COMMODITY FUTURES TRADING COMMISSION

17 CFR Part 162

RIN: 3038-AD14

SECURITIES AND EXCHANGE COMMISSION

17 CFR Part 248

[Release No. IC-29969; File No. S7-02-12]

RIN: 3235-AL26

Identity Theft Red Flags Rules

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

ACTIONS: Joint proposed rules and guidelines.

SUMMARY: The Commodity Futures Trading Commission ("CFTC") and the Securities and Exchange Commission ("SEC," together with the CFTC, the "Commissions") are jointly issuing proposed rules and guidelines to implement new statutory provisions enacted by Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act. These provisions amend section 615(e) of the Fair Credit Reporting Act and direct the Commissions to prescribe rules requiring entities that are subject to the Commissions' jurisdiction to address identity theft in two ways. First, the proposed rules and guidelines would require financial institutions and creditors to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with certain existing accounts or the opening of new accounts. The Commissions also are proposing guidelines to assist entities in the formulation and maintenance of a program that would satisfy the requirements of the proposed rules. Second, the proposed rules would establish special requirements for any credit and debit

card issuers that are subject to the Commissions' jurisdiction, to assess the validity of notifications of changes of address under certain circumstances.

DATES: Comments must be received on or before May 7, 2012.

ADDRESSES: Comments may be submitted by any of the following methods:

CFTC:

- Agency web site, via its Comments Online Process: Comments may be submitted to http://comments.cftc.gov. Follow the instructions for submitting comments on the Internet web site.
- Mail: David A. Stawick, Secretary, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581.
- Hand Delivery/Courier: Same as mail above.
- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

All comments must be submitted in English, or if not, accompanied by an English translation. Comments will be posted as received to www.cftc.gov. You should submit only information that you wish to make available publicly. If you wish the CFTC to consider information that may be exempt from disclosure under the Freedom of Information Act, a petition for confidential treatment of the exempt information may be submitted according to the established procedures in 17 CFR 145.9.

The CFTC reserves the right, but shall not have the obligation, to review, pre-screen, filter, redact, refuse, or remove any or all submissions from www.cftc.gov that it may deem to be inappropriate for publication, such as obscene language. All submissions that have been redacted or removed that contain comments on the merits of the rulemaking will be retained in

the public comment file and will be considered as required under the Administrative Procedure Act, 5 U.S.C. 551, et seq., and other applicable laws, and may be accessible under the Freedom of Information Act, 5 U.S.C. 552.

SEC:

Electronic comments:

- Use the SEC's Internet comment form (http://www.sec.gov/rules/proposed.shtml); or
- Send an e-mail to rule-comments@sec.gov. Please include File Number S7-02-12 on the subject line; or
- Use the Federal eRulemaking Portal (http://www.regulations.gov). Follow the instructions for submitting comments.

Paper comments:

- Send paper comments in triplicate to Elizabeth M. Murphy, Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-1090.

All submissions should refer to File Number S7-02-12.

. This file number should be included on the subject line if e-mail is used. To help us process and review your comments more efficiently, please use only one method. The SEC will post all comments on the SEC's website (http://www.sec.gov/rules/proposed.shtml). Comments are also available for website viewing and printing in the SEC's Public Reference Room, 100 F Street, NE, Washington, DC 20549 on official business days between the hours of 10:00 a.m. and 3:00 p.m. All comments received will be posted without change; we do not edit personal identifying information from submissions. You should submit only information that you wish to make available publicly.

FOR FURTHER INFORMATION CONTACT: CFTC: Carl E. Kennedy, Counsel, at Commodity Futures Trading Commission, Office of the General Counsel, Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581, telephone number (202) 418-6625, facsimile number (202) 418-5524, e-mail c_kennedy@cftc.gov; SEC: with regard to investment companies and investment advisers, contact Thoreau Bartmann, Senior Counsel, 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, or Joseph Furey, Assistant 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.

SUPPLEMENTARY INFORMATION:

The Commissions are proposing new rules and guidelines on identity theft red flags for entities subject to their respective jurisdiction. The CFTC is proposing to add new subpart C ("Identity Theft Red Flags") to part 162 of the CFTC's regulations [17 CFR part 162] and the SEC is proposing to add new subpart C ("Regulation S-ID: Identity Theft Red Flags") to part 248 of the SEC's regulations [17 CFR part 248], under the Fair Credit Reporting Act of 1970 [15 U.S.C. 1681], the Commodity Exchange Act [7 U.S.C. 1], the Securities Exchange Act of 1934 [15 U.S.C. 78], the Investment Company Act of 1940 [15 U.S.C. 80a], and the Investment Advisers Act of 1940 [15 U.S.C. 80b].

TABLE OF CONTENTS

I. BACKGROUND

II. EXPLANATION OF THE PROPOSED RULES AND GUIDELINES

A. Proposed Identity Theft Red Flags Rules
1. Which Financial Institutions and Creditors Would Be Required to Have a Program
2. The Objectives of the Program
3. The Elements of the Program
4. Administration of the Program

B. Proposed Guidelines
1. Section I of the Proposed Guidelines — Identity Theft Prevention Program
2. Section II of the Proposed Guidelines — Identifying Relevant Red Flags
3. Section III of the Proposed Guidelines — Detecting Red Flags
4. Section IV of the Proposed Guidelines — Preventing and Mitigating Identity Theft
5. Section V of the Proposed Guidelines — Updating the Identity Theft Prevention Program
6. Section VI of the Proposed Guidelines — Methods for Administering the Identity Theft Prevention Program
7. Section VII of the Proposed Guidelines — Other Applicable Legal Requirements
8. Proposed Supplement A to the Guidelines

C. Proposed Card Issuer Rules
1. Definition of "Cardholder" and Other Terms
2. Address Validation Requirements
3. Form of Notice

D. Proposed Effective and Compliance Dates

III. RELATED MATTERS

A. Cost-Benefit Analysis (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 PROPOSED AMENDMENTS

I. BACKGROUND

The growth and advancement 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 integrity and privacy of personal information.[1] 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.[2]

The Fair Credit Reporting Act of 1970[3] ("FCRA") sets standards for the collection, communication, and use of information about consumers by consumer reporting agencies.[4] Congress has amended the FCRA numerous times since 1970 to augment the protections the law provides. For example, the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act")[5]

---

1 *See, e.g.*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, INFORMATION SECURITY: FEDERAL GUIDANCE NEEDED TO ADDRESS CONTROL ISSUES WITH IMPLEMENTING CLOUD COMPUTING (May 2010) (available at http://www.gao.gov/new.items/d10513.pdf) (discussing information security implications of cloud computing); DEPARTMENT OF COMMERCE, INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK, at Section I (2010) (available at http://www.ntia.doc.gov/reports/2010/iptf_privacy_greenpaper_12162010.pdf) (reviewing recent technological changes that necessitate a new approach to commercial data protection). *See also* FRED H. CATE, PRIVACY IN THE INFORMATION AGE, at 13-16 (1997) (discussing the privacy and data security issues that arose during early increases in the use of digital data).

2 *See, e.g.*, Report of President's Identity Theft Task Force (Sept. 2008) (available at http://www.ftc.gov/os/2008/10/081021taskforcereport.pdf) (documenting governmental efforts to reduce identity theft); Testimony of Edith Ramirez, Commissioner of Federal Trade Commission, on Data Security, before House Subcommittee on Commerce, Manufacturing, and Trade, June 15, 2011 (available at http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf) (describing efforts of the Federal Trade Commission to promote data security).

3 Pub. L. 91-508, 84 Stat. 1114 (1970), *codified at* 15 U.S.C. § 1681 *et seq.*

4 The FCRA states that its purpose is "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information ...." *Id.*

5 *See* Pub. L. 108-159, 117 Stat. 1952 (2003).

amended the FCRA to enhance the ability of consumers to combat identity theft.[6] The FACT Act also amended the FCRA to direct certain federal agencies to jointly issue rules and guidelines related to identity theft.[7]

Under the FACT Act's amendments to the FCRA, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission (the "FTC") (together, the "Agencies") were required to issue joint rules and guidelines regarding the detection, prevention, and mitigation of identity theft for entities that are subject to their respective enforcement authority (the "identity theft red flags rules and guidelines").[8] The Agencies also were required to prescribe joint rules applicable to issuers of credit and debit cards, to require that such issuers assess the validity of notifications of

---

6 The Federal Trade Commission has defined "identity theft" as "a fraud committed or attempted using the identifying information of another person without authority." *See* 16 CFR 603.2(a).

7 Section 114 of the FACT Act.

8 *See* sections 615(e)(1)(A) – (B) of the FCRA, 15 U.S.C. 1681m(e)(1)(A) – (B). Section 615(e)(1)(A) of the FCRA provides that the Agencies shall 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." Section 615(e)(1)(B) provides that the Agencies shall jointly "prescribe regulations requiring each financial institution and each creditor to establish reasonable policies and procedures for implementing the guidelines established pursuant to [section 615(e)(1)(A)], to identify possible risks to account holders or customers or to the safety and soundness of the institution or customers."

changes of address under certain circumstances (the "card issuer rules").[9] In 2007, the Agencies issued joint final identity theft rules and guidelines, and joint final card issuer rules.[10]

On July 21, 2010, President Obama signed into law the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act").[11] Title X of the Dodd-Frank Act, which is titled the Consumer Financial Protection Act of 2010 ("CFP Act"), established a Bureau of Consumer Financial Protection within the Federal Reserve System and gave this new agency certain rulemaking, enforcement, and supervisory powers over many consumer financial products and services, as well as the entities that sell them. In addition, Title X amended a number of other federal consumer protection laws enacted prior to the Dodd-Frank Act, including the FCRA.

Within Title X, section 1088(a)(8),(10) of the Dodd-Frank Act amended the FCRA by adding the Commissions (CFTC and SEC) to the list of federal agencies required to jointly

---

9 Section 615(e)(1)(C) of the FCRA provides that the Agencies shall jointly "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" follows certain procedures (including notifying the cardholder at the former address) to assess the validity of the change of address. 15 U.S.C. 1681m(e)(1)(C).

10 *See* Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 FR 63718 (Nov. 9, 2007) ("2007 Adopting Release"). The Agencies' final rules also implemented section 315 of the FACT Act, which required the Agencies to adopt joint rules providing guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy. *See* 15 U.S.C. 1681c(h). The Dodd-Frank Act does not authorize the Commissions to propose rules under section 315 of the FACT Act, and therefore entities under the authority of the Commissions, for purposes of the identity theft red flags rules and guidelines, will be subject to other agencies' rules on address discrepancies. *See, e.g.,* 16 CFR 641.1 (FTC).

11 Pub. L. 111-203, 124 Stat. 1376 (2010). The text of the Dodd-Frank Act is available at http://www.cftc.gov/LawRegulation/OTCDERIVATIVES/index.htm.

prescribe and enforce identity theft red flags rules and guidelines and card issuer rules.[12] Thus, the Dodd-Frank Act provides for the transfer of rulemaking responsibility and enforcement authority to the CFTC and SEC with respect to the entities under their respective jurisdiction. Accordingly, the Commissions are now jointly proposing for public notice and comment identity theft rules and guidelines and card issuer rules.[13] The proposed rules and guidelines[14] are substantially similar to those adopted by the Agencies in 2007.[15] As discussed further below, the Commissions recognize that most of the entities over which they have jurisdiction are likely to be already in compliance with the final rules and guidelines that the Agencies adopted in 2007, to the extent that these entities' activities fall within the scope of the Agencies' final rules and guidelines. The proposed rules and guidelines, if adopted, would not contain new requirements not already in the Agencies' final rules, nor would they expand the scope of those rules to

---

12 *See* section 615(e)(1) of the FCRA, 15 U.S.C. 1681m(e)(1). In addition, section 1088(a)(10) of the Dodd-Frank Act added the Commissions to the list of federal administrative agencies responsible for enforcement of rules pursuant to section 621(b) of the FCRA. *See infra* note 19. Section 1100H of the Dodd-Frank Act provides that the Commissions' new enforcement authority (as well as other changes in various agencies' authority under other provisions) becomes effective as of the "designated transfer date" to be established by the Secretary 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. 20, 2010).

13 The CFTC is proposing to add the proposed rules and guidelines in this release as a new subpart C to part 162 of the CFTC's regulations, 17 CFR 162. *See* Business Affiliate Marketing and Disposal of Consumer Information Rules, 76 FR 43879 (July 22, 2011). As a result, the purpose, scope, and definitions in part 162 would apply to the proposed identity theft red flags rules and guidelines, as well as to the proposed card issuer rules. The new subpart C would be titled "Identity Theft Red Flags." The SEC is proposing to add the proposed rules and guidelines in this release as a new subpart C to part 248 of the SEC's regulations. 17 CFR part 248. The new subpart C is titled "Regulation S-ID: Identity Theft Red Flags."

14 For ease of reference, unless the context indicates otherwise, our general use of the term "rules and guidelines" in this preamble will refer to both the identity theft red flags rules and guidelines and the card issuer rules.

15 *See* 15 U.S.C. 1681m(e)(1).

include new entities that were not already previously covered by the Agencies' rules.[16] The proposed rules and guidelines do contain examples and minor language changes designed to help guide entities under the Commissions' jurisdiction in complying with the rules. The Commissions anticipate that the proposed rules, if adopted, may help some entities discern whether and how the identity theft rules and guidelines apply to their circumstances.

II. EXPLANATION OF THE PROPOSED RULES AND GUIDELINES

A. Proposed 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 prescribe rules requiring such institutions and creditors to establish reasonable policies and procedures for the implementation of those guidelines.[17] The Commissions have sought to propose identity theft red flags rules and guidelines that are substantially similar to the Agencies' final identity theft red flags rules and guidelines, and that would provide flexibility and guidance to the entities subject to the Commissions' jurisdiction. To that end, the proposed rules discussed below would specify: (1) which financial institutions and creditors would be required to develop and implement a written identity theft prevention program ("Program"); (2) the objectives of the Program; (3) the elements that the Program would be required to contain; and (4) the steps financial institutions and creditors would need to take to administer the Program.

---

16 The CFTC notes that the Dodd-Frank Act creates two new entities that must comply with these proposed rules and guidelines: swap dealers and major swap participants. The CFTC anticipates that to the extent that these new entities currently maintain or offer covered accounts (as discussed below), they also may be in compliance with the Agencies' final rules.

17 15 U.S.C. 1681m(e)(1)(A) and (B). Key terms such as financial institution and creditor are defined in the proposed rules and discussed later in this Section.

1. *Which Financial Institutions and Creditors Would Be Required to Have a Program*

The "scope" subsections of the proposed rules generally set forth the types of entities that would be subject to the Commissions' identity theft red flags rules and guidelines.[18] Under these proposed subsections, the rules would apply to entities over which the Commissions have recently been granted enforcement authority under the FCRA.[19] The Commissions' proposed scope provisions are similar to the scope provisions of the rules adopted by the Agencies.[20]

The CFTC has tailored its proposed "scope" subsection, as well as the definitions of "financial institution" and "creditor," to describe the entities to which its proposed identity theft red flags rules and guidelines would apply.[21] The CFTC's proposed rule states that it would apply to futures commission merchants ("FCMs"), retail foreign exchange dealers, commodity

---

18 Proposed § 162.30(a) (CFTC); § 248.201(a) (SEC).

19 Section 1088(a)(10)(A) of the Dodd-Frank Act amended section 621(b) of the FCRA to add the Commissions to the list of federal agencies responsible for enforcement of the FCRA. As amended, section 621(b) of the FCRA specifically provides that enforcement of the requirements imposed under the FCRA "with respect to consumer reporting agencies, persons who use consumer reports from such agencies, persons who furnish information to such agencies, and users of [certain information] shall be enforced under ... the Commodity Exchange Act, with respect to a person subject to the jurisdiction of the [CFTC]; [and under] the Federal securities laws, and any other laws that are subject to the jurisdiction of the [SEC], with respect to a person that is subject to the jurisdiction of the [SEC] ...." 15 U.S.C. 1681s(b)(1)(F) – (G). *See also* 15 U.S.C. 1681a(f) (defining "consumer reporting agency").

20 *See, e.g.,* 12 CFR 717.90 (stating that the National Credit Union Administration red flags rule "applies to a financial institution or creditor that is a federal credit union"). The Commissions do not have general regulatory jurisdiction over banks, savings and loan associations, or credit unions that hold a transaction account, although the Commissions may have supervisory authority over specific activities of those persons. For example, the CFTC may have jurisdiction over those persons to the extent that they engage in the trading of, or the provision of advice related to, futures or swaps. Similarly, the SEC may have jurisdiction over these persons to the extent that they engage in the trading of, or the provision of advice related to, securities or security-based swaps.

21 Proposed § 162.30(a).

trading advisors ("CTAs"), commodity pool operators ("CPOs"), introducing brokers ("IBs"), swap dealers, and major swap participants.[22]

The SEC's proposed "scope" subsection provides that the proposed rules and guidelines would 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, 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
- an investment adviser that is registered or required to be registered under the Investment Advisers Act of 1940.[23]

The entities listed in the proposed scope section are the entities regulated by the SEC that are most likely to be "financial institutions" or "creditors," *i.e.*, registered brokers or dealers ("broker-dealers"), investment companies and investment advisers.[24] The proposed scope

---

22 The CFTC has determined that the proposed identity theft red flags rules and guidelines would apply to these entities because of the increased likelihood that these entities open or maintain covered accounts, or pose a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft. This approach is consistent with the scope of part 162. *See* 76 FR at 43884.

23 Proposed § 248.201(a).

24 The SEC's proposed rules would define the scope of the proposed identity theft red flags rules and guidelines, proposed § 248.201(a), differently than Regulation S-AM, the affiliate marketing rule the SEC adopted under FCRA, defines its scope. *See* 17 CFR 248.101(b) (providing that Regulation S-AM applies to any brokers or dealers (other than notice-registered brokers or dealers), any investment companies, and any investment advisers or transfer agents registered with the Commission). Section 214(b) of the FACT Act, pursuant to which the SEC adopted Regulation S-AM, did not specify the types of entities that would be subject to the SEC's rules, and did not state that the affiliate marketing rules should apply to all persons over which the SEC has jurisdiction. By contrast, the Dodd-Frank Act specifies that the SEC's identity theft red flags

section also would include other entities that are registered or are required to register under the Exchange Act. The section would not specifically identify those entities, such as nationally recognized statistical ratings organizations, self-regulatory organizations, and municipal advisors and municipal securities dealers, because, as discussed below, they are unlikely to qualify as "financial institutions" or "creditors" under the FCRA.[25] The proposed scope section also would not include entities that are not themselves registered with the Commission,[26] even if they register securities under the Securities Act of 1933 or the Exchange Act, or report information under the Investment Advisers Act of 1940.[27]

- The Commissions solicit comment on the "scope" section of the proposed identity theft red flags rules.
- Should the SEC's proposed scope section specifically list all of the entities that would be covered by the rule if they were to qualify as financial institutions or

---

rules and guidelines should apply to a "person that is subject to the jurisdiction" of the SEC. *See* Dodd-Frank Act section 1088(a)(8), (10).

The scope of the SEC's proposed rules also would differ from that of Regulation S-P, 17 CFR part 248, subpart A, the privacy rule the SEC adopted in 2000 pursuant to the Gramm-Leach-Bliley Act. Pub. L. 106-102 (1999). Regulation S-P was adopted under Title V of that Act, which, unlike the FCRA, limited the SEC's regulatory authority to (i) brokers and dealers, (ii) investment companies, and (iii) investment advisers registered under the Investment Advisers Act of 1940. *See* 15 U.S.C. 6805(a)(3)-(5).

25 Although the Commission preliminarily believes that municipal advisors and municipal securities dealers are unlikely to qualify as "financial institutions" because they are unlikely to maintain transaction accounts for consumers, we welcome comment on this point specifically, as well as on the general issue of whether the list of entities in the proposed scope section should include any other entities.

26 The Dodd-Frank Act defines a "person regulated by the [SEC]," for other purposes of that Act, as certain entities that are registered or required to be registered with the SEC, and certain employees, agents and contractors of those entities. *See* section 1002(21) of the Dodd-Frank Act.

27 *See* Exemptions for Advisers to Venture Capital Funds, Private Fund Advisers With Less Than $150 Million in Assets Under Management, and Foreign Private Advisers, Investment Advisers Act Release No. 3222 (June 22, 2011) [76 FR 39646 (July 6, 2011)] (adopting rules related to investment advisers exempt from registration with the SEC, including "exempt reporting advisers").

creditors under the FCRA? Are the entities specifically listed in the proposed rule the registered entities that are most likely to be financial institutions or creditors under the FCRA? Should the SEC exclude any entities that are listed? Should it include any other entities that are not listed? Should the SEC include entities that register securities with the SEC or that report certain information to the SEC even if the entities themselves do not register with the SEC?

i. *Definition of Financial Institution*

As discussed above, the Commissions' proposed red flags rules and guidelines would apply to "financial institutions" and "creditors." The Commissions are proposing to define the term "financial institution" by reference to the definition of the term in section 603(t) of the FCRA.[28] That section defines a 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."[29] Section 19(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 of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third parties or others."[30]

---

28 15 U.S.C. 1681a(t). *See* proposed § 162.30(b)(7) (CFTC); proposed § 248.201(b)(7) (SEC). The Agencies also defined "financial institution," in their identity theft red flags rules and guidelines, by reference to the FCRA. *See, e.g.,* 16 CFR 681.1(b)(7) (FTC) ("Financial institution has the same meaning as in 15 U.S.C. 1681a(t).").

29 15 U.S.C. 1681a(t).

30 12 U.S.C. 461(b)(1)(C). Section 19(b) further states that a transaction account "includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts."

Accordingly, the Commissions are proposing to define "financial institution" as having the same meaning as in the FCRA. The CFTC's proposed definition, however, also specifies that the term "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 customer."[31]

The SEC is not proposing to mention specific entities in its definition of "financial institution" because the SEC's proposed scope section lists specific entities subject to the SEC's rule.[32] The SEC notes that entities under its jurisdiction that may be financial institutions because they hold customers' transaction accounts would likely include broker-dealers that offer custodial accounts and investment companies that enable investors to make wire transfers to other parties or that offer check-writing privileges. The SEC recognizes that most registered investment advisers are unlikely to hold transaction accounts and thus would not qualify as financial institutions. The proposed definition nonetheless does not exclude investment advisers or any other entities regulated by the SEC because they may hold transaction accounts or otherwise meet the definition of "financial institution."

- The Commissions solicit comment on their proposed definitions of financial institution. Should the Commissions provide further guidance on the types of accounts that an entity might hold that would qualify the entity as a financial institution? Should the Commissions tailor the definition in any way to reflect the characteristics of the entities that would be subject to the rule? If so, how? Would

---

31 *See* proposed § 162.30(b)(7).

32 *See* proposed § 248.201(a).

defining "financial institution" instead in a way that differs from the Agencies' definition compromise the substantial similarity of the red flags rules?

- What type of entities regulated by the Commissions would most likely qualify as financial institutions under the proposed definition?
- Should the SEC's rule omit investment advisers or any other SEC-registered entity from the list of entities covered by the proposed rule?

ii. *Definition of Creditor*

The Commissions are proposing to define "creditor" to reflect a recent statutory definition of the term. In December 2010, President Obama signed into law the Red Flag Program Clarification Act of 2010 ("Clarification Act"), which amended the definition of "creditor" in the FCRA for purposes of identity theft red flag rules and guidelines.[33] The Commissions' proposed definition of "creditor" would refer to the definition in the FCRA as amended by the Clarification Act.[34]

The FCRA now defines a "creditor," for purposes of the red flags rules and guidelines, as a creditor as defined in the Equal Credit Opportunity Act[35] ("ECOA") (*i.e.*, a person that regularly extends, renews or continues credit,[36] or makes those arrangements) that "regularly and

---

33 Red Flag Program Clarification Act of 2010, Pub. L. 111-319 (2010) (inserting new section 4 at the end of section 615(e) of the FCRA), *codified at* 15 U.S.C. 1681m(e)(4).

34 *See* proposed § 162.30(b)(5) (CFTC); proposed § 248.201(b)(5) (SEC). The Commissions understand that the Agencies are likely to amend their red flags rules and guidelines to reflect the new definition of "creditor" in the FCRA enacted by the Red Flag Program Clarification Act.

35 Section 702(e) of the ECOA defines "creditor" to mean "any person who regularly extends, renews, 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. 1691a(e).

36 The Commissions are proposing to define "credit" by reference to its definition in the FCRA. *See* proposed § 162.30(b)(4) (CFTC); proposed § 248.201(b)(4) (SEC). That definition refers to the definition of credit in the ECOA, which means "the right granted by a creditor to a debtor to defer

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."[37] 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 ...."[38] 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 does indicate 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 and guidelines.[39]

As discussed above, the Commissions propose to define "creditor" by reference to its definition in section 615(e)(4) of the FCRA as added by the Clarification Act.[40] The CFTC's proposed definition also would include certain entities (such as FCMs and CTAs) that regularly

---

payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor." The Agencies defined "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. 1681a(r)(5), which defines "credit" as having the same meaning as in section 702 of the ECOA).

37 15 U.S.C. 1681m(e)(4)(A)(iii). 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 consumer reporting agencies ... in connection with a credit transaction ...." 15 U.S.C. 1681m(e)(4)(A)(i) - (ii).

38 Section 615(e)(4)(B) of the FCRA, 15 U.S.C. 1681m(e)(4)(B). The definition of "creditor" also authorizes the Agencies and the Commissions to include other entities in the definition of "creditor" if those entities are determined to offer or maintain accounts that are subject to a reasonably foreseeable risk of identity theft. 15 U.S.C. 1681m(e)(4)(C). The Commissions are not at this time proposing to include other types of entities in the definition of "creditor" that are not included in the statutory definition.

39 *See* 156 Cong. Rec. S8288-9 (daily ed. Nov. 30, 2010) (statements of Senators Thune and Dodd).

40 *See* proposed § 162.30(b)(5); proposed § 248.201(b)(5).

extend, renew or continue credit or make those credit arrangements.[41] The SEC's proposed definition also would include "lenders such as brokers or dealers offering margin accounts, securities lending services, and short selling services."[42] These entities are likely to qualify as "creditors" under the proposed definition because the funds that are advanced in these accounts do not appear to be for "expenses incidental to a service provided." The proposed definition of "creditor" would not include, however, CTAs or investment advisers because they bill in arrears, *i.e.,* on a deferred basis, if they do not "advance" funds to investors and clients.[43]

- The Commissions request comment on their proposed definitions of the terms credit and creditor. Should the proposed terms be tailored to take into account the particular characteristics of the entities regulated by the Commissions? If so, how? Should the Commissions provide further guidance, in the rule text or elsewhere, regarding the types of activities that might qualify an entity as a creditor? Should the Commissions provide guidance regarding the circumstances in which expenses, paid for by advanced funds, are "incidental" to services provided?
- Do commenters agree that broker-dealers that offer margin accounts, securities lending services, or short-selling services are likely to qualify as "creditors" under the proposed definition? Are there other activities that would likely cause SEC-registered entities to qualify as "creditors"?

---

41 *See* proposed § 162.30(b)(5).

42 *See* proposed § 248.201(b)(5).

43 Investment advisers that bill for their services on a quarterly or other deferred basis might have qualified as "creditors" if the term were defined as under section 702 of the Equal Credit Opportunity Act, but they would not qualify as creditors under the definition the Commissions are proposing because they are not "advanc[ing] funds."

- Are there any other entities under the CFTC's or SEC's jurisdiction that maintain accounts that pose a reasonably foreseeable risk of identity theft and that the Commissions should include as "creditors" under the definition?[44]

iii. *Definition of Covered Account and Other Terms*

Under the proposed rules, entities that adopt red flags Programs would focus their attention on "covered accounts" for indicia of possible identity theft. The Commissions propose to define a "covered account" as: (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; and (ii) any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers[45] or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.[46] The CFTC's proposed definition includes a margin account as an example of a covered account.[47] The SEC's proposed definition includes a brokerage account with a broker-dealer or an account maintained by a

---

44 *See* 15 U.S.C. 1681m(e)(4)(C).

45 Proposed § 162.30(b)(6) (CFTC) and proposed § 248.201(b)(6) (SEC) would define a "customer" to mean a person who has a covered account with a financial institution or creditor. The Commissions propose this definition for two reasons. First, this definition is the same as the definition of "customer" in the Agencies' final rules and guidelines. Second, because the definition uses the term "person," it would cover various 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, a financial institution or creditor would be required to determine which type of accounts its Program will cover, because the proposed identity theft red flags rules and guidelines are risk-based.

46 Proposed § 162.30(b)(3) (CFTC); proposed § 248.201(b)(3) (SEC).

47 *See* proposed § 162.30(b)(3)(i).

mutual fund (or its agent) that permits wire transfers or other payments to third parties as examples of such an account.[48]

The Commissions are proposing to define "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."[49] The CFTC's proposed definition would specifically include an extension of credit, such as the purchase of property or services involving a deferred payment.[50] The SEC's proposed definition would specifically include "a brokerage account, a 'mutual fund' account (*i.e.*, an account with an open-end investment company, which may be maintained by a transfer agent or other service provider), and an investment advisory account."[51] Both the CFTC's and SEC's proposed definitions would differ from the definitions in the Agencies' final rules and guidelines by not including a "deposit account." Deposit accounts typically are offered by banks in connection with their banking activities, and not by the entities regulated by the Commissions.[52]

The proposed identity theft red flags rules and guidelines would define several other terms as the Agencies defined them in their final rules and guidelines, where appropriate, to

---

48 *See* proposed § 248.201(b)(3)(i).

49 Proposed § 162.30(b)(1) (CFTC) and proposed § 248.201(b)(1) (SEC).

50 Proposed § 162.30(b)(1).

51 Proposed § 248.201(b)(1).

52 *See, e.g.,* Uniform Commercial Code § 9-102(a)(29) ("'Deposit account' means a demand, time, savings, passbook, or similar account maintained with a bank.").

avoid needless conflicts among regulations.[53] In addition, terms that are not defined in Regulation S-ID would have the same meaning as in the FCRA.[54]

- The Commissions request comment on the proposed definition of "covered account." Should the Commissions include the proposed examples of covered accounts? Should the definition include additional examples of accounts that may be covered accounts? If so, what other types of examples should be included?
- What other types of accounts that are offered or maintained by financial institutions or creditors subject to the Commissions' enforcement authority may pose a reasonably foreseeable risk of identity theft? Should the Commissions explicitly identify them and include them as examples in the proposed rule?
- Are deposit accounts offered by any of the entities regulated by the Commissions?
- The Commissions request comment on other terms defined in the proposed rules and guidelines.

iv. *Determination of Whether a Covered Account is Offered or Maintained*

Under the proposed rules, each financial institution or creditor would be required to periodically determine whether it offers or maintains covered accounts.[55] As a part of this

---

53 *See, e.g.,* proposed § 162.30(b)(10) (CFTC); proposed § 248.201(b)(10) (SEC) (definition of "Red Flag").

54 *See* proposed § 248.201(b)(12)(vi) (SEC). The Agencies defined "identity theft" in their identity theft red flags rules and guidelines by referring to a definition previously adopted by the FTC. *See, e.g.,* 12 CFR 334.90(b)(8) (FDIC). The FTC defined "identity theft" as "a fraud committed or attempted using the identifying information of another person without authority." *See* 16 CFR 603.2(a) The FTC also has defined "identifying information," a term used in its definition of "identity theft." *See* 16 CFR 603.2(b). The Commissions are proposing to define the terms "identifying information" and "identity theft" by including the same definition of the terms as they appear in 16 CFR 603.2. *See* proposed § 162.30(b)(8) and (9) (CFTC); proposed § 248.201(b)(8) and (9) (SEC).

periodic determination, a financial institution or creditor would be required to 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.[56] Under the proposed rules, 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 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 would maintain records concerning their periodic determinations.[57]

The Commissions acknowledge that some financial institutions or creditors regulated by the Commissions may engage only 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 it does not need to develop and implement a Program,[58] or that

---

55 Proposed § 162.30(c) (CFTC) and proposed § 248.201(c) (SEC). As discussed above, the proposed rules would define a "covered account" as (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. Proposed § 162.30(b)(3) (CFTC); proposed § 248.201(b)(3) (SEC).

56 Proposed § 162.30(c) (CFTC) and proposed § 248.201(c) (SEC).

57 *See, e.g.,* FREQUENTLY ASKED QUESTIONS: IDENTITY THEFT RED FLAGS AND ADDRESS DISCREPANCIES at I.1, *available at* http://www.ftc.gov/os/2009/06/090611redflagsfaq.pdf.

58 For example, an FCM that would otherwise be subject to the proposed identity theft red flags rules and guidelines and that handles accounts only for large, institutional investors might make a risk-based determination that because it is subject to a low risk of identity theft, it does not need to develop and implement a Program. Similarly, a money market fund that would otherwise be

it may develop and implement a Program that applies only to a limited range of its activities, such as certain accounts or types of accounts.[59] Under the proposed rules, a financial institution or creditor that initially determines that it does not need to have a Program would be required to periodically reassess whether it must develop and implement a Program in light of changes in the accounts that it offers or maintains and the various other factors set forth in proposed § 162.30(c) (CFTC) and proposed § 248.201(c) (SEC).

- The Commissions request comment regarding the proposed requirement to periodically determine whether a financial institution or creditor offers or maintains covered accounts. Do the proposed rules provide adequate guidance for making the periodic determinations? Should the rules specifically require the documentation of such determinations?

2. *The Objectives of the Program*

The proposed rules would provide that each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.[60] These proposed provisions also would require that each Program be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. Thus, the proposed rules are designed to be scalable, by permitting Programs that take into account the operations of smaller institutions.

---

subject to the proposed red flags rules but that permits investments only by other institutions and separately verifies and authenticates transaction requests might make such a risk-based determination that it need not develop a Program.

59 Even a Program limited in scale, however, would need to comply with all of the provisions of the proposed rules and guidelines. *See, e.g.,* proposed § 162.30(d) – (f) (CFTC) and proposed § 248.201(d) – (f) (SEC) (Program requirements).

60 *See* proposed § 162.30(d)(1) (CFTC) and proposed § 248.201(d)(1) (SEC).

- The Commissions request comment on the proposed objectives of the Program.

3. *The Elements of the Program*

The proposed rules set out the four elements that financial institutions and creditors would be required to include in their Programs.[61] These elements are identical to the elements required under the Agencies' final identity theft red flag rules.[62]

First, the proposed rule would require financial institutions and creditors to develop Programs that include reasonable policies and procedures to identify relevant red flags[63] for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those red flags into its Program.[64] Rather than singling out specific red flags as mandatory or requiring specific policies and procedures to identify possible red flags, this first element would provide 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 proposed guidelines, which are appended to the proposed rules.[65] Given the changing nature of identity theft, the Commissions believe that this element would allow

---

61 *See* proposed § 162.30(d)(2) (CFTC) and proposed § 248.201(d)(2) (SEC).

62 *See* 2007 Adopting Release, *supra* note 10, at 63726-63730.

63 Proposed § 162.30(b)(10) (CFTC) and proposed § 248.201(b)(10) (SEC) define "red flags" to mean a pattern, practice, or specific activity that indicates the possible existence of identity theft.

64 *See* proposed § 162.30(d)(2)(i) (CFTC) and proposed § 248.201(d)(2)(i) (SEC). The board of directors, appropriate committee thereof, or designated 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. However, the board (or designated employee) must conduct an independent review to ensure that the Program is suitable and complies with the requirements of the red flags rules and guidelines. *See* 2007 Adopting Release, *supra* note 10.

65 The factors and examples are discussed below in Section II.B.2.

financial institutions or creditors to respond and adapt to new forms of identity theft and the attendant risks as they arise.

Second, the proposed rule would require financial institutions and creditors to have reasonable policies and procedures to detect red flags that have been incorporated into the Program of the financial institution or creditor.[66] This element would not provide a specific method of detection. Instead, section III of the proposed guidelines provides examples of various means to detect red flags.[67]

Third, the proposed rule would require financial institutions and creditors to have reasonable policies and procedures to respond appropriately to any red flags that are detected.[68] This element would incorporate the requirement that a financial institution or creditor assess whether the red flags 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 proposed guidelines sets out a list of aggravating factors and examples that a financial institution or creditor should consider in determining the appropriate response.[69]

Finally, the proposed rule would require financial institutions and creditors to have reasonable policies and procedures to ensure that 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.[70] As discussed above, financial institutions and creditors would be required to determine which red

---

66 *See* proposed § 162.30(d)(2)(ii) (CFTC) and proposed § 248.201(d)(2)(ii) (SEC).

67 These examples are discussed below in Section II.B.3.

68 *See* proposed § 162.30(d)(2)(iii) (CFTC) and proposed § 248.201(d)(2)(iii) (SEC).

69 The aggravating factors and examples are discussed below in Section II.B.4.

70 *See* proposed § 162.30(d)(2)(iv) (CFTC) and proposed § 248.201(d)(2)(iv) (SEC).

flags are relevant to their businesses and the covered accounts they manage. The Commissions are proposing a periodic update, rather than immediate or continuous updates, to be parallel with the final identity theft red flags rules of the Agencies and to avoid unnecessary regulatory burdens. Section V of the proposed guidelines provides a set of factors that should cause a financial institution or creditor to update its Program.[71]

- The Commissions request comment on whether the proposed four elements of the Program would provide effective protection against identity theft and whether any additional elements should be included.
- The Commissions anticipate that a financial institution or creditor that adopts a Program could integrate the policies and procedures with other policies and procedures it has adopted pursuant to other legal requirements, such as compliance[72] and safeguards rules.[73] Should the Commissions provide guidance on how financial institutions or creditors could integrate identity theft policies and procedures with other policies and procedures?

4. *Administration of the Program*

The Commissions are proposing to provide direction to financial institutions and creditors regarding the administration of Programs to enhance the effectiveness of those Programs. Accordingly, the proposed rule would prescribe the steps that financial institutions and creditors would have to take to administer a Program.[74] These sections would provide that

---

71 These factors are discussed below in Section II.B.5.

72 *See* rule 38a-1 under the Investment Company Act, 17 CFR 270.38a-1; rule 206(4)-7 under the Investment Advisers Act, 17 CFR 275.206(4)-7.

73 Regulation S-P, 17 CFR 248.30 (applicable to broker-dealers, investment companies, and investment advisers).

74 *See* proposed § 162.30(e) (CFTC) and proposed § 248.201(e) (SEC).

each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and meet four additional requirements.

First, the proposed rules would require that a financial institution or creditor obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors.[75] This proposed requirement highlights the responsibility of the board of directors and senior management in approving a Program. This requirement would not mandate that a board be responsible for the day-to-day operations of the Program. The proposed rules provide that the board or appropriate committee must approve only the initial written Program. This provision is designed to enable a financial institution or creditor to update its Program in a timely manner. After the initial approval, at the discretion of the entity, the board, a committee, or senior management may update the Program.

Second, the proposed rules would provide that financial institutions and creditors must 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.[76] The proposed rules would provide discretion to a financial institution or creditor to determine who would be responsible for the oversight, development, implementation, and administration of the Program in allowing the board of directors to delegate these functions. The Commissions appreciate that boards of directors have many responsibilities and that it

---

75 *See* proposed § 162.30(e)(1) (CFTC) and proposed § 248.201(e)(1) (SEC). Proposed § 162.30(b)(2) (CFTC) and proposed § 248.201(b)(2) (SEC) define the term "board of directors" to include: (i) in the case of a branch or agency of a non-U.S-based financial institution or creditor, the managing official in charge 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 senior management employee.

76 *See* proposed § 162.30(e)(2) (CFTC) and proposed § 248.201(e)(2) (SEC). Section VI of the proposed guidelines elaborates on the proposed provision.

generally is not feasible for a board to involve itself in these functions on a daily basis. A designated management official who is responsible for the oversight of a broker-dealer's, investment company's or investment adviser's Program may also be the entity's chief compliance officer.[77]

Third, the proposed rules would provide that financial institutions and creditors must train staff, as necessary, to effectively implement their Programs.[78] The Commissions believe that proper training would enable relevant staff to address the risk of identity theft. For example, staff would be trained to detect red flags with regard to new and existing accounts, such as discrepancies in identification presented by a person opening an account. Staff also would need to be trained to mitigate identity theft, for example, by recognizing when an account should not be opened.

Finally, the proposed rules would provide that financial institutions and creditors must exercise appropriate and effective oversight of service provider arrangements.[79] The Commissions believe that it is important that the proposed rules address service provider arrangements so that financial institutions and creditors would remain legally responsible for compliance with the proposed rules, irrespective of whether such institutions and creditors outsource their identity theft red flags detection, prevention, and mitigation operations to a third-party service provider.[80] The proposed rules do not prescribe a specific manner in which

---

77 *See, e.g.,* rule 38a-1(a)(4) under the Investment Company Act (description of chief compliance officer), 17 CFR 270.38a-1(a)(4); rule 206(4)-7(c) under the Investment Advisers Act, 17 CFR 275.206(4)-7 (same).

78 *See* proposed § 162.30(e)(3) (CFTC) and proposed § 248.201(e)(3) (SEC).

79 *See* proposed § 162.30(e)(4) (CFTC) and proposed § 248.201(e)(4) (SEC). Proposed § 162.30(b)(11) (CFTC) and proposed § 248.201(b)(11) (SEC) would define the term "service provider" to mean a person that provides a service directly to the financial institution or creditor.

80 For example, a financial institution or creditor that uses a service provider to open accounts on its

appropriate and effective oversight of service provider arrangements must occur. Instead, the proposed requirement would provide flexibility to financial institutions and creditors in maintaining their service provider arrangements, while making clear that such institutions and creditors would still be required to fulfill their legal compliance obligations.[81] Section VI(c) of the proposed guidelines specifies what a financial institution or creditor could do so 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.[82]

- The Commissions solicit comment on whether the proposed four steps to administer the Program are appropriate and whether any additional or alternate steps should be included.

B. Proposed 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."[83] Accordingly, the Commissions are jointly proposing guidelines in an appendix to the proposed rules that are intended to assist financial institutions and creditors in the formulation and maintenance of a

---

behalf, could reserve for itself the responsibility to verify the identity of a person opening a new account, may direct the service provider to do so, or may use another service provider to verify identity. Ultimately, however, the financial institution or creditor would remain responsible for ensuring that the activity is being conducted in compliance with a Program that meets the requirements of the proposed identity theft red flags rules and guidelines.

81 These legal compliance obligations would include the maintenance of records in connection with any service provider arrangements.

82 Section VI(c) of the proposed guidelines is discussed below in Section II.B.6.

83 15 U.S.C. 1681m(e)(1)(A).

Program that would satisfy the requirements of those proposed rules. These guidelines are substantially similar to the guidelines adopted by the Agencies. The changes we are proposing to make to the Agencies' guidelines are designed to tailor the guidelines to the circumstances of the entities within the Commissions' regulatory jurisdiction, such as by modifying the examples provided by the guidelines. We believe this approach would meet the Commissions' obligation under section 615(e)(1)(A) of the FCRA to jointly establish and maintain guidelines for financial institutions and creditors.

The proposed rules would explain the relationship of the proposed rules to the proposed guidelines.[84] In particular, they would require each financial institution or creditor that is required to implement a Program to consider the guidelines. The proposed guidelines set forth policies and procedures that financial institutions and creditors would be required to consider and use, if appropriate. Although a financial institution or creditor could determine that a particular guideline is not appropriate for its circumstances, its Program would need to contain reasonable policies and procedures to fulfill the requirements of the proposed rules. As discussed above, the proposed guidelines are substantially similar to the final guidelines issued by the Agencies. In the Commissions' view, the proposed guidelines would provide financial institutions and creditors with flexibility to determine "how best to develop and implement the required policies and procedures."[85]

The proposed guidelines are organized into seven sections and a supplement. Each section in the proposed guidelines corresponds with the provisions in the proposed rules.

---

84 *See* proposed § 162.30(f) (CFTC) and proposed § 248.201(f) (SEC).

85 *See* H.R. Rep. No. 108-263 at 43, Sept. 4, 2003 (accompanying H.R. 2622); S. Rep. No. 108-166 at 13, Oct. 17, 2003 (accompanying S. 1753).

- The Commissions request comment on all sections, including Supplement A, of the proposed guidelines described below.

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

As noted above, proposed § 162.30(d)(1) (CFTC) and proposed § 248.201(d)(1) (SEC) would require each financial institution or creditor that offers or maintains one or more covered accounts to develop and maintain a program that is designed to detect, prevent, and mitigate identity theft. Section I of the proposed guidelines corresponds with these provisions. Section I of the proposed guidelines makes clear that a covered entity 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. The Commissions believe that this section of the proposed guidelines would allow financial institutions and creditors to minimize cost and time burdens associated with the development and implementation of new policies, procedures, and arrangements by leveraging existing policies, procedures, and arrangements and avoiding unnecessary duplication.

- The Commissions request comment on this section of the proposed guidelines.

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

As recently amended by the Dodd-Frank Act, section 615(e)(2)(A) of the FCRA provides that, in developing identity theft red flags guidelines as required by the FCRA, the Commissions must identify patterns, practices, and specific forms of activity that indicate the possible

existence of identity theft. Section II of the proposed guidelines would identify those patterns, practices and forms of activity. Section II(a) of the proposed guidelines sets out several risk factors that a financial institution or creditor would be required to consider 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. Thus, for example, red flags relevant to margin accounts may differ from those relevant to advisory accounts, and those applicable to consumer accounts may differ from those applicable to business accounts. Red flags relevant to accounts that may be opened or accessed remotely may differ from those relevant to accounts that require face-to-face contact. In addition, under the proposed guidelines, a financial institution or creditor should consider identifying as relevant those red flags that directly relate to its previous experiences with identity theft.

Section II(b) of the proposed guidelines sets out examples of sources from which financial institutions and creditors should derive relevant red flags. This proposed section provides that a financial institution or creditor should incorporate relevant red flags from such sources as: (1) incidents of identity theft that the financial institution or creditor has experienced; (2) methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and (3) applicable regulatory guidance (*i.e.,* guidance received from regulatory authorities). As discussed above in Section II.B, this proposed section would not require financial institutions and creditors to incorporate relevant red flags strictly from these three sources. Instead, the section would require that financial institutions and creditors consider them when developing a Program.

As noted above, the proposed rules would not identify specific red flags that financial institutions or creditors must include in their Programs.[86] Instead, under the proposed guidelines, a Program would be required to identify and incorporate relevant red flags that are appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities. Section II(c) of the proposed guidelines identifies five categories of red flags that financial institutions and creditors must consider including in their Programs:

- 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.

In Supplement A to the proposed guidelines, the Commissions include a non-comprehensive list of examples of red flags from each of these categories that a financial institution or creditor may experience.[87]

---

86 *See* proposed § 162.30(d) (CFTC) and § 248.201(d) (SEC).

87 These examples are discussed below in Section II.B.8.

- The Commissions request comment on this section of the proposed guidelines. Are there specific, additional red flags associated with the types of institutions subject to the Commissions' jurisdiction that the Commissions should identify?
- Would the five categories of red flags discussed in the proposed guidelines provide flexible and adequate guidance for financial institutions and creditors that they can use to develop a Program?

3. *Section III of the Proposed Guidelines — Detecting Red Flags*

As noted above, the proposed rules would provide that a financial institution or creditor must have reasonable policies and procedures to detect red flags in its Program.[88] Section III of the proposed guidelines would provide examples of policies and procedures that a financial institution or creditor must consider including in its Program for the purpose of detecting red flags. These would include (1) in the case of the opening of a covered account, obtaining identifying information about, and verifying the identity of, the person opening the account, and (2) in the case of existing covered accounts, authenticating customer identities, monitoring transactions, and verifying the validity of change of address requests. Entities that are currently subject to the Agencies' final identity theft red flag rules and guidelines,[89] the federal customer identification program ("CIP") rules[90] or other Bank Secrecy Act rules,[91] the Federal Financial

---

88 *See* proposed § 162.30(d)(2)(ii) (CFTC) and proposed § 248.201(d)(2)(ii) (SEC).

89 *See* 2007 Adopting Release, *supra* note 10.

90 *See, e.g.,* 31 CFR 1023.220 (broker-dealers), 1024.220 (mutual funds), and 1026.220 (futures commission merchants and introducing brokers). The CIP regulations implement section 326 of the USA PATRIOT Act, codified at 31 U.S.C. 5318(l).

91 *See, e.g.,* 31 CFR 103.130 (anti-money laundering programs for mutual funds).

Institutions Examination Council's guidance on authentication,[92] or the Federal Information Processing Standards[93] may already be engaged in detecting red flags.

In developing the proposed rules and guidelines, the Commissions sought to minimize the burdens that would be imposed on entities that may be in compliance with existing similar laws. 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. For example, the CIP rules were written to implement section 326[94] of the USA PATRIOT Act,[95] an Act directed towards facilitating the prevention, detection and prosecution of international money laundering and the financing of terrorism. 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. Accordingly, the Commissions would expect that, if the proposed rules are adopted, all financial institutions and creditors would evaluate the adequacy of existing policies and procedures, and develop and implement risk-based policies and procedures that detect red flags in an effective and comprehensive manner.

---

92 *See* "Authentication in an Internet Banking Environment," Oct. 12, 2005, available at: http://www.ffiec.gov/press/pr101205.htm.

93 The Federal Information Processing Standards are issued by the National Institute of Standards and Technology ("NIST") after approval by the Secretary of Commerce pursuant to section 5131 of the Information Technology Management Reform Act of 1996, Pub. L. 104-106, 110 Stat. 702, Feb. 10, 1996, and the Federal Information Security Management Act of 2002, 44 U.S.C. 3541, et seq. NIST manages and publishes the most current Federal Information Processing Standards at: http://csrc.nist.gov/publications/PubsFIPS.html.

94 31 U.S.C. 5318(*l*).

95 Pub. L. 107-56 (2001).

- The Commissions request comment on this section of the proposed guidelines. Should the Commission provide further guidance on the integration of or differentiation between identity theft red flags programs and other existing procedures?

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

As noted above, the proposed rules would require that a Program include reasonable policies and procedures to respond appropriately to red flags that are detected.[96] Section IV of the proposed guidelines states that a Program's policies and procedures should include a list of 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.[97] In determining an appropriate response, under the proposed guidelines, a financial institution or creditor would be required to consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor, or to a fraudulent Internet website.

Section IV of the proposed guidelines also provides several examples of appropriate responses, such as monitoring a covered account for evidence of identity theft, contacting the customer, and changing any passwords, security codes, or other security devices that permit

---

96 *See* proposed § 162.30(d)(2)(iii) (CFTC) and proposed § 248.201(d)(2)(iii) (SEC).

97 A financial institution or creditor, in order to respond appropriately, would have to assess whether the red flags indicate risk of identity theft, and must have a reasonable basis for concluding that a red flag does not demonstrate a risk of identity theft.

access to a covered account.[98] The Commissions are proposing to include the same list of examples presented in the Agencies' final guidelines, because, upon review, the Commissions believe the list is comprehensive, relevant to entities regulated by the Commissions, and designed to enhance consistency of regulations and Programs.

- The Commissions seek comment on this section of the proposed guidelines. Should the Commission revise the guidelines to add, modify, or delete any examples?

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

As discussed above, the proposed rules would require each financial institution or creditor to periodically update its Program (including the relevant red flags) to reflect changes in risks to its customers or to the safety and soundness of the financial institution or creditor from identity theft.[99] Section V of the proposed guidelines would include a list of factors on which a financial institution or creditor could base the updates to its Program: (a) the experiences of the financial institution or creditor with identity theft; (b) changes in methods of identity theft; (c) changes in methods to detect, prevent, and mitigate identity theft; (d) changes in the types of accounts that the financial institution or creditor offers or maintains; and (e) changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

---

98 Other examples of appropriate responses provided in the proposed guidelines are: reopening a covered account with a new account number; not opening a new covered account; closing an existing covered account; not attempting to collect on a covered account or not selling a covered account to a debt collector; notifying law enforcement; and determining that no response is warranted under the particular circumstances. The final proposed example – no response – might be appropriate, for example, when a financial institution or creditor has a reasonable basis for concluding that the red flags do not evidence a risk of identity theft.

99 *See* proposed § 162.30(d)(2)(iv) (CFTC) and proposed § 248.201(d)(2)(iv) (SEC).

- The Commissions request comment on this section of the proposed guidelines. Should the Commissions provide any further guidance regarding the updating of Programs?

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

Section VI of the proposed guidelines would provide additional guidance for financial institutions and creditors to consider in administering their identity theft Programs.[100] These proposed guideline provisions are identical to those prescribed by the Agencies in their final guidelines, which were modeled on sections of the Federal Information Processing Standards.[101]

i. *Oversight of Identity Theft Prevention Program*

Section VI(a) of the proposed guidelines would state that oversight by the board of directors, an appropriate committee of the board, or a designated senior management employee 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 the proposed rules; and (3) 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 proposed 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

---

100 *See* proposed § 162.30(e) (CFTC) and proposed § 248.201(e) (SEC) (administration of Programs).

101 *See supra* note 93 (brief explanation of the Federal Information Processing Standards).

with the proposed rules. In addition, section VI(b) of the proposed guidelines provides that the report should address material matters related to the Program and evaluate several issues, such as: (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; (iii) significant incidents involving identity theft and management's response; and (iv) recommendations for material changes to the Program.

iii. *Oversight of Service Provider Arrangements*

Section VI(c) of the proposed guidelines would provide 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. The Commissions believe that these guidelines would 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 proposed identity theft red flags rules.

Section VI(c) of the proposed guidelines would also include, 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 would 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.

- The Commissions request comment on section VI of the proposed guidelines.
- The SEC anticipates that information about compliance with an entity's Program could be included in any periodic reports submitted by the entity's chief compliance officer to its board of directors. The SEC requests comment on whether such reports are an appropriate means for reporting information to the board about the entity's compliance with its identity theft Program.

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

Section VII of the proposed guidelines would identify other applicable legal requirements that financial institutions and creditors should keep in mind when developing, implementing, and administering their Programs. Specifically, section VII of the proposed guidelines identifies section 351 of the USA PATRIOT Act, which sets out the requirements for financial institutions that must file "Suspicious Activity Reports" in accordance with applicable law and regulation.[102] In addition, section VII of the proposed guidelines identifies the following three requirements under the FCRA, which a financial institution or creditor should keep in mind: (1) implementing any requirements under section 605A(h) of the FCRA, 15 U.S.C. 1681c-1(h), regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;[103] (2) implementing any requirements for furnishers of

---

102 31 U.S.C. 5318(g).

103 Section 603(q)(2) of the FCRA defines the terms "fraud alert" and "active duty alert" as "a statement in the file of a consumer that – (A) notifies all prospective users of a consumer report

information to consumer reporting agencies under section 623 of the FCRA, 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 (3) complying with the prohibitions in section 615 of the FCRA, 15 U.S.C. 1681m, regarding the sale, transfer, and placement for collection of certain debts resulting from identity theft.

- The Commissions request comment on this section of the proposed guidelines.

8. *Proposed Supplement A to the Guidelines*

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

- Alerts, notifications, or warnings from a consumer reporting agency;
- Suspicious documents;
- Suspicious personal identifying information;
- Unusual use of, or suspicious activity related to, the covered account; and
- Notice from others regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.[104]

---

relating to the consumer that the consumer may be a victim of fraud, including identity theft, or is an active duty military consumer, as applicable; and (B) is presented in a manner that facilitates a clear and conspicuous view of the statement described in subparagraph (A) by any person requesting such consumer report." 15 U.S.C. 1681a(q)(2).

104 *See supra* Section II.B.2.

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. It is the Commissions' intention that Supplement A to the proposed 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 proposed rules would not require a financial institution or creditor to justify to the Commissions its failure to include in its Program a specific red flag from the list of examples, a financial institution or creditor would have 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.

- The Commissions request comment on Supplement A to the proposed guidelines. Are there any additional examples of red flags that the Supplement should include? For instance, should the Supplement include examples of fraud by electronic mail, such as when a financial institution or creditor receives an urgent request to wire money from a covered account to a remote account from an email address that may have been compromised?[105]

---

105 The Federal Bureau of Investigation ("FBI") and other organizations recently issued alerts that warned of thefts of customer money through emails from compromised customer email accounts. *See* FBI and Internet Crime Complaint Center, FRAUD ALERT INVOLVING E-MAIL INTRUSIONS TO FACILITATE WIRE TRANSFERS OVERSEAS, *available at* *http://www.ic3.gov/media/2012/EmailFraudWireTransferAlert.pdf;* FINRA, Regulatory Notice 12-05, CUSTOMER ACCOUNT PROTECTION, VERIFICATION OF EMAILED INSTRUCTIONS TO TRANSMIT OR WITHDRAW ASSETS FROM CUSTOMER ACCOUNTS, *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p125462.pdf (January, 2012); FINRA Investor Alert, EMAIL HACK ATTACK? BE SURE TO NOTIFY BROKERAGE FIRMS AND OTHER FINANCIAL INSTITUTIONS, *available at* http://www.finra.org/Investors/ProtectYourself/InvestorAlerts/FraudsAndScams/P125460.

C. Proposed Card Issuer Rules

Section 615(e)(1)(C) of the FCRA now provides that the CFTC and SEC must "prescribe regulations applicable to card issuers to ensure that, if a card 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 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 discussed below.[106] Congress singled out this scenario involving card issuers as being a possible indicator of identity theft. Accordingly, the Commissions are proposing the card issuer rules in conjunction with the identity theft red flags rules.

The Commissions are proposing rules that would set out the duties of card issuers regarding changes of address, which would be similar to the final card issuer rules adopted by the Agencies.[107] The proposed rules would provide that the card issuer rules apply only to a person that issues a debit or credit card ("card issuer") and that is subject to the jurisdiction of either Commission.[108]

The CFTC is not aware of any entities subject to its jurisdiction that issue debit or credit cards. The CFTC notes that several of the CFTC regulated-entities that are identified as falling within the scope of the proposed card issuer rules (*e.g.*, FCMs, IBs, CPOs, CTAs, etc.) do not typically engage in the type of activities that are the subject of such rules and guidelines. As a matter of practice, it is highly unlikely that these CFTC regulated-entities would issue debit or

---

106 15 U.S.C. 1681m(e)(1)(C).

107 *See* § 162.32 (CFTC) and § 248.202 (SEC).

108 *See supra* Section II.A.1.

credit cards. In fact, there are statutory provisions, regulations, or other laws that expressly prohibit some of these entities from engaging in many of these activities. For example, the Commodity Exchange Act ("CEA") and the CFTC's regulations expressly prohibit an IB from extending credit in connection with their primary business activities.[109] With respect to FCMs, while the CEA permits an FCM to extend credit to customers in lieu of accepting money, securities, or property for the purposes of collecting margin on a commodity interest, the CFTC's regulations prohibit an FCM from doing so.[110] Lastly, the National Futures Association's ("NFA") rules prohibit its members registered as CPOs from making loans to limited partners using interests in the partnerships as collateral.[111]

- The CFTC requests comment on the extent to which the proposed card issuer rules would affect the business operations of entities that would fall under the CFTC's jurisdiction.

The SEC understands that a number of entities under its jurisdiction issue cards in partnership with affiliated or unaffiliated banks and financial institutions. Generally, these cards

---

109 *See* 7 U.S.C. 1(a)(31) (An IB is defined as any person that "is engaged in soliciting or in accepting orders for the purchase or sale of any commodity for future delivery, security futures product, [...] swap," any foreign exchange transaction, any retail commodity transaction, any authorized commodity option, or any authorized leverage transaction, "and does not accept money securities, or property (or extend credit in lieu thereof) to margin, guarantee, or secure any trades or contracts that result or may result therefrom."); *see also* 17 CFR 1.57(c) (prohibiting IBs from, among other things, extending credit in lieu of accepting money, securities or property to margin, guarantee or secure any trades or contracts of customers) and 17 CFR 1.56(b) (prohibiting IBs from representing that they will guarantee any person against loss with respect to any commodity interest in any account carried by an FCM for or on behalf of any person).

110 *See* 17 CFR 1.56(b) (prohibiting FCMs from representing that they will guarantee any person against loss with respect to any commodity interest in any account carried by an FCM for or on behalf of any person).

111 *See* NFA Rule 2-45, available at *http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=RULE%202-45&Section=4*, which provides that "[n]o Member CPO may permit a commodity pool to use any means to make a direct or indirect loan or advance of pool assets to the CPO or any other affiliated person or entity."

are issued by the partner bank, and not by the entity under the SEC's jurisdiction. For example, a broker-dealer may offer automated teller machine (ATM) access to a customer account through a debit card, but the debit card would generally be issued by a partner bank and not by the broker-dealer itself. The SEC therefore expects that few, if any, entities under its jurisdiction would be subject to the proposed card issuer rules. Nonetheless, the SEC is proposing the card issuer rules below so that any entity under its jurisdiction that does issue cards provides appropriate identity theft protection.

- The SEC requests comment on the extent to which the proposed card holder rules may affect the entities under its jurisdiction. Do any SEC-regulated entities issue cards? What types of arrangements are used to establish the card-issuing partnership between SEC-regulated entities and issuing banks? Would the proposed card issuer rules affect those arrangements?

1. *Definition of "Cardholder" and Other Terms*

Section 615(e)(1)(C) of the FCRA uses the term "cardholder" but does not define the term. The legislative history on this provision indicates that "issuers of credit cards and debit cards who receive a consumer request for an additional or replacement card for an existing account" may assess the validity of the request by notifying "the cardholder."[112] The proposed rules provide that the term "cardholder" means a consumer[113] who has been issued a credit or

---

112 149 Cong. Rec. E2513 (daily ed. Dec. 8, 2003) (statement of Rep. Oxley).

113 A "consumer" means an individual person, as defined in section 603(c) of the FCRA and § 162.2(f) of the CFTC's regulations. *See* 15 U.S.C. 1681a(c) and 76 FR at 43885. As mentioned above, the rules proposed by the CFTC in this release would be a part of part 162 of the CFTC's regulations, and therefore, all definitions in part 162 would apply to these rules. *See* 76 FR at 43884-6. The SEC is proposing to define all terms that are not defined in subpart C (including the term "consumer") to have the same meaning as defined in the FCRA. *See* proposed § 248.202(b)(3).

debit card.[114] Both "credit card" and "debit card" are defined in section 603(r) of the FCRA.[115] "Credit card" is defined by reference to section 103 of the Truth in Lending Act.[116] "Debit card" is defined as any card issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account of a consumer at such financial institution for the purpose of transferring money between accounts or obtaining money, property, labor, or services.[117] The term "clear and conspicuous" is defined in § 162.2(b) of the CFTC's regulations and in the SEC's proposed § 248.202(b)(2) to mean reasonably understandable and designed to call attention to the nature and significance of the information presented in the notice. The proposed definitions of "cardholder" and "clear and conspicuous" are identical to the definitions in the Agencies' final card issuer rules because, upon review, the Commissions believe that the definitions are comprehensive, likely to be relevant to any entities regulated by the Commissions under these proposed rules, and designed to enhance consistency and comparability of regulations and Programs.[118]

- The Commissions' proposed definition of "cardholder" refers to the definition of "credit card" and "debit card" in section 603(r) of the FCRA. Should the proposed definition instead separately define "credit card" and "debit card"?

2. *Address Validation Requirements*

Section 615(e) of the FCRA provides the address validation requirements and methods, and the proposed rules would set out the address validation rules to reflect those requirements

---

114 *See* proposed § 162.32(b) (CFTC) and proposed § 248.202(b) (SEC).

115 15 U.S.C. 1681.

116 15 U.S.C. 1601.

117 15 U.S.C. 1681a(r)(3).

118 *See* 2007 Adopting Release, *supra* note 10, at 63733.

and methods.[119] These sections would require a card issuer to establish and implement reasonable written policies and procedures to assess the validity of a change of address if it (1) receives notification of a change of address for a consumer's debit or credit card account and (2) within a short period of time afterwards (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. Under these circumstances, the proposed rules would prohibit the card issuer from issuing an additional or replacement card until, in accordance with its reasonable policies and procedures, it uses one of two methods to assess the validity of the change of address. Under the first method, the card issuer must notify the cardholder of the request either at the cardholder's former address,[120] or by any other means of communication that the card issuer and the cardholder have previously agreed to use.[121] In addition, the card issuer must provide the cardholder with a reasonable means of promptly reporting incorrect address changes. Under the second method, the card issuer would be required to otherwise assess the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to the proposed rules.[122]

The proposed rules would provide card issuers with an alternative time period in which to assess the validation of a cardholder's address.[123] Specifically, this section provides that the card issuer would be able to satisfy the requirements of proposed § 162.32(c) (CFTC) and proposed § 248.202(c) (SEC) if it validates an address pursuant to the methods in proposed

---

119 *See* proposed § 162.32(c) (CFTC) and proposed § 248.202(c) (SEC).

120 *See* 15 U.S.C. 1681m(e)(1)(C)(i).

121 *See* 15 U.S.C. 1681m(e)(1)(C)(ii).

122 *See* proposed § 162.32(c) (CFTC) and proposed § 248.202(c) (SEC).

123 *See* proposed § 162.32(d) (CFTC) and proposed § 248.202(d) (SEC).

§§ 162.32(c)(1) or (c)(2) (CFTC) and proposed §§ 248.202(c)(1) or (c)(2) (SEC) when it receives an address change notification, before it receives a request for an additional or replacement card. The proposed rules would not require a card issuer that issues an additional or replacement card to validate an address whenever it receives a request for such a card; section 615(e)(1)(C) of the FCRA (and proposed § 162.32(c) (CFTC) and proposed § 248.202(c) (SEC)) would require the validation of an address only when the card issuer also has received a notification of a change in address. The Commissions believe, however, that a card issuer that does not validate an address when it receives an address change notification may find it prudent to validate the address before issuing an additional or replacement card, even when it receives a request for such a card more than 30 days after the notification of address change. Ultimately, the Commissions expect card issuers to exercise diligence commensurate with (*i.e.*, augmented by) their own experiences with identity theft.

- The Commissions request comment on the proposed address validation requirements for card issuers.

3. *Form of Notice*

To highlight the important and urgent nature of notice that a consumer receives from a card issuer, the Commissions are proposing to require that any written or electronic notice that the card issuer provides under this section would be required to be clear and conspicuous and be provided separately from its regular correspondence with the cardholder.[124] This proposed requirement would be consistent with the requirement in the Agencies' final card issuer rules

---

124 *See* proposed § 162.32(e) (CFTC) and proposed § 248.202(e) (SEC). As noted above, "clear and conspicuous" would mean reasonably understandable and designed to call attention to the nature and significance of the information presented in the notice. *See supra* Section II.C.1. *See also* § 162.2(b) (CFTC) and proposed § 248.202(b)(2) (SEC).

because, upon review, the Commissions believe the requirement is comprehensive, relevant to any entities regulated by the Commissions under these proposed rules, and designed to enhance consistency and comparability of regulations and Programs.

- The Commissions request comment on the proposed requirements regarding the form of notice that must be sent to card holders.

D. Proposed Effective and Compliance Dates

The Commissions propose to make the rules and guidelines effective 30 days after the date of publication of final rules in the *Federal Register*. Financial institutions and creditors subject to the Commissions' enforcement authority should already be in compliance with the red flags rules of the FTC or the other Agencies. Newly formed entities under the Commissions' enforcement authority likely comply with the existing rules of the FTC or the other Agencies. The rules and guidelines that the Commissions are proposing today are substantially similar to the existing rules of the Agencies and should not require significant changes to financial institution or creditor policies or operations. As a result, the Commissions do not expect that entities subject to their enforcement authority should have difficulty in complying with the proposed rules and guidelines immediately, and are not proposing a delayed compliance date.

- The Commissions request comment on the proposed effective and compliance dates for the proposed rules and guidelines. Should there be a delayed effective or compliance date? If so, what should the delay be (*e.g.*, 30, 60, or 90 days, or longer)?

III. RELATED MATTERS

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

CFTC:

Section 15(a) of the CEA[125] requires the CFTC to consider the costs and benefits of its actions before promulgating a regulation under the CEA or issuing an order. 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 proposed rules and guidelines are broken down into two categories of requirements. First, the proposed identity theft red flag rules and guidelines found in proposed § 162.30, and second, the proposed card issuer rules found in proposed § 162.32. A Section 15(a) analysis of each category is set out immediately below.

1. Cost Benefit Considerations of Proposed Identity Theft Red Flag Rules and Guidelines.

As noted above, the proposed identity theft red flags rules and guidelines would require financial institutions and creditors that are subject to CFTC's enforcement authority under the FCRA[126] and that offer or maintain covered accounts to develop, implement, and administer a written Program. Each Program must be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. In addition, each Program must be appropriately tailored to the size and complexity of the financial

---

125 7 U.S.C. 19(a)

126 As stated above, section 1088(a)(10) of the Dodd-Frank Act amended section 621(b) of the FCRA to add the Commissions to the list of federal agencies responsible for administrative enforcement of the FCRA. *See* Pub. L. 111-203 (2010).

institution or creditor and the nature and scope of its activities. There are various steps that a financial institution or creditor must take in order to comply with the requirements under the proposed identity theft red flags rules, including training staff, providing annual reports to board of directors, and when applicable, monitoring the use of third-party service providers.

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 and guidelines. To carry out this requirement, the CFTC is proposing § 162.30, which is substantially similar to the identity theft red flags rules and guidelines adopted by the Agencies in 2007.

Proposed § 162.30 would shift oversight of identity theft rules and guidelines of CFTC-regulated entities from the FTC to the CFTC. These entities should already be in compliance with the FTC's existing rules and guidelines, which the FTC began enforcing on December 31, 2010. Because proposed § 162.30 is substantially similar to those existing rules and guidelines, these entities should not bear any new costs in coming into compliance with proposed § 162.30. The new regulation does not contain new requirements, nor does it expand the scope of the rules to include new entities that were not already previously covered by the Agencies' rules. The new regulation does contain examples and minor language changes designed to help guide entities under the CFTC's jurisdiction in complying with the 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 proposed § 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 proposed § 162.30. These hours and costs would be transferred from the Agencies' PRA allotment to the CFTC. No new costs should result from the adoption of proposed § 160.30.

These existing costs related to proposed § 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.[127] 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.[128]

---

127 CFTC staff estimates that the one-time burden of compliance would include 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. CFTC staff estimates that, of the 31 hours incurred, 12 hours would be spent by internal counsel at an hourly rate of $354, 17 hours would be spent by administrative assistants at an hourly rate of $66, and 2 hours would be spent by the board of directors as a whole, at an hourly rate of $4000, for a total cost of $13,370 per entity for entities that need to come into compliance with proposed subpart C to Part 162. This estimate is based on the following calculations: $354 x 12 hours = $4,248; $66 x 17 = $1,122; $4,000 x 2 = $8,000; $4,248 + $1,122 + $8,000 = $13,370.

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 financial institution or creditor. Of these 702 entities, 54 entities would maintain covered accounts. *See infra* note 153 and text following note 153. 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 x 2 = $708; $708 x 702 = $497,016. CFTC staff estimates that 54 entities would bear the remaining specified costs for a total cost of $683,748 (54 x $12,662 = $683,748). *See* SIFMA "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 $1,596,250 (125 x $12,770 = $1,596,250).

128 CFTC staff estimates that the ongoing burden of compliance would 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. CFTC staff estimates that, of the 8 hours incurred, 7 hours would be spent by internal counsel at an

The benefits related to adoption of proposed § 160.30, which already exist in connection with the Agencies' red flags rules and guidelines, 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 determine with precision the dollar value associated with the benefits that will inure to the public from this proposed rules and guidelines, as the quantity or value of identity theft deterred or prevented is not knowable. The Commission, 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 and guidelines 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' rules and guidelines, the CFTC has designed proposed § 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.

---

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 $6,500. This estimate is based on the following calculations rounded to two significant digits : $354 x 7 hours = $2,478; $4,000 x 1 hour = $4,000; $2,478 + $4,000 = $6,478 ≈ $6,500.

As discussed in the PRA analysis, CFTC staff estimates that 3,124 existing CFTC-regulated entities would be financial institutions or creditors, of which 268 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 (or 3,124 entities) would bear this cost for a total cost of $2,200,000 based on the following calculations rounded to two significant digits: $354 x 2 = $708; $708 x 3,124 = $2,211,792 ≈ $2,200,000. CFTC staff estimates that 268 entities would bear the remaining specified ongoing costs for a total cost of $1,500,000 (268 x $5,770 = $1,546,360 ≈ $1,500,000).

Accordingly, as previously discussed, proposed § 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, 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 preventing identity theft, an illegal act that may be costly to them in both time and money.[129] Because, however, these proposed rules and guidelines create no new requirements—rather, as explained above, the CFTC is adopting rules that reflect requirements already in place—their cost and benefits have no incremental impact on the five section 15(a) factors. Customers of CFTC-registrants will continue to benefit from these proposed rules and guidelines in the same way they have benefited from the rules as they were administered by the Agencies.

2. Cost Benefit Considerations of Card Issuer Rules

With respect to specific types of identity theft, section 615(e) of the FCRA identified the scenario involving debit and credit card issuers as being a possible indicator of identity theft. Accordingly, the proposed card issuer rules in this release set out the duties of card issuers

---

[129] 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.*

regarding changes of address. The proposed card issuer rules will apply only to a person that issues a debit or credit card and that is subject to the CFTC's jurisdiction. The proposed 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 from a cardholder, 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 it complies with those procedures. The procedures include: (1) notifying the cardholder of the request in writing or electronically 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.

Proposed § 162.32 would shift oversight of card issuer rules of CFTC-regulated entities from the FTC to the CFTC. These entities should already be in compliance with the FTC's existing card issuer rules, which the FTC began enforcing on December 31, 2010. Because proposed § 162.32 is substantially similar to those existing card issuer rules, these entities should not bear any new costs in coming into compliance. The new regulation does not contain new requirements, nor does it expand the scope of the rules to include new entities that were not already previously covered by the Agencies' card issuer rules.

The existing costs related to proposed § 162.32 would 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 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, CFTC staff does not expect that any CFTC-regulated entities would be subject to the requirements of proposed § 162.32.

The benefits related to adoption of proposed § 162.32, which already exist in connection with the Agencies' card issuer rules, 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 determine with precision the dollar value associated with the benefits that will inure to the public from these proposed card issuer rules. As is true of the Agencies' card issuer rules, the CFTC has designed proposed § 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 proposed 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 proposed rules and guidelines protect market participants and the public by preventing identity theft, an

illegal act that may be costly to them in both time and money.[130] Because, however, these rules create no new requirements—rather, as explained above, the CFTC is adopting rules that reflect requirements already in place—their cost and benefits have no incremental impact on the five section 15(a) factors. Customers of CFTC-registrants will continue to benefit from these proposed rules and guidelines in the same way they have benefited from the rules as they were administered by the Agencies.

3. Questions

- The CFTC requests comment on all aspects of this cost-benefit analysis, including identification, quantification, and assessment of any costs and benefits, whether or not discussed in the above analysis. The CFTC encourages commenters to identify, discuss, analyze, and supply relevant data regarding any additional costs and benefits.
- The CFTC requests comment on the accuracy of the cost estimates in each section of this analysis, and requests that commenters provide data that may be relevant to these cost estimates, including quantification.

In addition, the CFTC seeks estimates and views regarding these costs and benefits for all affected entities, including small entities, as well as any other costs or benefits that may result from the adoption of proposed subpart C to Part 162.

SEC:

The SEC is sensitive to the costs and benefits imposed by its rules. Proposed Regulation S-ID would require financial institutions and creditors that are subject to the SEC's enforcement

---

130 *See id.*

authority under the FCRA[131] and that offer or maintain covered accounts to develop, implement, and administer a written identity theft prevention Program. A financial institution or creditor would have to design its Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. In addition, a financial institution or creditor would have to appropriately tailor its Program to its size and complexity, and to the nature and scope of its activities. There are various steps that a financial institution or creditor would have to take in order to comply with the requirements under the proposed identity theft red flags rules, including training staff, providing annual reports to board of directors, and, when applicable, monitoring the use of third-party 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 proposed card issuer rules in this release set out the duties of card issuers regarding changes of address. The proposed card issuer rules would apply only to SEC-regulated entities that issue credit or debit cards.[132] The proposed card issuer rules would 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 from a cardholder, 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

---

131 *See supra* note 19.

132 *See* proposed § 248.202(a) (defining scope of proposed rule).

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.

As discussed above, the Dodd-Frank Act shifted enforcement authority over SEC-regulated entities that are subject to section 615(e) of the FCRA from the FTC 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 proposing Regulation S-ID, which is substantially similar to the identity theft red flags rules and guidelines adopted by the Agencies in 2007.

Proposed Regulation S-ID would shift oversight of identity theft rules and guidelines of SEC-regulated entities from the FTC to the SEC. These entities should already be in compliance with the FTC's existing rules and guidelines, which the FTC began enforcing on December 31, 2010. Because proposed Regulation S-ID is substantially similar to those existing rules and guidelines, these entities should not bear any new costs in coming into compliance with proposed Regulation S-ID. The new regulation does not contain new requirements, nor does it expand the scope of the rules to include new entities that were not already previously covered by the Agencies' rules. The new regulation does contain examples and minor language changes designed to help guide entities under the SEC's jurisdiction in complying with the 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 proposed Regulation S-ID.[133] However, these costs are not new costs, but are

---

133 Unless otherwise stated, all cost estimates for personnel time are derived from SIFMA's Management & Professional Earnings in the Securities Industry 2010, modified to account for an 1800-hour work-year and multiplied by 5.35 to account for bonuses, firm size, employee benefits, and overhead.

current costs associated with compliance with the Agencies' existing rules. SEC-regulated entities will incur these hours and costs regardless of whether the SEC adopts proposed Regulation S-ID. These hours and costs would be transferred from the Agencies' PRA allotment to the SEC. No new costs should result from the adoption of proposed Regulation S-ID.

These existing costs related to § 248.201 of proposed Regulation S-ID would include, for newly formed SEC-regulated entities, the incremental 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.[134] The existing costs would also include the incremental ongoing cost to periodically review and update the program, report periodically on the Program, and conduct periodic assessments of covered accounts.[135] The existing costs

---

134 SEC staff estimates that the incremental one-time burden of compliance would include 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 would be spent by internal counsel at an hourly rate of $354, 17 hours would be spent by administrative assistants at an hourly rate of $66, and 2 hours would be spent by the board of directors as a whole, at an hourly rate of $4000, for a total cost of $13,370 per entity for entities that need to come into compliance with proposed Regulation S-ID. This estimate is based on the following calculations: $354 x 12 hours = $4248; $66 x 17 = $1,122; $4000 x 2 = $8000; $4248 + $1,122 + $8000 = $13,370.

As discussed in the PRA analysis, SEC staff estimates that there are 1327 SEC-regulated entities that newly form each year and would be financial institutions or creditors, of which 465 would maintain covered accounts. *See infra* note 153 and following text. SEC staff estimates that 2 hours of internal counsel's time would be spent conducting an initial assessment of covered accounts and that all newly formed financial institutions or creditors subject to the proposed rule (or 1327 entities) would bear this cost for a total cost of $939,516 based on the following calculation: $354 x 2 = $708; $708 x 1327 = $939,516. SEC staff estimates that 465 entities would bear the remaining specified costs for a total cost of $5,887,830 (465 x $12,662 = $5,887,830).

135 SEC staff estimates that the incremental ongoing burden of compliance would 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 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 $4000, for a total hourly cost of $6478. This estimate is based on the following calculations: $354 x 7 hours = $2478; $4000 x 1 hour = $4000; $2478 + $4000 = $6478.

related to § 248.202 of proposed Regulation S-ID would include the incremental 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 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 would be subject to the requirements of § 248.202 of proposed Regulation S-ID.

The benefits related to adoption of Regulation S-ID, which already exist in connection with the Agencies' red flags rules and guidelines, 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. Joint adoption by the Commissions of identity theft red flags rules in a form that is substantially similar to the Agencies' identity theft red flags rules and guidelines 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' rules and guidelines, the SEC has designed proposed 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

---

As discussed in the PRA analysis, SEC staff estimates that 7978 existing SEC-regulated entities would be financial institutions or creditors under the proposal and 7180 of these entities maintain covered accounts. *See infra* note 156 and following text. SEC 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 (or 7978 entities) would bear this cost for a total cost of $5,648,424 based on the following calculations: $354 x 2 = $708; $708 x 7978 = $5,648,424. SEC staff estimates that 7180 entities would bear the remaining specified ongoing costs for a total cost of $41,428,600 (7180 x $5770 = $41,428,600).

address verification procedures.

Accordingly, as previously discussed, proposed Regulation S-ID 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 SEC, does not include any significant new requirements, and does not include new entities that were not previously covered by the Agencies' rules.

- The SEC requests comment on all aspects of this cost-benefit analysis, including identification and assessment of any costs and benefits not discussed in this analysis. The SEC encourages commenters to identify, discuss, analyze, and supply relevant data regarding any additional costs and benefits.
- The SEC requests comment on the accuracy of the cost estimates in each section of this analysis, and requests that commenters provide data that may be relevant to these cost estimates.
- In addition, the SEC seeks estimates and views regarding these costs and benefits for all affected entities, including small entities, as well as any other costs or benefits that may result from the adoption of proposed Regulation S-ID.

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

Section 3(f) of the Securities 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 or appropriate in 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 proposing rules under the Exchange Act, to consider the impact the proposed 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.[136]

As discussed in the cost benefit analysis above, proposed Regulation S-ID would carry out the requirement in the Dodd-Frank Act that the SEC adopt rules and guidelines governing identity theft protections, pursuant to section 615(e) of the FCRA with regard to entities that are subject to the SEC's jurisdiction. This requirement was designed to transfer regulatory oversight of identity theft rules and guidelines of SEC-regulated entities from the FTC to the SEC. Proposed Regulation S-ID is substantially similar to the identity theft red flags rules and guidelines adopted by the FTC and other regulatory agencies in 2007, and does not contain new requirements. The entities covered by proposed Regulation S-ID should already be in compliance with existing rules and guidelines, which the FTC began to enforce on December 31, 2010.

For the reasons discussed above, proposed Regulation S-ID should not have an effect on efficiency, competition, or capital formation because it does not include new requirements and does not include new entities that were not previously covered by the Agencies' rules.

- The SEC seeks comment on the potential impact of the proposed rules on efficiency, competition, and capital formation. For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), the SEC also requests information regarding the potential effect of the proposed rules on the U.S. economy on an annual basis. Commenters are requested to provide empirical data to support their views.

---

136 *See infra* Section IV (setting forth statutory authority under, among other things, the Exchange Act and Investment Company Act for proposed rules).

C. Paperwork Reduction Act

CFTC:

Provisions of proposed §§ 162.30 and 162.32 would result in new collection of information requirements within the meaning of the PRA. The CFTC, therefore, is submitting this proposal to the Office of Management and Budget ("OMB") for review in accordance with 44 U.S.C. 3507(d) and 5 CFR 1320.11. OMB has not yet assigned a control number to the new collection. The title for this collection of information is "Part 162 Subpart C—Identity Theft." If adopted, responses to this new collection of information would be mandatory.

1. *Information Provided by Reporting Entities/Persons*

Under proposed part 162, subpart C, CFTC regulated entities – which presently would include approximately 268 CFTC registrants[137] plus 125 new CFTC registrants pursuant to Title VII of the Dodd-Frank Act[138] – may be required to design, develop and implement reasonable policies and procedures to identify relevant red flags, and potentially notifying cardholders of

---

137 *See* the NFA's Internet web site at: *http://www.nfa.futures.org/NFA-registration/NFA-membership-and-dues.HTML* for the most up-to-date number of CFTC regulated entities. For the purposes of the PRA calculation, CFTC staff used the number of registered FCMs, CTAs, CPOs IBs and RFEDs on the NFA's Internet web site as of October 31, 2011. The NFA's site states that there are 3,663 CFTC registrants as of September 30, 2011. Of this total, there are 111 FCMs, 1,441 IBs, 1,054 CTAs, 1,035 CPOs, and 14 RFEDs. CFTC staff has observed that approximately 50 percent of all CPOs are dually registered as CTAs. Based on this observation, CFTC has determined that the total number of entities is 3,124 (518 CPOs that are also registered as CTAs). With respect to RFEDs, CFTC staff also has observed that all entities registering as RFEDs also register as FCMs.

Of the total 3,124 entities, all of the FCMs are likely to qualify as financial institutions or creditors carrying covered accounts, 10 percent of CTAs and CPOs are likely to qualify as financial institutions or creditors carrying covered accounts and none of the IBs are likely to qualify as a financial institution or creditor carrying covered accounts, for a total of 268 financial institutions or creditors that would bear the initial one-time burden of compliance with the CFTC's proposed identity theft rules and guidelines and proposed card issuer rules.

138 CFTC staff estimates that 125 swap dealers and major swap participants will register with the CFTC following the issuance of final rules under the Dodd-Frank Act further defining the terms "swap dealers" and "major swap participants" and setting forth a registration regime for these entities. The CFTC estimates the number of MSPs to be quite small, at six or fewer.

identity theft risks. In addition, CFTC-regulated entities would be 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 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 and guidelines jointly adopted by the FTC with the Agencies, as of December 31, 2010. Consequently, these entities may already have in place many of the customary protections addressing identity theft and changes of address proposed 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 rules and guidelines jointly adopted by the FTC with the Agencies may have occurred, the CFTC estimates the time and cost burdens of complying with proposed part 162 to be both one-time and ongoing burdens. However, any initial or one-time burdens associated with compliance with proposed 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 proposed 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 [139] 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.[140] 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 5,549 hours,[141] for a total burden among newly registered entities of 7,203 hours.[142]

---

139 Based on a review of new registrations typically filed with the CFTC each year, CFTC staff estimates that approximately, 7 FCMs, 225 IBs, 400 CTAs, and 140 CPOs are newly formed each year, for a total of 772 entities. CFTC staff also has observed that approximately 50 percent of all CPOs are duly registered as CTAs. Based on this observation, CFTC has determined that the total number of newly formed financial institutions and creditors is 702 (772 – 70 CPOs that are also registered as CTAs). With respect to RFEDs, CFTC staff has observed that all entities registering as RFEDs also register as FCMs. Each of these 702 financial institutions or creditors would bear the initial one-time burden of compliance with the proposed identity theft rules and guidelines and proposed card issuer rules.

Of the total 702 newly formed entities, staff estimates that all of the FCMs are likely to carry covered accounts, 10 percent of CTAs and CPOs are likely to carry covered accounts, and none of the IBs are likely to carry covered accounts, for a total of 54 newly formed financial institutions or creditors carrying covered accounts that would be required to conduct an initial one-time burden of compliance with subpart C or Part 162.

140 This estimate is based on the following calculation: 827 entities x 2 hours = 1,654 hours.

141 This estimate is based on the following calculation: 179 entities x 31 hours = 5,549 hours.

142 This estimate is based on the following calculation: 1,654 hours for all newly registered CFTC registrants + 7,203 hours for the one-time burden of newly registered entities with covered accounts.

The CFTC requests comments on these estimates of numbers of persons affected and the total hours involved.

ii. Ongoing Burden

The CFTC staff estimates that the ongoing compliance burden associated with proposed 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 3,249 persons may maintain covered accounts, and that they would be required to periodically review their accounts to determine if they comply with these proposed rules, for a total of 76,498 hours for these entities.[143] Of these 3,249 persons, the CFTC estimates that approximately 393 maintain covered accounts, and thus would need to incur the additional burdens related to complying with the rule, for a total of 2,358.[144] The total ongoing burden for all CFTC registrants is 11,256.[145]

2. *Information Collection Comments*

The CFTC invites the public and other federal agencies to comment on any aspect of the burdens discussed above. Pursuant to 44 U.S.C. 3506(c)(2)(B), the CFTC solicits comments in

---

143 This estimate is based on the following calculation: 3,249 entities x 2 hours = 6,498hours.

144 This estimate is based on the following calculation: 393 entities x 6 hours = 2,358 hours.

145 This estimate is based on the following calculation: 6,498hours + 2,358 hours = 8,856 hours.

order to: (i) evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the CFTC, including whether the information will have practical utility; (ii) evaluate the accuracy of the CFTC's estimate of the burden of the proposed collection of information; (iii) determine whether there are ways to enhance the quality, utility, and clarity of the information to be collected; and (iv) minimize the burden of the collection of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology.

Comments may be submitted directly to the Office of Information and Regulatory Affairs, by fax at (202) 395–6566 or by e-mail at *OIRAsubmissions@omb.eop.gov.* Please provide the CFTC with a copy of submitted comments so that all comments can be summarized and addressed in the final rule preamble. Refer to the Addresses section of this notice of proposed rules and guidelines for comment submission instructions to the CFTC. A copy of the supporting statements for the collections of information discussed above may be obtained by visiting *RegInfo.gov*. OMB is required to make a decision concerning the collection of information between 30 and 60 days after publication of this release. Consequently, a comment to OMB is most assured of being fully effective if received by OMB (and the CFTC) within 30 days after publication of this notice of proposed rulemaking.

SEC:

Provisions of proposed §§ 248.201 and 248.202 would result in new collection of information requirements within the meaning of the PRA. The SEC therefore is submitting this proposal to the Office of Management and Budget ("OMB") for review in accordance with 44 U.S.C. 3507(d) and 5 CFR 1320.11. OMB has not yet assigned a control number to the new collection. The title for this collection of information is "Part 248, Subpart C – Regulation S-

ID." An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number. If the rules are adopted, responses to the new collection of information provisions would be mandatory, and the information, when provided to the Commission in connection with staff examinations or investigations, would be kept confidential to the extent permitted by law.

1. *Description of the Collections*

Under proposed Regulation S-ID, SEC-regulated entities would be 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. Proposed § 248.201 of Regulation S-ID would include 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; (2) periodic staff reporting on compliance with the identify theft red flags rules and guidelines, as required to be considered by section VI of the proposed guidelines; and (3) training of staff to implement the Program. Proposed § 248.202 of Regulation S-ID would include the following "collections of information" by any SEC-regulated entities that are credit or debit card issuers: (1) establishment of policies and procedures that assess the validity of a change of address notification if a request for an additional card on the account follows soon after the address change, (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 staff expects that SEC-regulated entities that would comply with the collections of information required by proposed Regulation S-ID should already be fully in compliance with the identity theft red flags rules and guidelines that the FTC jointly adopted with the Agencies and began enforcing on December 31, 2010. The requirements of those rules and guidelines are substantially similar and comparable to the requirements of proposed Regulation S-ID.[146]

In addition, SEC staff understands that most SEC-regulated entities that are financial institutions or creditors would likely already have in place many of the protections regarding identity theft and changes of address that the proposed regulations would require 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 proposed requirements as a result of having to comply (or an affiliate having to comply) with other, existing regulations and guidance, such as the Customer Identification Program regulations implementing section 326 of the USA PATRIOT Act,[147] the Federal Information Processing Standards that implement section 501(b) of the Gramm-Leach-Bliley Act (GLBA),[148] section 216 of the FACT Act,[149] and guidance issued by the Agencies or the Federal Financial Institutions Examination Council regarding information security, authentication, identity theft, and response programs.[150]

---

146 *See* 2007 Adopting Release, *supra* note 10; "FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule" at *http://www.ftc.gov/opa/2010/05/redflags.shtm.*

147 31 U.S.C. 5318(l) (requiring verification of the identity of persons opening new accounts).

148 15 U.S.C. 6801.

149 15 U.S.C. 1681w.

150 *See* 2007 Adopting Release, *supra* note 10, at nn. 55-57 (describing applicable regulations and guidance).

As a result, SEC staff estimates of time and cost burdens here represent the incremental one-time burden of complying with proposed Regulation S-ID for newly formed SEC-regulated entities, and the incremental ongoing costs of compliance for all SEC-regulated entities.[151] SEC staff estimates also attribute all burdens to covered entities, which are entities directly subject to the requirements of the proposed rulemaking. A covered entity that outsources activities to an affiliate or a third-party service provider is, in effect, reallocating to that affiliate or service provider the burden that it would otherwise have carried itself. Under these circumstances, the burden is, by contract, shifted from the covered entity to the service provider, but the total amount of burden is not increased. Thus, affiliate and third-party service provider burdens are already included in the burden estimates provided for covered entities. The time and cost estimates made here are based on conversations with industry representatives and on a review of the estimates made in the regulatory analyses of the identity theft red flags rules and guidelines previously issued by the Agencies.

2. *Proposed § 248.201 (duties regarding the detection, prevention, and mitigation of identity theft)*

The collections of information required by proposed § 248.201 would apply to SEC-regulated entities that are financial institutions or creditors.[152] As stated above, SEC staff expects that all existing SEC-regulated entities would already have incurred one-time burdens

---

151 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 proposed Regulation S-ID, most broker-dealers, many investment companies (including almost all open-end investment companies and employees' securities companies ("ESCs")), and some registered investment advisers would likely qualify as financial institutions or creditors. SEC staff expects that most other SEC-regulated entities described in the scope section of proposed Regulation S-ID, such as transfer agents, NRSROs, SROs, and clearing agencies are unlikely to be financial institutions or creditors as defined in the proposed rule, and therefore we do not include these entities in our estimates.

152 Proposed § 248.201(a).

associated with compliance with proposed Regulation S-ID because they should already be in compliance with the substantially identical requirements of the Agencies' red flags rules and guidelines. Therefore, any initial or one-time burdens associated with compliance with § 248.201 of proposed Regulation S-ID would apply only to newly formed entities. The ongoing burden would apply to all SEC-regulated entities that are financial institutions or creditors.

i. *Initial Burden*

SEC staff estimates that the incremental one-time burden of compliance with proposed § 248.201 for SEC-regulated financial institutions and creditors with covered accounts would be: (i) 25 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 would be spent by internal counsel, 17 hours would be spent by administrative assistants, and 2 hours would be spent by the board of directors as a whole for entities that need to come into compliance with proposed Regulation S-ID.

SEC staff estimates that approximately 517 SEC-regulated financial institutions and creditors are newly formed each year.[153] Each of these 517 entities would need to conduct an

---

153 Based on a review of new registrations typically filed with the SEC each year, SEC staff estimates that approximately 900 investment advisers, 300 broker dealers, 117 open-end investment companies and 10 employees' securities companies typically apply for registration with the SEC or otherwise are newly formed each year, for a total of 1327 entities that would be financial institutions or creditors. The staff estimate of 900 investment advisers is made in light of the recently adopted amendments to rules under the Investment Advisers Act that carry out requirements of the Dodd-Frank Act to transfer oversight of certain investment advisers from the SEC to state regulators and to require certain investment advisers to private funds to register with the SEC. *See* Rules Implementing Amendments to the Investment Advisers Act of 1940, Investment Advisers Act Release No. 3221 (June 22, 2011) [76 FR 42950 (July 19, 2011)]. Of these, SEC staff estimates that all of the investment companies and broker-dealers are likely to qualify as financial institutions or creditors, and 10% (or 90) of investment advisers are likely to also qualify, for a total of 517 total newly formed financial institutions or creditors that would bear the initial one-time burden of compliance with proposed Regulation S-ID.

initial assessment of covered accounts, for a total of 1034 hours.[154] Of these, SEC staff estimates that approximately 90% (or 465) maintain covered accounts. Accordingly, SEC staff estimates that the total one-time burden for the 465 entities would be 14,415 hours, and the total one-time burden for all SEC regulated entities would be 15,449 hours.[155]

- The SEC requests comments on these estimates. Is the estimate that 90% of all financial institutions and creditors maintain covered accounts correct?

ii. *Ongoing Burden*

SEC staff estimates that the incremental ongoing burden of compliance with proposed § 248.201 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 service 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. SEC staff estimates that of the 8 hours incurred, 7 hours would be spent by internal counsel and 1 hour would be spent by the board of directors as a whole.

SEC staff estimates that there are 7978 SEC regulated entities that are either financial institutions or creditors, and that all of these would be required to periodically review their accounts to determine if they offer or maintain covered accounts, for a total of 15,956 hours for these entities.[156] Of these 7978 entities, SEC staff estimates that approximately 90 percent, or

---

154 This estimate is based on the following calculation: 517 entities x 2 hours = 1034 hours.

155 These estimates are based on the following calculations: 465 entities x 31 hours = 14,415 hours; 14,415 hours + 1034 hours = 15,449 hours.

156 Based on a review of entities that the SEC regulates, SEC staff estimates that, as of the end of December 2010, there are approximately 5063 broker-dealers, 1790 active open-end investment companies and 150 employees' securities companies. In light of recently adopted amendments to

7180, maintain covered accounts, and thus would need to bear the additional burdens related to complying with the rule.[157] Accordingly, SEC staff estimates that the total ongoing burden for the 7180 entities to be 43,080 hours, and the total ongoing burden for all SEC-regulated entities as a whole to be 59,036 hours.[158]

- SEC staff requests comments on these estimates.

3. *Proposed § 248.202 (duties of card issuers regarding changes of address).*

The collections of information required by proposed § 248.202 would apply only to SEC-regulated entities that issue credit or debit cards.[159] SEC staff understands that SEC-regulated entities generally do not issue credit or debit cards, but instead partner with other entities, such as banks, that issue cards on their behalf. These partner 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 and guidelines. 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

---

rules under the Investment Advisers Act that carry out requirements of the Dodd-Frank Act to transfer oversight of certain investment advisers from the SEC to state regulators and to require certain investment advisers to private funds to register with the SEC, SEC staff estimates that, when these amendments become effective, there will be approximately 9750 investment advisers registered with the SEC. *See supra* note 153. Of these, SEC staff estimates that all of the broker-dealers, open-end investment companies and employees' securities companies are likely to qualify as financial institutions or creditors, and 10% (or 975) of investment advisers are likely to qualify, for a total of 7978 total financial institutions or creditors that would bear the ongoing burden of compliance with proposed Regulation S-ID. The SEC staff estimates that the other types of entities that are covered by the scope of the SEC's proposed rule would not be financial institutions or creditors that maintain covered accounts. *See* proposed § 248.201(a). This estimate is based on the following calculation: (7978 entities x 2 hours = 15,956 hours).

157 If a financial institution or creditor does not maintain covered accounts, there would be no ongoing annual burden for purposes of the PRA.

158 These estimates are based on the following calculations: (7180 entities x 6 hours = 43,080 hours; 43,080 hours + 15,956 hours = 59,036 hours).

159 Proposed § 248.202(a).

changes of address. Therefore, implementation of this requirement would pose no further burden.

SEC staff does not expect that any SEC-regulated entities would be subject to the information collection requirements of proposed § 248.202. Accordingly, SEC staff estimates that there will be no hourly or cost burden for SEC-regulated entities related to proposed § 248.202.[160]

- SEC staff requests comment on this estimate. Are there any SEC-regulated entities that issue credit or debit cards? If so, what incremental time or cost burden would be imposed by proposed § 248.202 of Regulation S-ID?

4. *Request for Comment*

The SEC requests comment on the accuracy of the estimates provided in this description of collections of information. Pursuant to 44 U.S.C. 3506(c)(2)(B), the SEC solicits comments in order to: (i) evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the SEC, including whether the information will have practical utility; (ii) evaluate the accuracy of the SEC's estimate of the burden of the proposed collections of information; (iii) determine whether there are ways to enhance the quality, utility, and clarity of the information to be collected; and (iv) minimize the burden of the collections of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology.

---

160 When the Agencies adopted their red flags rules, they estimated that it would require approximately 4 hours to develop policies and procedures to assess the validity of changes of address, and that there would be no burden associated with notifying cardholders because all entities already have such a process in place. *See* 2007 Adopting Release, *supra* note 10, at text following n.57. SEC staff estimates that if any SEC-regulated entities do issue cards, the burden for complying with proposed § 248.202 would be comparable to the Agencies' estimates.

Persons wishing to submit comments on the collection of information requirements of the proposed amendments should direct them to the Office of Management and Budget, Attention Desk Officer for the Securities and Exchange Commission, Office of Information and Regulatory Affairs, Room 10102, New Executive Office Building, Washington, DC 20503, and should send a copy to Elizabeth M. Murphy, Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-1090, with reference to File No. S7-02-12. OMB is required to make a decision concerning the collections of information between 30 and 60 days after publication of this release; therefore a comment to OMB is best assured of having its full effect if OMB receives it within 30 days after publication of this release. Requests for materials submitted to OMB by the SEC with regard to these collections of information should be in writing, refer to File No. S7-02-12, and be submitted to the Securities and Exchange Commission, Office of Investor Education and Advocacy, 100 F Street, NE, Washington, DC 20549-0213.

D. Regulatory Flexibility Act

CFTC:

The Regulatory Flexibility Act ("RFA")[161] requires that federal agencies consider whether the regulations 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.[162] The regulations proposed by the CFTC shall affect FCMs, retail foreign exchange dealers, IBs, CTAs, CPOs, swap dealers, and major swap participants. The CFTC has determined that the requirements on financial institutions and creditors, and card issuers set forth

---

161 *See* 5 U.S.C. 601 et seq.

162 *See* 5 U.S.C. 601 et seq.

in the proposed identity theft red flags rules and guidelines and the proposed card issuer 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 final rules and guidelines of the Agencies. Moreover, the CFTC believes that the proposed rules and guidelines include a great deal of flexibility to assist its regulated entities in complying with such rules and guidelines.

Notwithstanding this determination, the CFTC previously determined that FCMs and CPOs are not small entities for the purposes of the RFA.[163] Similarly, in another proposed rulemaking promulgated under the Dodd-Frank Act, the CFTC determined that swap dealers and major swap participants are not, in fact, "small entities" for the purposes of the RFA.[164]

Accordingly, the Chairman, on behalf of the CFTC, hereby certifies pursuant to 5 U.S.C. 605(b) that the proposed rules and guidelines will not have a significant impact on a substantial number of small entities.

- The CFTC invites public comments on its certification.

---

163 *See* the CFTC's previous determinations for FCMs and CPOs at 47 FR 18618, 18619 (Apr. 30, 1982).

164 *See* Confirmation, Portfolio Reconciliation, and Portfolio Compression Requirements for Swap Dealers and Major Swap Participants, 75 FR 81519 (Dec. 28, 2010), in which the CFTC reasoned that swap dealers will be subject to minimum capital and margin requirements and are expected to comprise the largest global financial firms. As a result, swap dealers are not likely to be small entities for the purposes of the RFA. In addition, the CFTC reasoned that major swap participants, by statutory definition, maintain substantial positions in swaps or maintain outstanding swap positions that create substantial counterparty exposure that could have serious adverse effects on the financial stability of the U.S. banking system or financial markets. Based on this analysis, the CFTC concluded that major swap participants are not likely to be small entities for the purposes of the RFA.

SEC:

The SEC's Initial Regulatory Flexibility Analysis ("IRFA") has been prepared in accordance with 5 U.S.C. 603. It relates to the SEC's proposed identity theft red flags rules and guidelines in proposed Regulation S-ID under section 615(e)(1)(C) of the FCRA.[165]

1. *Reasons for, and Objectives of, the Proposed Actions*

The FACT Act, which amended FCRA, 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 prescribe rules related to the detection, prevention, and mitigation of identity theft. The SEC is proposing rules to implement the statutory directives in section 615(e) of the FCRA, which require the SEC to prescribe identity theft regulations jointly with other agencies.

Section 615(e) requires the SEC to prescribe regulations 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 regulations applicable to credit and debit card issuers to implement policies and procedures to assess the validity of change of address requests.

2. *Legal Basis*

The SEC is proposing Regulation S-ID under the authority set forth in 15 U.S.C. 78q, 78q-1, 78*o*-4, 78*o*-5, 78w,, 80a-30, 80a-37, 80b-4, 80b-11, 1681m(e), 1681s(b), 1681s-3 and note, 1681w(a)(1), 6801-6809, and 6825; Pub. L. 111-203, sec. 1088(a)(8), (a)(10), and sec. 1088(b).

---

165 15 U.S.C. 1681m(e).

3. *Small Entities Subject to the Rule*

For purposes of the 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 122 investment companies of the 1790 total registered on Form N-1A meet this definition.[166]

Under SEC rules, for purposes of the Advisers Act and the RFA, an investment adviser generally is a small entity if it: (i) has assets under management having a total value of less than $25 million; (ii) did not have total assets of $5 million or more on the last day of its most recent fiscal year; and (iii) does not control, is not controlled by, and is not under common control with another investment adviser that has assets under management of $25 million or more, or any person (other than a natural person) that had total assets of $5 million or more on the last day of its most recent fiscal year.[167] Based on information in filings submitted to the SEC, 570 of the approximately 11,500 investment advisers registered with the SEC are small entities.[168]

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

---

166 This information is based on staff analysis of information from filings on Form N-SAR and from databases compiled by third-party information providers, including Lipper Inc.

167 Rule 0-7(a).

168 This information is based on data from the Investment Adviser Registration Depository.

entity that is not a small business.[169] SEC staff estimates that approximately 879 broker-dealers meet this definition.[170]

4. *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 prescribe regulations that require financial institutions and creditors to establish reasonable policies and procedures to implement guidelines established by the SEC and other federal agencies that address identity theft with respect to account holders and customers. Section 248.201 of proposed Regulation S-ID would implement this mandate by requiring a covered financial institution or creditor to create an Identity Theft Prevention Program that detects, prevents, and mitigates the risk of identity theft applicable to its accounts.

Section 615(e) also requires the SEC to adopt regulations applicable to credit and debit card issuers to implement policies and procedures to assess the validity of change of address requests. Section 248.202 of proposed Regulation S-ID would implement 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 or more), 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 red flags rules and guidelines that the FTC began enforcing on December 31, 2010, proposed Regulation S-ID should not impose new compliance, recordkeeping, or reporting burdens. If for any reason an SEC-regulated small entity is not

---

169 17 CFR 240.0–10.

170 This estimate is based on information provided in FOCUS Reports filed with the Commission. There are approximately 5063 broker-dealers registered with the Commission.

already in compliance with the existing red flags rules and guidelines issued by the Agencies, the burden of compliance with proposed Regulation S-ID should be minimal because entities already engage in various activities to minimize losses due to fraud as part of their usual and customary business practices. In particular, the rule will direct many of these entities to consolidate their existing policies and procedures into a written Program and may require some additional staff training. Accordingly, the impact of the proposed requirements would be merely incremental and not significant.

The SEC has estimated the costs of proposed Regulation S-ID for all entities (including small entities) in the PRA and cost benefit analyses included in this release. No new classes of skills would be required to comply with proposed Regulation S-ID. SEC staff does not anticipate that small entities would face unique or special burdens when complying with proposed Regulation S-ID.

5. *Duplicative, Overlapping, or Conflicting Federal Rules*

SEC staff has not identified any federal rules that duplicate, overlap, or conflict with the proposed rule or rule or form amendments.

6. *Significant Alternatives*

The Regulatory Flexibility Act 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 proposed Regulation S-ID, the SEC considered the following alternatives: (i) 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 the proposal for small entities; (iii) the use of performance rather than design standards; and (iv) an exemption from coverage of

the proposal, or any part thereof, for small entities.

The proposed rules would require financial institutions and creditors to create an identity theft prevention Program and report to the board of directors, a committee of the board, or senior management at least annually on compliance with the regulations. Credit and debit card issuers would be 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 proposed Regulation S-ID are flexible, and take into account a covered entity's size and sophistication, as well as the costs and benefits of alternative compliance methods. An identity theft prevention Program under proposed Regulation S-ID would 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 costs of compliance. Because small entities maintain covered accounts that pose a risk of identity theft for consumers just as larger entities do, we do not believe that providing an exemption from proposed Regulation S-ID for small entities would comply with the intent of section 615(e), and could subject consumers with covered accounts at small entities to a higher risk of identity theft.

Pursuant to the mandate of section 615(e) of the FCRA, as amended by section 1088 of the Dodd-Frank Act, the SEC and the CFTC are proposing identity theft red flags rules and guidelines jointly, and they would be substantially similar and comparable to the identity theft red flags rules and guidelines 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 proposed by the Commissions and the rules adopted by the Agencies. Because all SEC-regulated entities,

including small entities, should already be in compliance with the substantially similar red flags rules and guidelines that the FTC began enforcing on December 31, 2010, SEC staff does not expect that small entities would need a delayed effective or compliance date.

- The SEC seeks comment and information on any need for alternative compliance methods that, consistent with the statutory requirements, would reduce the economic impact of the rule on such small entities, including whether to delay the rule's effective date to provide additional time for small business compliance.

7. *General Request for Comment*

The SEC requests comments regarding this analysis. It requests comment on the number of small entities that would be subject to the proposed rules and guidelines and whether the proposed rules and guidelines would have any effects that have not been discussed. The SEC requests that commenters describe the nature of any effects on small entities subject to the rules and provide empirical data to support the nature and extent of such effects. It also requests comment on the compliance burdens and how they would affect small entities.

IV. STATUTORY AUTHORITY AND TEXT OF PROPOSED AMENDMENTS

The CFTC is proposing to amend Part 162 under the authority set forth in sections 1088(a)(8), 1088(a)(10) and 1088(b) of the Dodd-Frank Act, Pub.L.111-203, 124 Stat.1376 (2010) and; sections 615(e) [15 U.S.C 1681m(e)], 621(b) [15 U.S.C 1681s(b)], 624 [15 U.S.C 1681s-3 and note], 628 [15 U.S.C. 1681w(a)(1)] of the Fair Credit Reporting Act.

The SEC is proposing Regulation S-ID under the authority set forth in Section 1088(a)(8) of the Dodd-Frank Act,[171] Section 615(e) of the FCRA,[172] Sections 17 and 36 of the Exchange

---

171 Pub. L. No. 111-203, Section 1088(a)(8), 124 Stat. 1376 (2010).

172 15 U.S.C. 1681m(e).

Act,[173] Sections 31 and 38 of the Investment Company Act,[174] and Sections 204 and 211 of the Investment Advisers Act.[175]

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, Fair and Accurate Credit Transactions Act, Fair Credit Reporting Act, Financial institutions, Futures commission merchants, Gramm-Leach-Bliley Act, 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, Consumer reports, Credit, Creditors, Dealers, Fair and Accurate Credit Transactions Act, Fair Credit Reporting Act, Financial institutions, Gramm-Leach-Bliley Act, Identity theft, Investment advisers, Investment companies, Privacy, Reporting and recordkeeping requirements, Securities, Security measures, Self-regulatory organizations, Transfer agents.

TEXT OF PROPOSED RULES

Commodity Futures Trading Commission

For the reasons stated above in the preamble, the Commodity Futures Trading Commission proposes to amend 17 CFR part 162 to read as follows:

---

173 15 U.S.C. 78q and 78mm.

174 15 U.S.C. 80a-30 and 80a-37.

175 15 U.S.C. 80b-4 and 80b-11.

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

Subpart C—Identity Theft Red Flags

Sec.

162.22 – 162.29 [Reserved]

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

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, 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(r)(5) of the FCRA, 15 U.S.C. 1681a(r)(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(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.

(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)(ii) 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) of this part 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)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

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

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

2. 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 of this part requires each financial institution or creditor that offers or maintains one or more covered accounts, as defined in § 162.30(b)(3) of this part, 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 of this part.

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 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 website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the 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 soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Identity Theft Prevention Program

(a) *Oversight of Identity Theft Prevention Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated senior management employee should include:

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

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 162.30 of this part; and

(3) Approving material changes to the Identity Theft Prevention Program as necessary to address changing identity theft risks.

(b) *Reports*. (1) *In general*. Staff of the financial institution or creditor responsible for development, implementation, and administration of its Identity Theft Prevention 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 § 162.30 of this part.

(2) *Contents of report*. The report should address material matters related to the Identity Theft Prevention Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Identity Theft Prevention Program.

(c) *Oversight of service provider arrangements*. Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and

procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix 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. 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(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 and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

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

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

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

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

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

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

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

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

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

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

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

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

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

18. For financial institutions 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 above in the preamble, the Securities and Exchange Commission proposes to amend 17 CFR part 248 to read as follows:

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

Authority: 15 U.S.C. 78q, 78q-1, 78*o*-4, 78*o*-5, 78w, 80a-30, 80a-37, 80b-4, 80b-11, 1681m(e), 1681s(b), 1681s-3 and note, 1681w(a)(1), 6801-6809, and 6825; Pub. L. 111-203, sec. 1088(a)(8), (a)(10), and sec. 1088(b).

2. Revise the heading for part 248 to read as follows:

Part 248 – REGULATIONS S-P, S-AM, AND S-ID

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

Sec.

248.129 – 248.200 [Reserved]

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

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

248.202 Duties of card issuers regarding changes of address.

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

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

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

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

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

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

(b) *Definitions*. For purposes of this subpart, and Appendix A of this subpart, the following definitions apply:

(1) *Account* means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business

purposes. Account includes a brokerage account, a *mutual fund* account (*i.e.*, an account with an open-end investment company), and an investment advisory account.

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

(i) In the case of a branch or agency of a non U.S. based 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(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681m(e)(4), and includes lenders such as brokers or dealers offering margin accounts, securities lending services, and short selling services.

(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)).

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

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

(iv) *Investment adviser* has the same meaning as in section 202(a)(11) of the Investment

Advisers Act of 1940 (15 U.S.C. 80b-2(a)(11)).

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

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

(c) *Periodic Identification of Covered Accounts*. Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program* –

(1) *Program requirement*. Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Program*. The Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or

creditor offers or maintains, and incorporate those Red Flags into its Program;

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

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

(iv) Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Program.* Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;

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

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

(f) *Guidelines.* Each financial institution or creditor that is required to implement a Program must consider the guidelines in Appendix A to this subpart and include in its Program those guidelines that are appropriate.

§ 248.202 Duties of card issuers regarding changes of address.

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

or debit card (card issuer).

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

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

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

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

(c) *Address validation requirements*. A card issuer must establish and implement reasonable written policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1) (i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the

policies and procedures the card issuer has established pursuant to § 248.201 of this part.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and be provided separately from its regular correspondence with the cardholder.

4. Add Appendix A to subpart C of part 248 to read as follows:

Appendix A to Subpart C of Part 248—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 248.201 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 248.201(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 248.201 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably

foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors*. A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;

(2) The methods it provides to open its covered accounts;

(3) The methods it provides to access its covered accounts; and

(4) Its previous experiences with identity theft.

(b) *Sources of Red Flags*. Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;

(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and

(3) Applicable regulatory guidance.

(c) *Categories of Red Flags*. The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious

address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(*l*) (31 CFR 1023.220 (broker-dealers) and 1024.220 (mutual funds)); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial

institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

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

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 248.201 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.*

(1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 248.201 of this part.

(2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements;

significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements*. Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s-2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is

inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix A

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix A to this subpart, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as referenced in Sec. 605(h) of the Fair Credit Reporting Act (15 U.S.C. 1681c(h)).

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a

financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

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

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

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

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

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

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

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

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

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

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

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

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

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

18. For financial institutions and creditors that use challenge questions, the person

opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

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

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement means of accessing the account or for the addition of an authorized user on the account.

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

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

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

c. A material change in purchasing or spending patterns; or

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

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

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

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

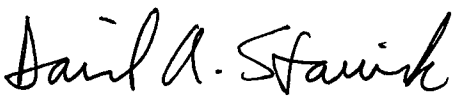
24. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

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

By the Commodity Futures Trading Commission.

February 28, 2012



David A. Stawick,
Secretary of the Commodity Futures Trading Commission

By the Securities and Exchange Commission.

February 28, 2012

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