of these, SEC staff estimates that all of the investment companies, ESCs, and broker-dealers are likely to qualify as financial institutions or creditors, and 33% (or 417) of investment顾问s are likely to qualify, for a total of 668 total financial institutions or creditors that will bear the initial one-time burden of assessing covered accounts under Regulation S–ID. Information regarding the method used to estimate that 33% of investment advisers are likely to qualify as financial institutions or creditors can be found in note 190 below.

176 SEC staff, however, understands that a number of investment advisers may not currently have identity theft red flags Programs. See supra note 55. Under the new guidance, for entities having now determined that they should comply with Regulation S–ID, the collections of information required by Regulation S–ID and the estimates of time and costs discussed below may be new. As discussed further below, SEC staff estimates that there are approximately 3791 investment advisers that are currently registered with the SEC and are likely to qualify as financial institutions or creditors. SEC staff is unable to estimate how many of these investment advisers previously complied with the Agencies’ identity theft red flags rules.

177 See 2007 Adopting Release, supra note 8, at nn.55–57 (describing applicable statutes, regulations, and guidance).

178 Based on discussions with industry representatives and a review of applicable law, SEC staff expects that, of the SEC-regulated entities that fall within the scope of Regulation S–ID, most broker-dealers, many investment companies (including almost all open-end investment companies and ESCs), and some registered investment advisers will likely qualify as financial institutions or creditors. SEC staff expects that other SEC-regulated entities described in the scope section of Regulation S–ID, such as BDCs, transfer agents, NRSROs, SROs, and clearing agencies may be less likely to be financial institutions or creditors as defined in the rules, and therefore we do not include these entities in our estimates.


180 See 2007 Adopting Release, supra note 8, at Section V.A. (discussing the PRA analysis with respect to the Agencies’ identity theft red flags rules); “FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule” at http://www.ftc.gov/opfa/2010/05/redflags.shtml.


182 See supra notes 55 and 56. SEC staff notes that the one-time estimate is based on new registrations typically filed with the SEC each year, and may not accurately reflect the actual burden experienced by SEC-regulated entities that are newly formed each year. However, the SEC staff believes that the estimate of 236 hours to develop and obtain board approval of a Program is within the range of the burden that entities will experience in order to comply with the rule.

183 See supra note 162 and accompanying text.

184 Based on a review of new registrations typically filed with the SEC each year, SEC staff estimates that approximately 900 investment advisers, 231 broker-dealers, 139 investment companies, and 1 ESC typically apply for registration with the SEC or otherwise are newly formed each year, for a total of 1271 entities that could be financial institutions or creditors. Of these, SEC staff estimates that all of the investment companies, ESCs, and broker-dealers are likely to qualify as financial institutions or creditors, and 33% (or 417) of investment advisers are likely to qualify, for a total of 668 total financial institutions or creditors that will bear the initial one-time burden of assessing covered accounts under Regulation S–ID. Information regarding the method used to estimate that 33% of investment advisers are likely to qualify as financial institutions or creditors can be found in note 190 below.

185 This estimate is based on the following calculation: 668 entities x 2 hours = 1336 hours.
601) maintain covered accounts.\footnote{In the Proposing Release, the SEC requested comment on the estimate that approximately 90% of all financial institutions and creditors maintain covered accounts; the SEC received no comments on this estimate.} SEC staff estimates that the total initial burden for the 601 newly formed SEC-regulated entities that are likely to qualify as financial institutions or creditors and maintain covered accounts is 18,631 hours, and the total initial burden for all newly formed SEC-regulated entities is 18,765 hours.\footnote{Based on a review of entities that the SEC regulates, SEC staff estimates that, as of July 1, 2012, there are approximately 11,622 investment advisers, 4,706 broker-dealers, 1,692 active open-end investment companies, and 150 ESs. Of these, SEC staff estimates that all of the broker-dealers, open-end investment companies and ESs are likely to qualify as financial institutions or creditors, and approximately 3,791 investment advisers (or about 33%, as explained further below) are likely to qualify, for a total of 10,339 total financial institutions or creditors that will bear the ongoing burden of assessing covered accounts under Regulation S–ID. (The SEC staff estimates that the other broker-dealers are covered by the scope of the SEC’s rules will not be financial institutions or creditors and therefore will not be subject to the rules’ requirements. \textit{See supra note 182.)}} Accordingly, SEC staff estimates that the total ongoing burden for 601 newly formed SEC-regulated entities that maintain covered accounts is 74,440 hours.\footnote{In the Proposing Release, the SEC requested comment on this same estimate of the burdens associated with the collections of information required by section 248.202 and received no comments on its burden estimate.} The estimated total ongoing burden for the 10,339 SEC-regulated entities that are financial institutions or creditors covered by Regulation S–ID will be 76,508 hours.\footnote{Based on a review of entities that the SEC regulates, SEC staff estimates that there are 10,339 SEC-regulated entities that are either financial institutions or creditors, and that all of these are required to periodically review their accounts to determine if they offer or maintain covered accounts, for a total of 20,678 hours for these entities. These entities, which are not regulated by the SEC, are already subject to substantially similar change of address obligations pursuant to the Agencies’ identity theft red flags rules. In addition, SEC staff understands that card issuers already assess the validity of change of address requests and, for the most part, have automated the process of notifying the cardholder or using other means to assess the validity of changes of address. Therefore, implementation of this requirement poses no further burden. SEC staff does not expect that any SEC-regulated entities will be subject to the information collection requirements of section 248.202. Accordingly, SEC staff estimates that there is no hourly or cost burden for SEC-regulated entities related to section 248.202. In the Proposing Release, the SEC solicited comment on this estimate of the burdens associated with the collections of information required by section 248.202 and received no comments on its burden estimate.} ii. Ongoing Burden

SEC staff estimates that the ongoing burden of compliance with section 248.201 includes: (i) 2 hours to conduct periodic assessments to determine if the entity offers or maintains covered accounts; (ii) 4 hours to prepare and present an annual report to the board; and (iii) 2 hours to periodically review and update the Program, including review and preservation of contracts with service providers, and review and preservation of any documentation received from service providers, for a total of 8 hours. SEC staff estimates that, of the 8 hours incurred, 7 hours will be spent by counsel and 1 hour will be spent by the board of directors as a whole.

SEC staff estimates that there are 10,339 SEC-regulated entities that are financial institutions or creditors, and that all of these are required to periodically review their accounts to determine if they offer or maintain covered accounts, for a total of 20,678 hours for these entities.\footnote{In the Proposing Release, the SEC requested comment on the estimate that approximately 90% of all financial institutions and creditors maintain covered accounts; the SEC received no comments on this estimate.} SEC staff estimates that the total ongoing burden for these 9305 financial institutions and creditors that maintain covered accounts will be 74,440 hours. The estimated total ongoing burden for the 10,339 SEC-regulated entities that are financial institutions or creditors covered by Regulation S–ID will be 76,508 hours.\footnote{The collections of information required by section 248.202 apply only to SEC-regulated entities that issue credit or debit cards. SEC staff understands that SEC-regulated entities generally do not issue credit or debit cards, but instead have arrangements with other entities, such as banks, that issue cards on their behalf. These other entities, which are not regulated by the SEC, are already subject to substantially similar change of address obligations pursuant to the Agencies’ identity theft red flags rules. In addition, SEC staff understands that card issuers already assess the validity of change of address requests and, for the most part, have automated the process of notifying the cardholder or using other means to assess the validity of changes of address. Therefore, implementation of this requirement poses no further burden. Accordingly, SEC staff estimates that there is no hourly or cost burden for SEC-regulated entities related to section 248.202. In the Proposing Release, the SEC solicited comment on this estimate of the burdens associated with the collections of information required by section 248.202 and received no comments on its burden estimate.} The following calculation. According to Investment Adviser Registration Depository (IARD) data, there are approximately 11,622 investment advisers registered with the SEC as of July 1, 2012. Of these advisers, approximately 7,327 could potentially be subject to the rule as financial institutions because they indicate they have customers who are natural persons. We estimate that approximately 16%, or 1,202 of these 7,327 advisers, hold transaction accounts belonging to natural persons and therefore would qualify as financial institutions under the rule. Additionally, 6,455 of the 11,622 advisers registered with the SEC have private fund clients. We expect that most of the funds advised by these advisers would have at least one natural person investor, and thus they could potentially meet the definition of “financial institution.” In addition, some of these private fund advisers may engage in lending activities that would also qualify them as creditors under the rule. In order to avoid duplication, however, we are deducting 1,466 private fund advisers from the total number of advisers we estimate will be subject to the rule, because they also indicated to the SEC that they have individual or high net worth clients and are already accounted for in our estimates above. Accordingly, the staff estimates that approximately 3,791 (i.e., 1,202 + 4055 – 1466) advisers registered with the SEC will be subject to the rule. These 3,791 advisers are about 33% of the 11,622 SEC-registered advisers.

Accordingly, SEC staff estimates that the total ongoing burden for the 10,339 SEC-regulated entities that are financial institutions or creditors covered by Regulation S–ID will be 76,508 hours.\footnote{In the Proposing Release, the SEC requested comment on this estimate of the burdens associated with the collections of information required by section 248.202 and received no comments on its burden estimate.} According to the CFTC’s final identity theft red flags regulations, FCMs, RFEDs, IBs, CTAs, CPOs, SDs, and MSPs. SDs and MSPs are new categories of registrants. Accordingly, the CFTC has noted in other rule proposals that it has not previously addressed the question of whether such persons were, in fact, small entities for purposes of the RFA.\footnote{In this regard, the CFTC has previously determined that FCMs should not be considered to be small entities for purposes of the RFA, based, in part, upon FCMS’ obligation to meet the minimum financial requirements established by the CFTC to enhance the protection of customers’ segregated funds and protect the financial condition of FCMS generally. Like FCMS, SDs will be subject to minimum capital and margin requirements, and therefore, are not considered ‘‘small entities’’ under the Regulatory Flexibility Act (‘‘RFA’’). While the CFTC recognizes that FCMs and SDs may have different business models and may have smaller operations than other financial institutions, the CFTC concluded that FCMs and SDs are not ‘‘small entities’’ for purposes of the RFA.\footnote{5 U.S.C. 601–612.}}

\textbf{2. Section 248.202 (Duties of Card Issuers Regarding Changes of Address).} The collections of information required by section 248.202 apply only to SEC-regulated entities that issue credit or debit cards. SEC staff understands that SEC-regulated entities generally do not issue credit or debit cards, but instead have arrangements with other entities, such as banks, that issue cards on their behalf. These other entities, which are not regulated by the SEC, are already subject to substantially similar change of address obligations pursuant to the Agencies’ identity theft red flags rules. In addition, SEC staff understands that card issuers already assess the validity of change of address requests and, for the most part, have automated the process of notifying the cardholder or using other means to assess the validity of changes of address. Therefore, implementation of this requirement poses no further burden. Accordingly, SEC staff estimates that there is no hourly or cost burden for SEC-regulated entities related to section 248.202. In the Proposing Release, the SEC solicited comment on this estimate of the burdens associated with the collections of information required by section 248.202 and received no comments on its burden estimate.

\textbf{D. Regulatory Flexibility Act}\n
\textbf{CFTC}\n
The Regulatory Flexibility Act (‘‘RFA’’) requires that federal agencies consider whether the rules they propose will have a significant economic impact on a substantial number of small entities and, if so, provide a regulatory flexibility analysis respecting the impact.\footnote{47 FR 18618 (Apr. 30, 1982).} The CFTC’s final identity theft red flags regulations affect FCMs, RFEDs, IBs, CTAs, CPOs, SDs, and MSPs. SDs and MSPs are new categories of registrants. Accordingly, the CFTC has noted in other rule proposals that it has not previously addressed the question of whether such persons were, in fact, small entities for purposes of the RFA.\footnote{75 FR 81519 (Dec. 28, 2010); 76 FR 6708 (Feb. 8, 2011); 76 FR 6715 (Feb. 8, 2011).}\n
In this regard, the CFTC has previously determined that FCMs should not be considered to be small entities for purposes of the RFA, based, in part, upon FCMS’ obligation to meet the minimum financial requirements established by the CFTC to enhance the protection of customers’ segregated funds and protect the financial condition of FCMS generally.\footnote{See, e.g., 75 FR 81519 (Dec. 28, 2010).} Like FCMS, SDs will be subject to minimum capital and margin requirements, and...
are expected to comprise the largest global financial institutions—and the CFTC is required to exempt from designation as an SD entities that engage in a de minimis level of swaps dealing in connection with transactions with or on behalf of customers. Accordingly, for purposes of the RFA, the CFTC has determined that SDs not be considered “small entities” for essentially the same reasons that it has previously determined FCMs not to be small entities.\(^{199}\)

The CFTC also has previously determined that large traders are not “small entities” for RFA purposes, with the CFTC considering the size of a trader’s position to be the only appropriate test for the purpose of large trader reporting.\(^{200}\) The CFTC also has noted that MSPs maintain substantial positions in swaps, creating substantial counterparty exposure that could have serious adverse effects on the financial stability of the United States banking system or financial markets.\(^{201}\)

Accordingly, for purposes of the RFA, the CFTC has determined that MSPs not be considered “small entities” for essentially the same reasons that it has previously determined large traders not to be small entities.\(^{202}\)

The CFTC did not receive any comments on its analysis of the application of the RFA to SDs and MSPs. Moreover, the CFTC has issued final rules in which it determined that the registration and regulation of SDs and MSPs would not have a significant economic impact on a substantial number of small entities.\(^{203}\)

Further, the CFTC has determined that the requirements on financial institutions and creditors, and card issuers set forth in the identity theft red flags rules, respectively, will not have a significant economic impact on a substantial number of small entities because many of these entities are already complying with the identity theft red flags rules of the Agencies. Moreover, the CFTC believes that the rules include a great deal of flexibility to assist its regulated entities in complying with such rules and guidelines.

In accordance with 5 U.S.C. 605(b), the CFTC Chairman, on behalf of the CFTC, certifies that these rules will not have a significant economic impact on a substantial number of small entities.\(^{204}\)

The SEC has prepared the following Final Regulatory Flexibility Analysis (“FRFA”) regarding Regulation S–ID in accordance with 5 U.S.C. 604. The SEC included an Initial Regulatory Flexibility Analysis (“IRFA”) in the Proposing Release in February 2012.\(^{204}\)

1. Need for Regulation S–ID

The FACT Act, which amended FCRA to address identity theft red flags, was enacted in part to help prevent the theft of consumer information. The statute contains several provisions relating to the detection, prevention, and mitigation of identity theft. Section 1088(a) of the Dodd-Frank Act amended section 615(e) of the FCRA by adding the SEC (and CFTC) to the list of federal agencies required to adopt rules related to the detection, prevention, and mitigation of identity theft. Regulation S–ID implements the statutory directives in section 615(e) of the FCRA, which require the SEC to adopt identity theft rules jointly with the Agencies and the CFTC.

Section 615(e) requires the SEC to adopt rules that require financial institutions and creditors to establish policies and procedures to implement guidelines established by the SEC that address identity theft with respect to account holders and customers. Section 615(e) also requires the SEC to adopt rules applicable to credit and debit card issuers to implement policies and procedures to assess the validity of change of address requests.

2. Significant Issues Raised by Public Comment

In the Proposing Release, we requested comment on the IRFA. None of the comment letters we received specifically addressed the IRFA. None of the comment letters made specific comments about Regulation S–ID’s impact on smaller financial institutions and creditors.

3. Small Entities Subject to the Rule

For purposes of the Regulatory Flexibility Act (“RFA”), an investment company is a small entity if it, together with other investment companies in the same group of related investment companies, has net assets of $50 million or less as of the end of its most recent fiscal year. SEC staff estimates that approximately 11,622 investment advisers registered with the SEC are small entities.\(^{205}\)

For purposes of the RFA, a broker-dealer is a small business if it had total capital (net worth plus subordinated liabilities) of less than $500,000 on the date in the prior fiscal year as of which its audited financial statements were prepared pursuant to rule 17a–5(d) of the Exchange Act or, if not required to file such statements, a broker-dealer that had total capital (net worth plus subordinated liabilities) of less than $500,000 on the last business day of the preceding fiscal year (or in the time that it has been in business, if shorter) and if it is not an affiliate of an entity that is not a small business.\(^{206}\) SEC staff estimates that approximately 797 broker-dealers meet this definition.\(^{207}\)

4. Projected Reporting, Recordkeeping, and Other Compliance Requirements

Section 615(e) of the FCRA, as amended by section 1088 of the Dodd-Frank Act, requires the SEC to adopt rules that require financial institutions and creditors to establish reasonable policies and procedures to implement guidelines established by the SEC that address identity theft with respect to account holders and customers. Section 248.201 of Regulation S–ID implements this mandate by requiring a covered financial institution or creditor that offers or maintains certain accounts to create an identity theft prevention Program that detects, prevents, and
mitigates the risk of identity theft applicable to these accounts.

Section 615(e) also requires the SEC to adopt rules applicable to credit and debit card issuers to implement policies and procedures to assess the validity of a change of address request. Section 248.202 of Regulation S–ID implements this requirement by requiring credit and debit card issuers to establish reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a credit or debit card account and within a short period of time afterwards (within 30 days), the issuer receives a request for an additional or replacement card for the same account.

Because all SEC-regulated entities, including small entities, should already be in compliance with the substantially similar identity theft red flags rules that the Agencies began enforcing in 2008 and 2011,210 Regulation S–ID should not impose new compliance, recordkeeping, or reporting burdens. If a SEC-regulated small entity is not already in compliance with the existing identity theft red flags rules issued by the Agencies, the burden of compliance with Regulation S–ID should be minimal because we understand that these entities already engage in various activities to minimize losses due to fraud as part of their usual and customary business practices. In particular, the rules allow these entities to consolidate their existing policies and procedures into their written Program and may require some additional staff training. Accordingly, the impact of the requirements should be largely incremental and not significant, and we do not anticipate that Regulation S–ID will disproportionately affect small entities.

The SEC has estimated the costs of Regulation S–ID for all entities (including small entities) in the PRA and economic analysis included in this release. No new classes of skills are required to comply with Regulation S–ID. SEC staff does not anticipate that small entities will face unique or special burdens when complying with Regulation S–ID.

5. Agency Action To Minimize Effect on Small Entities

The RFA directs the SEC to consider significant alternatives that would accomplish our stated objective, while minimizing any significant economic impact on small issuers. In connection with Regulation S–ID, the SEC considered the following alternatives: (i)

---

210 See supra note 8.

The establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (ii) the clarification, consolidation, or simplification of compliance requirements under Regulation S–ID for small entities; (iii) the use of performance rather than design standards; and (iv) an exemption from coverage of Regulation S–ID, or any part thereof, for small entities.

Regulation S–ID requires covered financial institutions and creditors that offer or maintain certain accounts to create an identity theft prevention Program and report to the board of directors, an appropriate committee thereof, or a designated senior management employee at least annually on compliance with the regulations. Credit and debit card issuers are required to respond to a change of address request by notifying the cardholder or using other means to assess the validity of a change of address.

The standards in Regulation S–ID are flexible, and take into account a covered financial institution or creditor’s size and sophistication, as well as the costs and benefits of alternative compliance methods. A Program under Regulation S–ID should be tailored to the risk of identity theft in a financial institution or creditor’s covered accounts, thereby permitting small entities whose accounts pose a low risk of identity theft to avoid much of the cost of compliance. Because small entities maintain covered accounts that pose a risk of identity theft for consumers just as larger entities do, providing an exemption from Regulation S–ID for small entities could subject consumers with covered accounts at small entities to a higher risk of identity theft.

Pursuant to section 615(e) of the FCRA, as amended by section 1088 of the Dodd-Frank Act, the SEC and the CFTC are jointly adopting identity theft red flags rules that are substantially similar and comparable to the identity theft red flags rules previously adopted by the Agencies. Providing a new exemption for small entities, or further consolidating or simplifying the regulations for small entities, could result in significant differences between the identity theft red flags rules adopted by the Commissions and the rules adopted by the Agencies. Because SEC-regulated entities, including small entities, should already be in compliance with the substantially similar identity theft red flags rules that the Agencies began enforcing in 2008 and 2011, SEC staff does not expect that small entities will need a delayed effective or compliance date beyond that already provided to all entities subject to the rules.

IV. Statutory Authority and Text of Amendments

The CFTC is amending Part 162 under the authority set forth in sections 1088(a)(8), 1088(a)(10), and 1088(b) of the Dodd-Frank Act.211 Section 615(e) of the FCRA.212 The SEC is adopting Regulation S–ID under the authority set forth in sections 1088(a)(6), 1088(a)(10), and 1088(b) of the Dodd-Frank Act.213 Section 615(e) of the FCRA.214 Sections 17 and 23 of the Exchange Act.215 Sections 31 and 38 of the Investment Company Act.216

List of Subjects

17 CFR Part 162

Cardholders, Card issuers, Commodity pool operators, Commodity trading advisors, Confidential business information, Consumer reports, Credit, Creditors, Consumer, Customer, Financial institutions, Futures commission merchants, Identity theft, Introducing brokers, Major swap participants, Privacy, Red flags, Reporting and recordkeeping requirements, Retail foreign exchange dealers, Self-regulatory organizations, Service provider, Swap dealers.

17 CFR Part 248

Affiliate marketing, Brokers, Cardholders, Card issuers, Confidential business information, Consumers, Consumer financial information, Consumer reports, Credit, Creditors, Customers, Dealers, Financial institutions, Identity theft, Investment advisers, Investment companies, Privacy, Red flags, Reporting and recordkeeping requirements, Securities, Security measures, Self-regulatory organizations, Service providers, Transfer agents.

Text of Final Rules

Commodity Futures Trading Commission

For the reasons stated above in the preamble, the Commodity Futures
Trading Commission is amending 17 CFR part 162 as follows:

PART 162—PROTECTION OF CONSUMER INFORMATION UNDER THE FAIR CREDIT REPORTING ACT

1. The authority citation for part 162 continues to read as follows:


2. Add subpart C to part 162 read as follows:

Subpart C—Identity Theft Red Flags

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

(a) Scope of this subpart. This section applies to financial institutions or creditors that are subject to administrative enforcement of the FCRA by the Commission pursuant to Sec. 621(b)(1) of the FCRA, 15 U.S.C. 1681s(b)(1).

(b) Special definitions for this subpart. For purposes of this section, and Appendix B to this part, 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 an extension of credit, such as the purchase of property or services involving a deferred payment.

(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 senior management employee.

(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 margin 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 in Sec. 603(f)(5) of the FCRA, 15 U.S.C. 1681a(f)(5).

(5) Creditor has the same meaning as in 15 U.S.C. 1681m(e)(4), and includes any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, swap dealer, or major swap participant that regularly extends, renews, or continues credit; regularly arranges for the extension, renewal, or continuation of credit; or in acting as an assignee of an original creditor, participates in the decision to extend, renew, or continue credit.

(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) and includes any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, swap dealer, or major swap participant that directly or indirectly holds a transaction account belonging to a consumer.

(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(a)).

(9) Identity theft means a fraud committed or attempted using the identifying 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.

(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 shall 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 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 Identity Theft Prevention 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 Identity Theft Prevention Program. The Identity Theft Prevention 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 Identity Theft Prevention Program;

(ii) Detect Red Flags that have been incorporated into the Identity Theft Prevention Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(iii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Identity Theft Prevention 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 Identity Theft Prevention Program. Each financial institution or creditor that is required to implement an Identity Theft Prevention Program must provide for the continued administration of the Identity Theft Prevention Program and must:

(1) Obtain approval of the initial written Identity Theft Prevention 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 Identity Theft Prevention Program;

(3) Train staff, as necessary, to effectively implement the Identity Theft Prevention Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) Guidelines. Each financial institution or creditor that is required to implement an Identity Theft Prevention Program must consider the guidelines in appendix B of this part and include in its Identity Theft Prevention Program those guidelines that are appropriate.

§ 162.31 [Reserved]

§ 162.32 Duties of card issuers regarding changes of address.

(a) Scope. This section applies to a person described in §162.30(a) that issues a debit or credit card (card issuer).

(b) Definition of cardholder. For purposes of this section, a cardholder means a consumer who has been issued a credit or debit card.

(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) Notifies the cardholder of the request;

(2) At the cardholder’s former address; or

(3) 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

(ii) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to §162.30.

(d) Alternative timing of address validation. A card issuer may satisfy the requirements of paragraph (c)(1) 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.

3. Add Appendix B to part 162 to read as follows:

Appendix B to Part 162—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 162.30 requires each financial institution or creditor that offers or maintains one or more covered accounts, as defined in §162.30(b)(3), to develop and provide for the continued administration of a written Identity Theft Prevention 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 an Identity Theft Prevention Program that satisfies the requirements of §162.30.

I. The Identity Theft Prevention Program

In designing its Identity Theft Prevention 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 Identity Theft Prevention 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 B.

(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 Identity Theft Prevention 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; 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 Identity Theft Prevention Program’s policies and procedures should provide for appropriate responses to the Red Flags that 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 or 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 Internet 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 Identity Theft Prevention Program

Financial institutions and creditors should update the Identity Theft Prevention Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and
VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other 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-4(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. 1681x-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 provisions 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 B

In addition to incorporating Red Flags from the sources recommended in section II(b) of the Guidelines in Appendix B of this part, each financial institution or creditor may consider incorporating into its Identity Theft Prevention 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 Sec. 609(f) of the Fair Credit Reporting Act (15 U.S.C. 1681(f)).

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 or 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 or 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 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.

Securities and Exchange Commission

For the reasons stated in the preamble, the Securities and Exchange Commission is amending 17 CFR part 248 as follows:


4. The authority citation for part 248 is revised to read as follows:

Authority: 15 U.S.C. 78q, 78q-1, 78q-4, 78q-5, 78w, 78mm, 80a-30, 80a-37, 808-4, 80b-11, 1681m(e), 1681s(b), 1681s-3 and note, 1681v(a)(1), 6801-6805, and 6825; Pub. L. 111–203, secs. 1088(a)(6), (a)(10), and sec. 1088(b), 124 Stat. 1376 (2010).

5. Revise the heading for part 248 to read as set forth above.

6. Add subpart C to part 248 to read as follows:

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

Sec. 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; or

(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 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(t)(5).

(5) Creditor has the same meaning as in 15 U.S.C. 1681m(o)(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 identifying 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)).


(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)(iii) 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 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(t).

(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.

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) Its previous experiences with identity theft.
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:

1. The experiences of the financial institution or creditor with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that the financial institution or creditor offers or maintains; and
5. 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. The report should:

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:

(a) 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;
(b) Significant incidents involving identity theft and management’s response; and
(c) Changes in methods to detect, prevent, and mitigate identity theft.

(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(b) 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 I.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 605(h) of the Fair Credit Reporting Act (15 U.S.C. 1681(c)).

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;

(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.

Suspicous 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.

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.


By the Commodity Futures Trading Commission.

Melissa Jurgens,
Secretary of the Commodity Futures Trading Commission.

Dated: April 10, 2013

By the Securities and Exchange Commission.

Elizabeth M. Murphy,
Secretary of the Securities and Exchange Commission.

[FR Doc. 2013–08830 Filed 4–18–13; 8:45 am]

BILLING CODE 6351–01–P; 8011–01–p